HSSEDI
Homeland Security Systems Engineering & Development Institute

Prepared for:
Department of Homeland Security

Cyber Threat Modeling:
Survey, Assessment, and Representative Framework

April 7, 2018

Authors:

Deborah J. Bodeau
Catherine D. McCollum
David B. Fox

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

Approved for Public Release; Distribution Unlimited.
Case Number 18-1174 / DHS reference number 16-J-00184-01

HSSEDI
Homeland Security Systems Engineering & Development Institute

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. The MITRE Corporation 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

Abstract

This report provides a survey of cyber threat modeling frameworks, presents a comparative assessment of the surveyed frameworks, and extends an existing framework to serve as a basis for cyber threat modeling for a variety of purposes. The Department of Homeland Security (DHS) Science and Technology Directorate (S&T) Next Generation Cyber Infrastructure (NGCI) Apex program will use threat modeling and cyber wargaming to inform the development and evaluation of risk metrics, technology foraging, and the evaluation of how identified technologies could decrease risks. A key finding of the assessment was that no existing framework or model was sufficient to meet the needs of the NGCI Apex program. Therefore, this paper also presents a threat modeling framework for the NGCI Apex program, with initial population of that framework. The survey, assessment, and framework as initially populated are general enough to be used by medium-to-large organizations in critical infrastructure sectors, particularly in the Financial Services Sector, seeking to ensure that cybersecurity and resilience efforts consider cyber threats in a rigorous, repeatable way.

Key Words

1. Cyber Threat Models
2. Next Generation Cyber Infrastructure (NGCI)
3. Cyber Risk Metrics
4. Cybersecurity
5. Threat Modeling Framework

This page intentionally left blank

Table of Contents

List of Figures

List of Tables

1 Introduction

This report provides a survey of cyber threat modeling frameworks, presents a comparative assessment of the surveyed frameworks, and extends an existing framework to serve as a basis for cyber threat modeling for a variety of purposes.

The work in this report was performed for the Department of Homeland Security (DHS) Science and Technology Directorate (S&T) Next Generation Cyber Infrastructure (NGCI) Apex Program. That program seeks to accelerate the adoption of effective information technology (IT) security risk-mitigating cyber technologies by the Financial Services Sector (FSS). However, while the NGCI Apex Program focuses on the FSS, cyber threat modeling is more broadly applicable to medium-to-large organizations in other critical infrastructure sectors; it is also applicable beyond individual organizations. Therefore, this report is offered as a general resource for non-military use.[1]

Cyber threat modeling is the process of developing and applying a representation of adversarial threats (sources, scenarios, and specific events) in cyberspace. Such threats can target or affect a device, an application, a system, a network, a mission or business function (and the system-of-systems which support that mission or business function), an organization, a region, or a critical infrastructure sector. The cyber threat modeling process can inform efforts related to cybersecurity and resilience in multiple ways:

- **Risk management**. Cyber threat modeling is a component of cyber risk framing, analysis and assessment, and evaluation of alternative responses (individually or in the context of cybersecurity portfolio management), which are components of enterprise risk management. While non-adversarial threats can – and must – also be considered in risk management, this paper focuses on adversarial threat models for cybersecurity and resilience. See Section 1.2.1.
- **Cyber wargaming**. Cyber threat modeling motivates and underlies the development of threat scenarios used in cyber wargaming. In this context, cyber threat modeling is strongly oriented toward the concerns of the stakeholders participating in or represented in wargaming activities. See Section 1.2.2.
- **Technology profiling and foraging**. Cyber threat modeling can motivate the selection of threat events or threat scenarios used to evaluate and compare the capabilities of technologies, products, services. That is, cyber threat modeling can enable technology profiling, both to characterize existing technologies and to identify research gaps. It can also support technology foraging, i.e., the process of scouting for and identifying technologies of potential interest. See Section 1.2.3.
- **Systems security engineering**. Cyber threat modeling can be used throughout the system development lifecycle (SDLC), including requirements definition, analysis and design, implementation, testing, and operations and maintenance (O&M). However, it is particularly important for design analysis and testing, where it motivates and underlies

[1] An excellent survey of the state of the art in cyber threat modeling for military purposes was prepared for Defence Research and Development Canada (DRDC) by Bell Canada and Sphyrna Security [Magar 2016]. The framework developed in that report is discussed in Section 2.

the development of threat scenarios used to design and test devices, applications, and/or systems [Kosten 2017]. Thus, cyber threat modeling can be oriented toward a specific layer or set of layers in a notional layered architecture. While this purpose is not the primary focus of this survey, some cyber threat modeling frameworks and approaches oriented to this purpose are included in the survey.

- **Security operations and analysis**. Cyber threat modeling can focus activities by cyber defenders, including threat hunting (searching for indicators or evidence of adversary activities), continuous monitoring and security assessment, and DevOps (rapid development and operational deployment of defense tools), on specific types of threat events. For this purpose, threat information sharing is crucial. To share threat information, a common conception is needed of what constitutes such information – what information is relevant and useful [NIST 2016c]. Some cyber threat modeling frameworks and approaches oriented to this purpose are included in the survey.

The process of cyber threat modeling involves selecting a cyber threat modeling framework and populating that framework with specific values (e.g., adversary expertise, attack patterns and attack events) as relevant to the intended scope (e.g., architectural layers or stakeholder concerns). The populated framework can be used to construct threat scenarios (for risk assessment, cyber wargaming, design analysis and testing); characterize controls, technologies, or research efforts (for technology foraging); and/or to share threat information and responses.

This introductory section presents key concepts and terminology, discusses some uses of cyber threat modeling, and provides background on the survey and assessment process used to develop this report. Section 2 provides a survey of cyber threat modeling frameworks and methodologies. Section 3 presents a survey of populated cyber threat models or sub-models. Figure 1 illustrates the fact that cyber threat modeling frameworks and methods have been developed as part of risk frameworks and modeling methods, as general approaches to cyber threat modeling, oriented toward enterprise information technology (EIT), and for non-EIT environments. The figure gives a sense of the range of modeling frameworks surveyed in Sections 2 and 3.

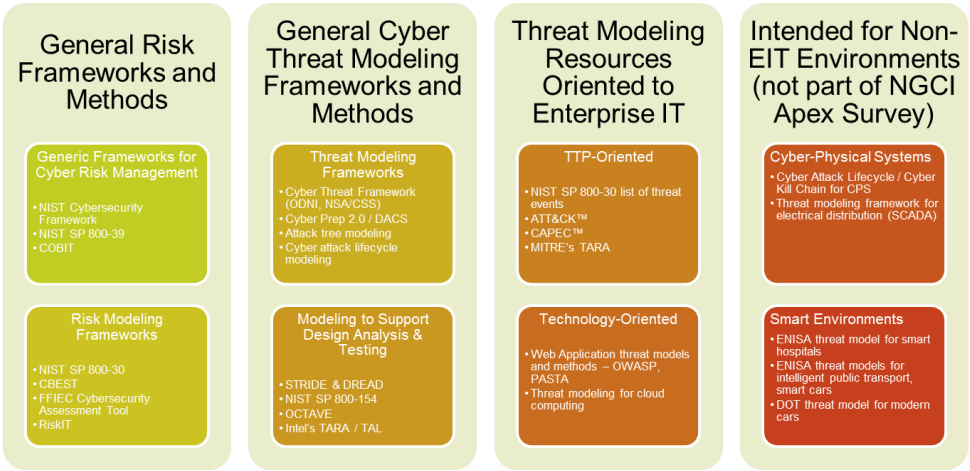

Figure 1. Threat Models Are Developed from a Variety of Perspectives

Section 4 presents the analysis and assessment of the surveyed materials with respect to the goals of the NGCI Apex Program. Section 5 provides an initial and partially populated cyber threat

modeling framework for use by the NGCI Apex Program, which may also be of broader use. Appendix A explains relevant threat modeling constructs. Finally, a glossary, list of acronyms, and references are provided.

1.1 Key Concepts and Terminology

A *model* is an abstract representation of some domain of human experience, used (1) to structure knowledge, (2) to provide a common language for discussing that knowledge, and (3) to perform analyses in that domain.

A variety of terms are used in threat modeling, including threat, threat actor, threat event, threat vector, threat scenario, campaign, attacker, attack, attack vector, attack activity, malicious cyber activity, and intrusion. Different threat modeling approaches define these terms differently, due to assumptions about the contexts and purposes for which they will be used. Terminology related to threat is embedded in a larger setting of terminology about risk. Definitions therefore depend on the larger understanding of risk, and on assumptions about the technological and operational environment in which risk will be managed.

At a minimum, a few concepts are key. These concepts relate to undesirable events; the forces or actors which could cause those events to occur; stories or structured accounts of how one or more undesirable events could result in harm; and the harms which could result. In general, the terms corresponding to these concepts are *threat event*, *threat source*, *threat scenario*, and *consequences*. For the NGCI Apex program, the focus is on cyber attacks as defined by [OFR 2017]: "Cyberattacks are deliberate efforts to disrupt, steal, alter, or destroy data stored on IT systems."

The Federal Financial Institutions Examination Council (FFIEC) Information Security (IS) Handbook on Risk Assessment[2] [FFIEC 2016] defines threats as events:

> *Threats* are events that could cause harm to the confidentiality, integrity, or availability of information or information systems, through unauthorized disclosure, misuse, alteration, or destruction of information or information systems.

However, the term "threat" is also used more broadly, to include circumstances and to modify other terms.

Risk assessment guidance is published by the National Institute of Standards and Technology (NIST) in NIST Special Publication (SP) 800-30R1 [NIST 2012]. NIST SP 800-30R1 defines several terms related to threat:

> *Threat*: Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service.

[2] The first (2001) version of NIST SP 800-30 is also specifically referenced by the FFIEC Handbook for Information Security as an example of elements that comprise a sound risk assessment process. The guide defines a threat model framework consisting of threat sources, threat events, vulnerabilities, likelihood (susceptibility), and impact. The 2001 version, though superseded, can be found for reference at http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf.

> *Threat event*: An event or situation that has the potential for causing undesirable consequences or impact.
>
> *Threat scenario*: A set of discrete threat events, associated with a specific threat source or multiple threat sources, partially ordered in time. Synonym for *Threat Campaign*.

In the FFIEC IS Handbook, threats come from *agents* (referred to in other references as *threat actors* or *adversaries*) who are internal or external. They have different capabilities and motivations, which require the use of different risk mitigation and control techniques. Note that this characterization (unlike the one provided in NIST SP 800-30R1) does not consider threats from nation-state sources, which might seek competitive intelligence but might also try to cause harm as a national security matter, whether illicitly or openly in coordination with other international conflict.

NIST SP 800-30R1 identifies four types of *threat sources*: adversarial, accidental, structural, and environmental. In Table D-2, NIST SP 800-30R1 describes adversarial threats (i.e., threat actors) as:

> Individuals, groups, organizations, or states that seek to exploit the organization's dependence on cyber resources (i.e., information in electronic form, information and communications technologies, and the communications and information-handling capabilities provided by those technologies).

An adversarial threat has two main aspects: characteristics (e.g., capabilities, intent, and targeting [NIST 2012]) and behaviors (often referred to as *malicious cyber activities* [NSTC 2016] or *attack activities*). Adversary characteristics related to capabilities can include methods resources that can be directed or allocated, and relationships [Bodeau 2013]. Intent can have multiple aspects: (i) cyber goals or intended cyber effects (e.g., denial of service, data modification), (ii) non-cyber goals (e.g., financial gain), and (iii) risk trade-offs [Bodeau 2014]. Behaviors can be described as tactics, techniques, and procedures (TTPs):

> "*Tactics* are high-level descriptions of behavior, *techniques* are detailed descriptions of behavior in the context of a tactic, and *procedures* are even lower-level, highly detailed descriptions in the context of a technique. TTPs could describe an actor's tendency to use a specific malware variant, order of operations, attack tool, delivery mechanism (e.g., phishing or watering hole attack), or exploit." [NIST 2016c]

Both the FFIEC IS Handbook and the NIST SP 800-30R1 definitions specifically enumerate the types of *consequences* that a (cyber) threat could cause, in terms of effects on information and information systems. These *cyber effects*, whether expressed as loss of confidentiality, integrity, or availability, or expressed using a more nuanced vocabulary [Temin 2010], can be translated into effects on: the organization; its customers, partners, or suppliers; its sector; mission or business functions within the organization or across the sector; or the Nation.

The behaviors or actions of an adversarial threat actor can be characterized in terms of the threat vector (or attack vector) they use:

> *Attack vectors* or avenues of attack are general approaches to achieving cyber effects, and can include cyber, physical or kinetic, social engineering, and supply chain attacks. [Bodeau 2014]

Attack vectors are strongly influenced by the underlying model or set of assumptions about the technical and operational environment in which an attack occurs. Thus, attack vectors are often enumerated in the context of incident handling [NIST 2012b] or vulnerability remediation [FIRST 2015].

Adversary behaviors can be organized, using a *cyber attack lifecycle* or *cyber kill chain model*, into a threat scenario or attack scenario. Numerous variants of these models have been developed. Examples include the Lockheed Martin cyber kill chain [Cloppert 2009] and the structure of a threat campaign given in NIST SP 800-30R1. See Section 2.1.6.3 for a discussion of cyber attack lifecycle models. Threat scenarios can be represented graphically (as *attack graphs*) or using a tree structure (as *attack trees*), as well as verbally (e.g., in an exercise).

1.2 Uses of Threat Modeling

As noted, cyber threat modeling can serve any of a variety of purposes. Three of these purposes were identified as particularly relevant to the NGCI Apex Program: input into the definition and evaluation of risk metrics, which support risk management; construction of threat scenarios to be used in cyber wargaming; and technology foraging. These are discussed below.

1.2.1 Risk Management and Risk Metrics

Risk management can be described as consisting of four component processes: risk framing, risk assessment, risk response, and risk monitoring [NIST 2011]. Risk framing involves stating assumptions about the environment in which risk will be managed and defining a risk management strategy (e.g., how alternative risk mitigations will be prioritized – what belongs in a portfolio of cybersecurity solutions). Assumptions about threat sources (particularly adversary characteristics) are central to risk framing, while characteristics or taxonomies of threat events can be used in cybersecurity portfolio management. Risk assessment brings together all aspects of the threat model with an environmental model (i.e., a representation of the operational and technical environment in which threats could occur), so that the likelihood and consequence severity of threat scenarios or individual threat events can be estimated or evaluated. Risk response involves evaluation of potential alternative risk mitigations (ways to reduce likelihood and/or severity of consequences), and thus focuses on the threat event and threat scenario portions of a threat model. Risk monitoring involves searching for indications of change in the environment, particularly indicators of adversary activity within systems undergoing continuous monitoring and security assessment; while the portion of risk monitoring focused on systems emphasizes threat events and relies on threat information sharing, higher-level intelligence analysis looks for changes in adversary characteristics, and feeds back into risk framing and risk assessment.

Cybersecurity risk can be managed at varying scopes. Within an organization, risk can be managed at the organizational tier (or executive level), the mission/business function tier (or business/process level), and the information system tier (or implementation/operations level) [NIST 2011]. Beyond these, two additional levels can be identified: the sector, region, or community-of-interest (COI) tier, and the national or transnational level [Bodeau 2014]. These are illustrated in Figure 2.

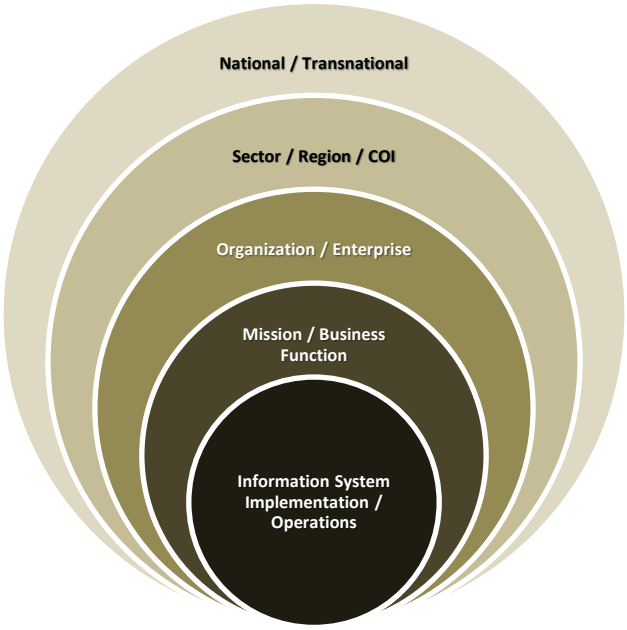

Figure 2. Scope of Risk Management Decisions to Be Supported by Threat Model

A threat model can be oriented toward one or more of these levels:

- At the system implementation or operations level, a threat model – or threat intelligence structured by a threat model – can motivate selection of specific security controls or courses of action. Depending on the stage in the SDLC, a threat model can inform design decisions or security operations.
- At the mission or business function level, a threat model can motivate elements of the enterprise architecture, the organization's information security architecture, and specific mission or business function architectures.
- At the organizational level, a threat model reflects and expresses the organization's assumptions about its threat environment; these are an integral part of the organization's risk frame [NIST 2011]. Note that risk management at the organizational level can consider not only a given organization's cyber resources, but also those resources it obtains from service providers (e.g., network telecommunications, cloud services, managed security services). For example, an organization's service level agreement (SLA) with a cloud provider can be based on a shared or an organization-defined threat model.
- At levels above the enterprise, a threat model can provide a common structure for threat intelligence information sharing and can support the development of multi-participant exercises or cyber wargames.

A threat model is part of the risk assessment deliverable identified as a standard requirement levied on a supplier of network-connectable software, systems or devices in the Procurement Requirements appendix of the Cyber Insurance Buying Guide [FSSCC 2016].

Threat modeling for risk assessment can be approached from three directions: by first modeling the threat, generally or specifically, and then applying it to a relevant environment; by first modeling the systems, data, and boundaries in the environment and then determining what

threats are relevant; or by first identifying the organizational assets that could be affected by threats, characterizing the threats that could affect or target those assets, and situating the assets in terms of systems [Potteiger 2016] [NIST 2016]. These three approaches are illustrated in Figure 3. Note that while each approach focuses on a different aspect of risk as a starting point, assumptions about the other aspects are used implicitly to determine the scope of the primary aspect.

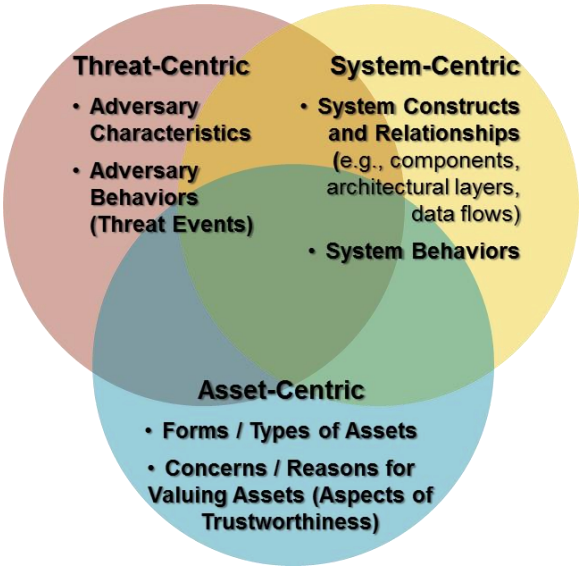

Figure 3. Threat Modeling Approaches

Using any of these threat modeling approaches, risk is estimated by assessing identified threat events or scenarios, in the context of relevant vulnerabilities and environmental assumptions, as to likelihood of occurrence and severity of impact. The resulting measure is the result of any inherent risk, minus the mitigation of threats provided by implemented controls, and constitutes a measure of residual risk. This process may iterate as additional controls are identified and implemented, and as evolving threat capabilities are identified and reported.

Measuring risk levels and identifying operational processes that support ongoing mitigation of cyber threats should result in a reporting capability for significant risk-based metrics. Development of metrics is outside the scope of this document, but risk metrics are critical to providing executive managers with oversight capabilities to establish a cyber program baseline to manage acceptable residual risk to the institution.

1.2.2 Cyber Wargaming

Cyber wargaming is 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. Examples include tabletop exercises, red-team exercises, and hybrid combinations of tabletop and red-team exercises. Red-team and hybrid exercises can simulate attack and defense activities on an operational system, on a cyber range, in a testbed, or in a laboratory. Modeling and simulation (M&S) can be used to develop scenarios for a cyber wargame, or can support hybrid exercises and simulation experiments (SIMEX, [MITRE 2009]).

Cyber threat modeling supports cyber wargaming by creating an adversary profile which is enacted by the red team (or represented in the script for a tabletop exercise, or as a set of parameters in M&S), in identifying plausible threat events, and developing threat scenarios.

1.2.3 Technology Profiling and Technology Foraging

Cybersecurity controls, technologies, and practices serve to mitigate risks. Any organization is resource-constrained, and thus cannot implement all possible risk mitigations. Potential risk mitigations can be characterized in terms of the threats (typically, the types of threat events) they address, as well as using other structuring frameworks. Threat models, consisting of verbal summaries of adversary characteristics and typical behaviors, are commonplace in published descriptions of research and development (R&D) efforts. A more detailed threat model, consisting of a list of threat events, is included in the Security Problem Definition section of a Protection Profile or of the Security Target for a product to be evaluated against the Common Criteria (CC) under the National Information Assurance Partnership (NIAP).[3]

To support technology foraging, categorizations such as matrix approaches can be used. By placing risk mitigations and threat events in the cells of such matrices, analysts can develop testable hypotheses about the effects of the mitigations. One structuring framework is derived in part from the NIST Cybersecurity Framework (CSF, [NIST 2014]), described in more detail in Section 2.1.1. In the Cyber Defense Matrix used by the Cyber Apex Review Team (CART) and illustrated in Figure 4, technologies and products are mapped to the five functions defined by the CSF (columns) they perform and the classes of assets (rows) for which they perform those functions. The Network-Detect cell, for instance, is at the intersection of the Detect function and the Network asset class. The CART's Cyber Defense Matrix has been elaborated, in some contexts, with additional cells for areas not directly captured by the function-asset mapping. In particular, cells are sometimes included for Analytics and Visualization and for Orchestration and Automation. The CART has identified four cells as of particular interest to the FSS: Network-Identify, Network-Detect, Data-Protect, and Data-Detect.

[3] See https://www.niap-ccevs.org/.

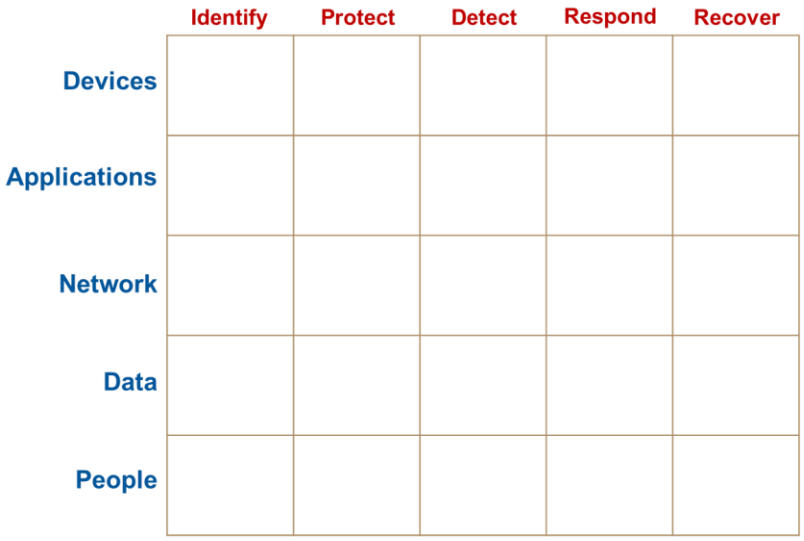

Figure 4. The Cyber Defense Matrix

Since threats can be characterized in terms of the types of assets they affect, the cells in the Cyber Defense Matrix can be viewed as characterizing the types of effects a given risk mitigation could have on a threat.

Two related matrices are those provided by the U.S. Cyber Consequences Unit (US-CCU) [Borg 2016]. One matrix characterizes vulnerabilities (and can be used to characterize specific adversary activities) in terms of an adversary's attack action (columns) and the type of assets in which the vulnerability is exploited (rows). Adversary attack actions include find, penetrate, co-opt, conceal, and make irreversible (Note that this categorization of attack actions is, in effect, a cyber attack lifecycle.) Asset types include hardware, software, networks, automation, users, and suppliers. The second matrix characterizes risk mitigations in terms of their effects on adversary goals (e.g., harder to find, harder to penetrate) for each type of asset.

Another matrix approach characterizes risk mitigations in terms of the phases of the Lockheed-Martin cyber kill chain (rows) and Department of Defense (DoD) effects on a military adversary (columns). Those effects include detect, deny, disrupt, degrade, deceive, and destroy [Cloppert 2009, Bedell 2016]. By contrast, the Community Attack Model developed by the Center for Internet Security (CIS) uses a matrix in which the rows correspond to the CSF functions, but the columns correspond to attack stages in a nine-stage cyber attack lifecycle [CIS 2016]; the CIS Critical Security Controls are mapped to cells in that matrix.

1.3 Survey and Assessment Approach

The set of frameworks and models described in Sections 2 and 3 was identified by subject matter experts (SMEs) within MITRE, the NGCI Apex program, and the CART. A few threat modeling approaches specific to DoD or other military organizations were identified by SMEs as potentially relevant to the FSS and used as inputs to the survey. The assessment was driven by the scope of desired uses for a cyber threat model identified by the NGCI Apex program – risk management, cyber wargaming within an organization and across a sector or sub-sector, technology foraging, and technology evaluation.

The survey and assessment focused on cyber threats targeting or exploiting enterprise IT, since the FSS depends heavily on it. However, other critical infrastructure sectors depend heavily on operational technology (OT). Even organizations in the FSS depend – or will increasingly depend – on cyber-physical systems (CPS) such as, for instance, automated teller machines (ATMs) and OT. For example, convergence between EIT and building access and control systems (BACS) can increase efficiency and decrease operating costs. Cyber threat modeling for CPS, OT, and the Internet of Things (IoT) is an area of future work.

2 Threat Modeling Frameworks and Methodologies

This section summarizes a number of threat modeling frameworks and methodologies. Some approaches to threat modeling are implicitly or explicitly included in risk management approaches; these are presented in Section 2.1. Other approaches are intended to be integrated into system design processes; these are discussed in Section 2.2. Finally, some threat modeling frameworks are intended to support or leverage threat information sharing; these are presented in Section 2.3. The frameworks and methodologies described in this section are either not populated with threat events, or include only a representative starting set of threat events. Populated threat models are described in Section 3.

2.1 Frameworks for Cyber Risk Management

Several frameworks for cyber risk management – management of risks due to dependence on cyber resources, given that cyberspace is contested or includes bad actors – assume an underlying threat model or threat modeling framework. In particular:

- Threat modeling is implicit in the NIST Framework for Improving Critical Infrastructure Cybersecurity (see Section 2.1.1).
- Threat modeling is explicit in NIST SP 800-30R1, and is integral to the view of risk management developed by the DoD's Joint Task Force (JTF) Transformation Initiative (described in Section 2.1.2) and represented by multiple NIST Special Publications (SPs).
- Threat modeling is integral to the assessment process in the Bank of England's CBEST[4] framework (discussed in Section 2.1.3).

Further, many cyber threat modeling approaches have some elements in common. Cyber attack lifecycle models or cyber kill chain models inform many of them. Attack trees or attack graphs provide a structuring framework for the development of threat scenarios.

2.1.1 NIST Framework for Improving Critical Infrastructure Cybersecurity

NIST released Version 1.0 of its Framework for Improving Critical Infrastructure Cybersecurity in February, 2014 [NIST 2014]. A revision was published in April, 2018 [NIST 2018b]. The Cybersecurity Framework (CSF) defines a high-level approach to risk management, to complement the cybersecurity programs and risk management processes of organizations in critical infrastructure sectors. As illustrated in Figure 5, the CSF has two major components: the four Implementation Tiers and the Framework Core.

[4] CBEST is not an acronym.

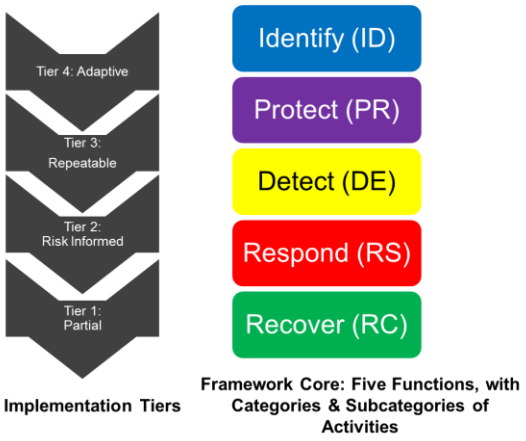

Figure 5. Risk Management Implementation Tiers and Functions in the NIST Cybersecurity Framework

In the CSF approach, as illustrated in Figure 6, an organization implicitly or explicitly asserts its assumptions about the risks to which it is subject, including assumptions about the threats it faces. Senior executives establish mission priorities and determine the organization's Implementation Tier. Based on this senior-level direction, mission and business process owners develop the organization's Framework Profile – selections and refinements of categories and sub-categories of activities under the five functions defined in the Framework Core, aligned with the business requirements, risk tolerance, and resources of the organization. For the organization's systems, risk management involves applying the organization's assumptions, priorities, and Framework Profile, together with (if the Implementation Tier is high enough) threat intelligence. Risk management at the system level also involves monitoring system status as well as changes to assets, vulnerabilities, and/or threats.

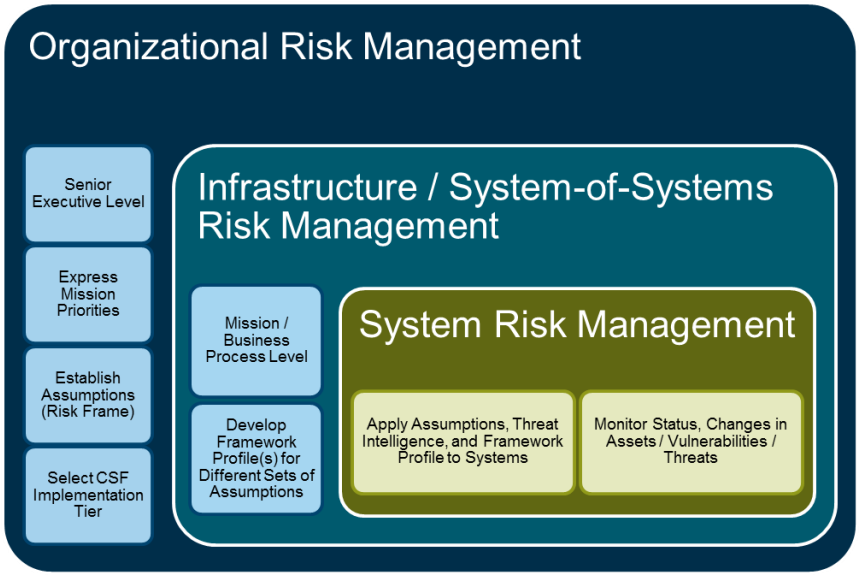

Figure 6. Risk Management Scope of Decision Making in the NIST Cybersecurity Framework

The CSF states that:

> "Cybersecurity threats exploit the increased complexity and connectivity of critical infrastructure systems, placing the Nation's security, economy, and public safety and health at risk."

The CSF does not define cyber threat modeling terms, but uses the following terms: cybersecurity threats, threat exposure, threat environment, evolving and sophisticated threats, and cyber threat intelligence.

It should be noted that the three levels at which risk management is performed in the NIST framework are consistent with the three levels of risk management defined in NIST SP 800-39, Managing Information Security Risk [NIST 2011]: organizational, mission / business function, and system. NIST SP 800-39 provides the organizational context for NIST SP 800-30 and the draft NIST SP 800-154.

In addition, the Framework's Core Functions can be used to group and review mitigations for identified threats. Coupled with NIST SP 800-30R1 [NIST 2012] and other risk processes, it provides a common framework that is consistent with, and can be applied using, other publications such as Control Objectives for IT (COBIT) (Section 2.1.4) and the Federal Financial Institutions Examination Council's Handbook for Information Security [FFIEC 2016].

2.1.2 Publications Produced by the Joint Task Force Transformation Initiative

The DoD, Intelligence Community (IC), and Federal agencies via representation by the NIST created the Joint Task Force Transformation Initiative to move from a compliance-oriented approach to cybersecurity to one based on risk management. Several NIST publications support this transition, including NIST SP 800-37 [NIST 2010], NIST SP 800-39 [NIST 2011], NIST SP 800-30R1 [NIST 2012], and NIST SP 800-53R4 [NIST 2013]. The Committee on National Security Systems (CNSS) has provided additional publications, including CNSS Instruction (CNSSI) 1253 [CNSS 2014].[5] [6]

The risk management process as defined in NIST SP 800-39 consists of four activities: risk framing, risk assessment, risk response, and risk monitoring. NIST SP 800-39 defines a risk frame as "the set of assumptions, constraints, risk tolerances, and priorities/trade-offs that shape an organization's approach for managing risk." The assumptions about threat sources and threat events – specifically including the types of adversarial tactics, techniques, and procedures (TTPs) to be addressed, and adversarial characteristics (e.g., capability, intent, targeting) – implicitly or explicitly define the organization's threat model. This threat model is further refined and

[5] In the context of the JTF publications, the phrase "risk management framework" (RMF) has various interpretations. As defined in CNSSI 4009 [CNSS 2015], the RMF is "a structured approach used to oversee and manage risk for an enterprise." This high-level and general definition encompasses risk management at all levels (organization, mission / business process, and system) in the approach to risk management defined in NIST SP 800-39. The risk management approach defined in NIST SP 800-39 uses the term "tier" – organizational tier, mission / business process tier, system tier. To avoid confusion with Implementation Tiers as defined in the CSF, this paper – like the draft Implementation Guidance for Federal Agencies [NIST 2017] – uses the term "level."

[6] However, the term RMF has been widely interpreted in other ways. Some focus on its primary purpose: as a framework designed to help authorizing officials (AO) make near real-time, risk informed decisions. Others tend to use the term RMF as a shorthand for referring to various documents (e.g., NIST SP 800-53, NIST SP 800-39, NIST SP 800-37, NIST SP 800-30R1, CNSSI 1253, etc.) that support and underlie the broader RMF construct. Still others use the term narrowly to refer to the six step process defined in NIST SP 800-37. Each of these uses is valid; it is the context that matters.

populated when risk assessments are performed, and the populated values are updated as part of risk monitoring.

NIST SP 800-30R1 provides a representative threat model as part of an overall risk assessment methodology. That threat model includes

- A taxonomy of threat sources (Table D-2), with accompanying characteristics for adversarial threats (capability, intent, and targeting) and for non-adversarial threats (range of effects).
- A representative set of adversarial threat events (Table E-2), organized using the structure of a cyber campaign (i.e., a cyber attack lifecycle), and a representative set of non-adversarial threat events (Table E-3).
- A taxonomy of predisposing conditions (i.e., environmental factors which affect the likelihood of threat events occurring or resulting in adverse consequences) (Table F-4). Because vulnerabilities are characterized in a wide variety of ways, NIST SP 800-30R1 does not include a taxonomy of vulnerabilities.

NIST SP 800-30R1 does not prescribe this threat model (nor the risk model of which it is a part). However, NIST SP 800-30R1 states:

> "To facilitate reciprocity of assessment results, organization-specific risk models include, or can be translated into, the risk factors (i.e., threat, vulnerability, impact, likelihood, and predisposing condition) defined in the appendices."

2.1.3 CBEST Intelligence-Led Cyber Threat Modelling

The CBEST approach to threat modeling [BOE 2016] is a subcomponent of a framework for cyber threat intelligence-driven system assessments and testing, published by the Bank of England in 2016. It outlines an analytical model of cyber threat actors in terms of their goals, capabilities used to pursue these goals, and methods and patterns of operation. The model is intended to act as a template for conducting a cyber threat assessment to define a set of realistic and threat-informed test scenarios. The CBEST approach focuses on identification of specific threat actors and their common attack patterns to generate actionable cyber reconnaissance.

Using as much intelligence as is available, analysts using the CBEST approach analyze each specific threat actor's identity and motivations more deeply than in most models, for instance, delving into geopolitical and socio-cultural factors affecting likely behavior. The approach characterizes the threat actor's capability in terms of resources, skill level and sophistication, persistence, indicators of potential access to the target system being assessed, and evidence of risk sensitivity. It models what is known about the threat actor's phases of operation; TTPs; countermeasures against discovery; timing; and coordination of activity. The CBEST approach is intended to enable analysts, given adequate cyber threat intelligence data, to derive a model of threat actors rigorous and precise enough to be predictive of likely threat events. Though this level of threat intelligence may often not be available, the CBEST approach seeks to generate the most realistic threat scenarios possible given the information at hand.

The CBEST approach includes clear guidance on the expected contents of a threat scenario. Key modeling constructs in CBEST include threat entity goal orientation (including identity, motivation, and intention), capabilities, and modus operandi.

2.1.4 COBIT 5 and Risk IT

Control Objectives for Information and Related Technologies (COBIT) is a framework for governance of IT environments with an extensive focus on controls. COBIT Version 5 was released by the Information Systems Audit and Control Association (ISACA) in April 2012 (http://www.isaca.org/cobit). COBIT is based on components of the International Organization for Standardization (ISO) standards, including incorporation of the ISO 38500 model for the corporate governance for IT and an ISO 15504 aligned COBIT Process Capability Assessment Model. Security controls are based on the ISO 27001 series of control objectives [ISO 2013]. This includes assessment considerations aligned with operational practice, implementation guidance, measurement, and risk management.

COBIT is accompanied by the Risk IT framework for managing business risks of IT [ISACA 2009]. Risk IT consists of a risk model together with a process model; processes are defined for the domains of risk governance, risk evaluation, and risk response. The model underlying risk evaluation in Risk IT is not a security risk model, but does identify security risk as a class of risk to be considered. A risk scenario is described in terms of threat type (which includes malicious threats), actor, type of event (i.e., type of impact), asset or resource affected, and time. ISACA offers guidance on developing risk scenarios, including 60 examples covering 20 categories of risk [ISACA 2014]. In addition, the scenario planning approach in Risk IT's risk assessment framework allows for risk consideration beyond an individual organizational or system view.

2.1.5 Topic-Focused Frameworks and Methodologies

As noted in Section 1.1, adversary characteristics and behaviors are key topics in discussions of cyber threats. Some frameworks and methodologies focus on specific topics, rather than representing all characteristics and behaviors. *Characteristic-focused* frameworks include the multi-tier threat model developed by the Defense Science Board (DSB) Task Force on Resilient Military Systems and Cyber Prep. *Behavior-focused* frameworks and methodologies include cyber attack lifecycle or cyber kill chain models, attack tree or attack graph modeling, and insider threat modeling.

2.1.5.1 DSB Six-Tier Threat Hierarchy

The DSB Task Force Report on Resilient Military Systems and the Advanced Cyber Threat [DSB 2013] defines a threat hierarchy, based primarily on potential attackers' capabilities. In that hierarchy, Tiers I and II exploit known vulnerabilities; Tiers III and IV discover new vulnerabilities; and Tiers V and VI create vulnerabilities. Other differentiators include attacker knowledge or expertise, resources, scale of operations, use of proxies, timeframe, and alignment with or sponsorship by criminal, terrorist, or nation-state entities.

The threat hierarchy is used to motivate and structure recommendations for risk management strategies. Risk is represented as a function of threat, vulnerability, and consequence. Threat has the characteristics of intent and capabilities; corresponding strategies are deter and disrupt. Vulnerability has the characteristics of inherent and introduced; corresponding strategies are defend and detect. Consequence has the characteristics of fixable and final, with corresponding strategies of restore and discard.

2.1.5.2 Cyber Prep Adversary Characterization Framework

The MITRE Corporation's Cyber Prep methodology [Bodeau 2017] uses the characteristics of an organization's expected cyber adversaries to motivate recommendations for preparedness against cyber threats. Cyber Prep is specifically oriented to the organizational level of risk management. The Cyber Prep framework defines fourteen aspects of organizational preparedness, in three areas: Governance, Operations, and Architecture & Engineering. Different adversary characteristics motivate different aspects of preparedness. Adversary characteristics include goals, scope or scale of operations, timeframe of operations, persistence, concern for stealth, stages of the cyber attack lifecycle used, cyber effects sought or produced, and capabilities. In addition to the modeling constructs indicated in Figure 7, Cyber Prep identifies a representative set of high-level attack scenarios. Characteristics of an organization – its missions, assets, and role in the larger cyber ecosystem – make different scenarios more or less attractive to adversaries with different characteristics [Sheingold 2017].

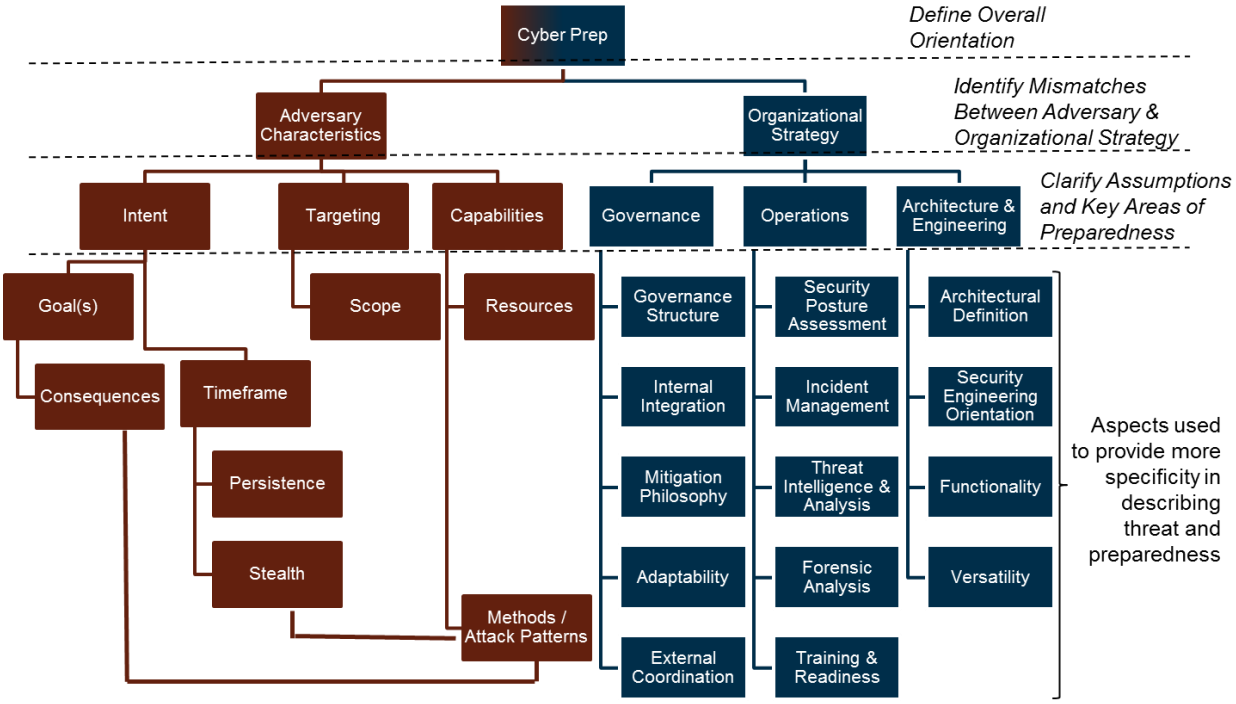

Figure 7. Cyber Prep Framework

The Cyber Prep threat modeling framework builds on the Describing and Analyzing Cyber Strategies (DACS) framework, which can be applied at any scope or scale [Bodeau 2014]. DACS provides additional detail on capabilities, as illustrated in Figure 8. A strategy for developing intelligence about, or having effects on, adversary capabilities could focus on one or more of these attributes.

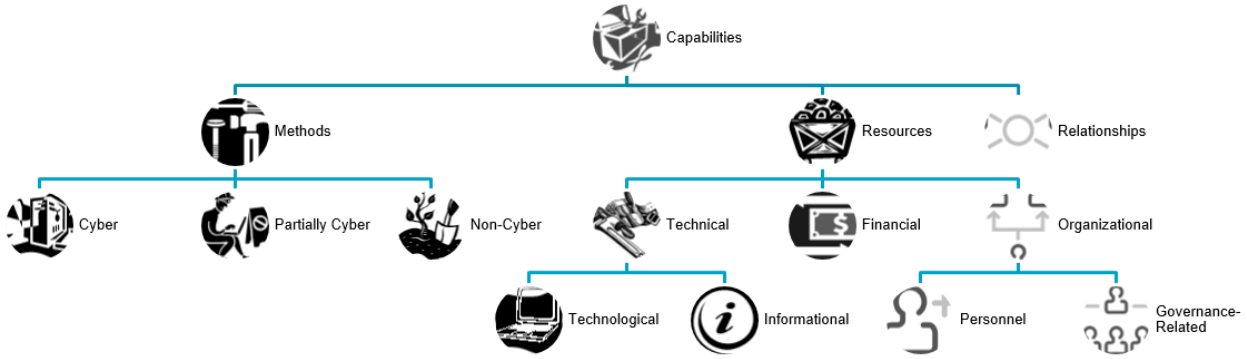

Figure 8. Attributes of Adversary Capabilities

2.1.5.3 Cyber Attack Lifecycle or Cyber Kill Chain Models[7]

The recognition that attacks or intrusions by advanced cyber adversaries against organizations or missions are multistage, and occur over periods of months or years, has led to the development of multistage models which can be used to "bin" or characterize attack events. Such a multistage model is frequently referred to as a "cyber kill chain," adapting military terminology; the phrase "cyber attack lifecycle" is a non-military alternative. An initial cyber kill chain model was developed by Lockheed Martin [Cloppert 2009].

Cyber attack lifecycle models are most commonly defined for external attacks on enterprise IT and command and control (C2) systems. NIST SP 800-30R1 and the 2013 DoD Guidelines for Cybersecurity Developmental Test and Evaluation (DT&E) [DoD 2013] use a seven-phase cyber attack lifecycle model, as illustrated in Figure 9.[8]

Variant attack lifecycles are common. Most focus on exfiltration of sensitive information as the adversary's objective. For example, an Advanced Research and Development Activity (ARDA) Workshop designed a version to characterize activities by insiders [Maybury 2005]: reconnaissance, access, entrenchment, exploitation, communication, manipulation, extraction & exfiltration, and counter intelligence. Raytheon uses a six-phase model: Footprint, Scan, Enumerate, Gain Access, Escalate Privileges, and Pilfer.[9] Dell Secureworks identifies 12 stages: define target, find and organize accomplices, build or acquire tools, research target infrastructure/employees, test for detection, deployment, initial intrusion, outbound connection initiated, expand access and obtain credentials, strengthen foothold, exfiltrate data, and cover tracks and remain undetected [SecureWorks 2016].

Other cyber attack lifecycles, like the one shown in Figure 9, do not specify the adversary's objectives, and thus enable cyber attacks that directly impact organizations and their missions (e.g., via denial of service, via data corruption or falsification) to be represented. Microsoft researchers have identified a set of ten "base types" of actions: reconnaissance, commencement,

[7] This section is adapted and updated from [Bodeau 2013].

[8] Later versions of the DoD Cybersecurity Test and Evaluation Guidebook have used different variants. The current version [DoD 2018] identifies four phases – Prepare, Gain Access, Propagate, and Affect – with two classes of activities (Reconnaissance and C2) applying across all four phases.

[9] The white paper in which this model was first presented is no longer accessible. However, the model is included in Patent US 8516596 B2, "Cyber attack analysis," granted August 20, 2013. See http://www.google.com/patents/US8516596.

entry, foothold, lateral movement, acquire control, acquire target, implement / execute, conceal & maintain, and withdraw [Espenschied 2012]. Mandiant [Mandiant 2013] describes an attack lifecycle consisting of Initial Recon; Initial Compromise; Establish a Foothold; Escalate Privileges, Internal Recon, Move Laterally, and Maintain Presence, which can repeat cyclically; and Complete Mission. The CIS Community Attack Model defines nine stages: Initial Recon, Acquire / Develop Tools, Delivery, Initial Compromise, Misuse / Escalate Privilege, Internal Recon, Lateral Movement, Establish Persistence, and Execute Mission Objectives [CIS 2016]. The National Cyber Security Centre (NCSC) defines a four-stage process: Survey, Delivery, Breach, and Affect [NCSC 2016]; this is similar to the four stages identified in the ODNI Cyber Threat Framework discussed in Section 2.3.4. Payments UK identifies twelve steps: Define target, Find and organize accomplices, Build or acquire tools, Research target infrastructures / employees, Test for detection, Deployment, Initial intrusion, Outbound connection initiated, Expand access and obtain credentials, Strengthen foothold, Exfiltrate data, and Cover tracks and remain undetected [Payments UK 2014].

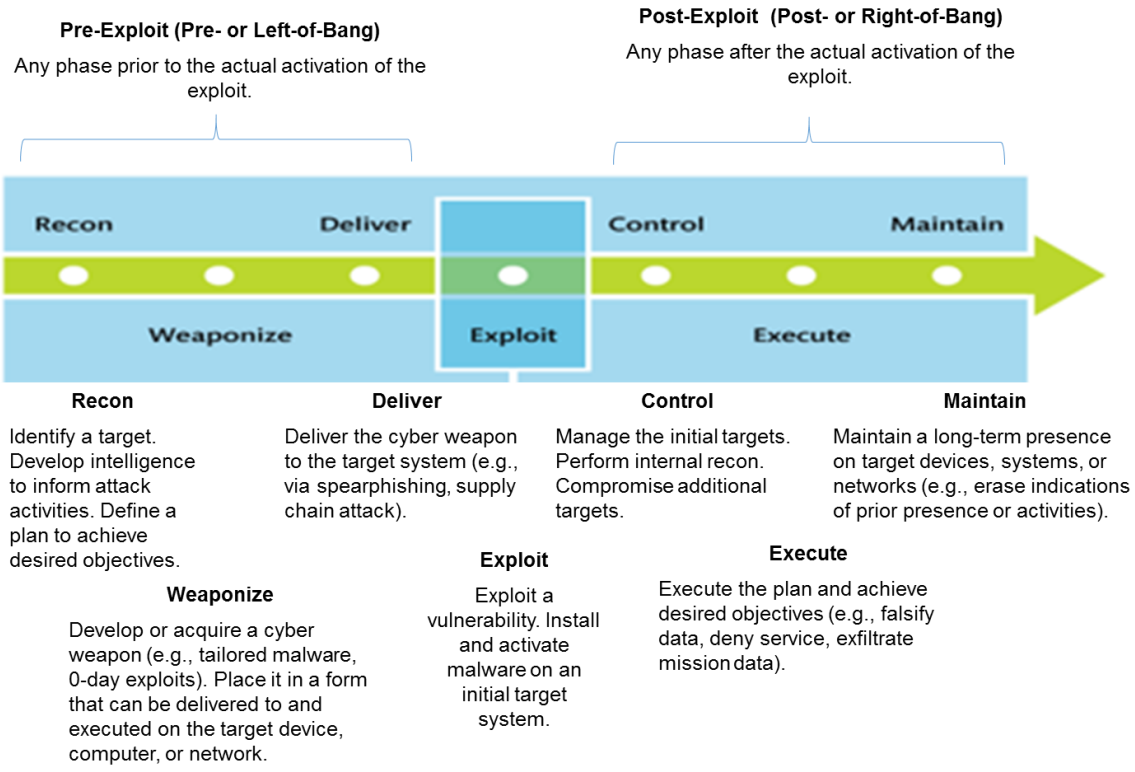

Figure 9. Cyber Attack Lifecycle

The concept of an attack lifecycle or kill chain has been extended to threats beyond those that exploit the exposure of an organization's systems in cyberspace, to insider threats, threats to industrial control systems and other cyber-physical systems, and the supply chain. A four-stage insider threat kill chain – recruitment / tipping point, search / recon, acquisition / collection, and exfiltration / action – was defined by the Federal Bureau of Investigation (FBI) [Reidy 2013] and has been adopted [TripWire 2015] and extended [ZoneFox 2015] more broadly. A version for industrial control systems (ICS) has been defined [Assante 2015], with two stages (Cyber Intrusion Preparation & Execution and ICS Attack Development & Execution), each of which

includes multiple phases. A version for cyber-physical systems (CPS) has been developed [Hahn 2015] which takes into consideration the three layers of a CPS (cyber, control, and physical). The stages are recon (spanning all three layers), weaponize (spanning cyber and control), deliver (cyber), cyber execution (cyber), perturb control (control), and achieve physical objective (physical). The DSB Task Force on Cyber Supply Chain [DSB 2017] has developed a four-phase kill chain: Intelligence & Planning, Design & Create, Insert, and Achieve Effect. A more detailed supply chain attack lifecycle [Shackleford 2015] represents two different attack vectors: physical and virtual.

2.1.5.4 Threat Modeling Using Attack Trees or Attack Graphs

Attack trees or attack graphs are a well-established approach to developing threat scenarios for risk assessment or cyber wargaming. Surveys of models and methodologies using directed acyclic graphs can be found in [Kordy 2014] and in Appendix B.1.2 of [Bodeau 2013]. In addition to the variants described there and other historical variants described in [Beyst 2016], products (e.g., http://threatmodeler.com) or prototype tools from a wide variety of research efforts can be used to generate attack trees or attack graphs. The Mission Oriented Risk and Design Analysis (MORDA) methodology [Buckshaw 2005] describes the use of attack trees, with consideration of adversary preferences, as part of risk assessment. NIST SP 800-30R1 accommodates but does not direct the use of attack trees.

2.1.5.5 Threat Characterization Framework Developed for DRDC

A survey of the state-of-the-art in cyber threat modeling was performed for Defence Research and Development Canada (DRDC) [Magar 2016]. That report (like this one) includes a proposed initial cyber threat modeling framework. That framework is intended to be used to develop a Canadian Armed Forces (CAF) cyber threat model to be demonstrated on the DRDC ARMOUR[10] platform. The framework identifies four key elements: adversary, attack, asset, and effect. Adversary attributes include type, motivation, commitment, and resources. Attack attributes include delivery mechanisms (local access, remote delivery, distributed delivery, or social engineering), tools, automation, and actions. Asset attributes include profile, container (hardware, software, object, or people), and vulnerability. Effect attributes include cyber effects and effects on military activities.

2.1.5.6 Insider Threat Modeling

Insider threat modeling includes models of insider behavior intended to help identify indicators of insider activity [Costa 2016]. Computational M&S is a key analytic approach [Moore 2016]. Insider threat modeling also includes models intended to predict whether and how an insider could become malicious, and to analyze and predict the effects of organizational actions on insider behavior. Such predictive analysis and modeling emphasizes psychosocial factors [Greitzer 2013]. Insider threat modeling via M&S is outside the scope of this survey.

Insider threat modeling overlaps with cyber threat modeling, insofar as insiders act in and on an organization's cyber resources. However, there are areas in which the two forms of modeling are distinct: First, cyber threat modeling considers external threat sources and malicious cyber activities at all layers in a layered architecture; insider threat modeling considers external threat

[10] ARMOUR is not an acronym, but refers to the DRDC Automated Computer Network Defence program.

actors only with respect to their efforts to influence or suborn insiders, and focuses on actions that an individual user can take. Second, insider threat modeling can include purely non-cyber threat scenarios (e.g., theft of physical goods or of information in non-electronic form).

2.2 Threat Modeling to Support Design Analysis and Testing

Several highly structured threat modeling approaches have been developed to be used in the system design and development process, to motivate and support system design decisions. These include the modeling approach in the draft NIST SP 800-154; the Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege (STRIDE) and Damage, Reliability, Exploitability, Affected Users, and Discoverability (DREAD) approaches created by Microsoft; Carnegie Mellon Software Engineering Institute's Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) methodology; and structured approaches used by Intel and Lockheed Martin. In addition, less structured brainstorming approaches are also in use [Steiger 2016, Shull 2016], but are not discussed below.

2.2.1 Draft NIST Special Publication 800-154, Guide to Data-Centric System Threat Modeling

NIST, in 2016, released a draft of a new threat modeling guidance document focused on identifying and prioritizing threats against specific types of data within systems [NIST 2016] in order to inform and assess approaches for securing the data. This guidance document may change, following a review and revision period. NIST SP 800-154 (DRAFT) lays out the following approach.

System boundaries are identified, and each specific type of data to be protected is identified and characterized as to authorized locations, movement between locations in the course of legitimate processing, security objectives to be met for the data, and applications, services, and classes of users authorized to access the data in ways relevant to the security objectives.

For each data type and location, a list of applicable attack vectors is then developed. Alterations of security controls to improve the protection of the data are identified and their effectiveness estimated against each of the attack vectors. Costs of security controls, in terms of resources or effects on functionality, usability, and performance, are also characterized.

The attack vectors for the data types and countermeasures, as characterized, make up the threat model, which is then analyzed as a whole to determine what set of countermeasures can best reduce risk across the data types and attack vectors. Some scoring methods for analysis are suggested but are not specified in detail.

2.2.2 STRIDE

Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege (STRIDE) was developed for internal use at Microsoft [Kohnfelder 1999], as part of their push to produce more secure software. Consequently, it takes a software development perspective on threat. It has subsequently been used widely within the community and embedded into a loose threat modeling methodology [Shostack 2014].

While sometimes referred to as a threat model or threat modeling framework, STRIDE serves primarily as a categorization of general types of threat vectors to be considered, helping analysts

identify a complete threat model, for example using attack tree analysis [Xin 2014]. STRIDE does not directly address level of detail or specific attack methods. It can be applied to software components, enterprise architectures, or particular assets to be protected.

Threat modeling using STRIDE begins by answering the question "what are you building?" with components and trust boundaries, which are used to identify interactions that cross trust boundaries and therefore may pose opportunities for adversaries. Potential adversaries and their objectives are postulated. The attack vector categories of the STRIDE mnemonic are then applied to specific interfaces, functions, data objects, and software techniques that are part of the system or component being protected. Based on the findings, an analyst or software developer might identify bugs that need to be fixed or conclude that there is an attack vector that needs to be mitigated in some other way (which could, for example, involve addition of a separate security component or product, a policy change, or elimination of a feature.)

2.2.3 DREAD

DREAD was also created at Microsoft for use in their software development process to improve the security of their products [Howard 2003]. The acronym stands for Damage, Reliability (of an attack – sometimes rendered as reproducibility), Exploitability, Affected Users, and Discoverability. DREAD provides a scheme by which threat vectors identified using STRIDE or other methodologies are evaluated and prioritized. Scores for each element of the title are determined on a scale of 1 to 10. Each individual threat vector is scored on the five elements and an average taken, which can then be used to compare its severity and likelihood to those of other threat vectors.

DREAD thus goes part of the way beyond threat modeling to risk assessment. However, as part of a software development methodology in a software vendor context, DREAD does not deal directly with the specific risks inherent in any particular enterprise environment and the threats facing it.

Microsoft has since deemed DREAD overly subjective and as of 2010 discontinued its use in their internal software development lifecycle [Howard 2014]; however, it is still circulating in the community and suggested as an element of threat and risk modeling. [Leblanc 2007] discusses some of the criticisms, as well as how it may be useful nonetheless, and suggests modifications to the scoring scheme.

2.2.4 Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE)

Carnegie Mellon Software Engineering Institute's OCTAVE methodology was originally published in September, 1999. It was refined into its current version known as Allegro v1.0, released in June, 2007 [Caralli 2007]. The goal of OCTAVE/Allegro is to produce more robust risk assessment results without the need for extensive risk assessment knowledge by focusing on information assets in the context of how they are used, where they are stored, transported, and processed, and how they are exposed to threats, vulnerabilities, and disruptions.

The approach consists of eight steps. The steps are: develop risk measurement criteria consistent with organizational drivers; profile critical information assets to identify security requirements; identify locations where the asset is stored, transported, or processed; identify areas of concern; identify threats in the context of these areas; identify risks; analyze risks; and select mitigation approaches.

The threat modeling portion of the OCTAVE/Allegro approach consists of identifying areas of concern (representative threats, in the sense of threat sources and the impacts they could have on information assets) and developing threat scenarios, represented visually as threat trees. Four classes of threats are identified, corresponding to the top node of an attack tree: human attackers using technical means, human attackers using physical means, technical problems, and other problems (e.g., natural disasters). Key attributes of a threat in the OCTAVE/Allegro threat modeling approach include actor, asset (what the threat targets or could affect), access or means, motive[11], and outcome (disclosure, modification, destruction, loss, or interruption).

2.2.5 Intel's Threat Agent Risk Assessment (TARA) and Threat Agent Library (TAL)

Intel Corporation published, in December 2009, its Threat Agent Risk Assessment (TARA) methodology [Intel 2009], which is designed to distill possible information security attacks into a digest of only those exposures most likely to occur. Its objective is to identify threat agents that are pursuing objectives which are reasonably attainable and could cause losses. The methodology identifies which threat agents pose the greatest risk, what they want to accomplish, and the likely methods they will employ. These methods are cross-referenced with existing vulnerabilities and controls to pinpoint the areas that are most exposed. The security strategy inherent in TARA then focuses on these areas to minimize efforts while maximizing effect.

Intel also published a library of threat agents [Intel 2007] to serve as a starting point for enterprise development of an organization-specific characterization of threat agents. The site at which the library white paper can be found was updated in 2015. The Threat Agent Library (TAL) defines 22 archetypes, using eight key attributes or parameters: intent, access, outcome, limits, resources, skill, objective, and visibility. Intel subsequently modified its list of key parameters to include motivation [Intel 2015]. In addition, Intel identified 10 elements of the motivation parameter (ideology, coercion, notoriety, personal satisfaction, organizational gain, personal financial gain, disgruntlement, accidental, dominance, and unpredictable), and modified its model so that each agent can have multiple motivations (defining motivation, co-motivation, subordinate motivation, binding motivation, and personal motivation). The concept of multiple motivations has been carried into the definition of the Threat Actor Domain Object in Structured Threat Information eXpression (STIX™) (see Section 2.3.1).

2.2.6 IDDIL/ATC

IDDIL/ATC is a mnemonic: Identify the assets; Define the attack surface; Decompose the system; Identify attack vectors; List threat actors; Analysis & assessment; Triage; Controls. Lockheed Martin's IDDIL/ATC methodology [Muckin 2015] provides a structured process for applying its cyber kill chain model, together with its variant of STRIDE (STRIDE-LM, which adds Lateral Movement), and attack trees. Using IDDIL/ATC, analysts can develop a system threat model, represented graphically. Key modeling constructs include assets, threat actors, and attack vectors. A threat profile (a tabular summary of threats, attacks, and related characteristics) identifies the asset or threat object; threat types (e.g., STRIDE-LM; threats to confidentiality, integrity, and/or availability); the attack surface; attack vectors; threat actors; the resultant

[11] Access or means and motive are relevant only to human actors.

condition; vulnerabilities, and controls. The published materials provide representative examples. Additional detail is included in proprietary tools.

2.3 Threat Modeling to Support Information Sharing and Security Operations

Threat information sharing is integral to many cyber risk management approaches, as discussed in Section 2.1, including the higher Implementation Tiers in the CSF, risk monitoring in the JTF risk management process, and CBEST. Three modeling frameworks focused on threat information sharing are of particular interest to the NGCI Apex Program: STIX, PRE-ATT&CK™, and the OMG Threat / Risk Standards Initiative. In addition, the Cyber Threat Framework (CTF) promulgated by the Office of the Director of National Intelligence (ODNI) provides a way to categorize, characterize, and share information about cyber threat events. This has been elaborated into the National Security Agency (NSA) / Central Security Service (CSS) Cyber Threat Framework.

2.3.1 STIX™

STIX™ (the Structured Threat Information eXpression) is a structured language for capturing and sharing cyber threat information [Barnum 2014]. STIX has been transitioned to the Organization for the Advancement of Structured Information Standards (OASIS).[12] STIX enables information to be shared about cyber threats and about courses of action which can defend against threat activities. In January 2017, the OASIS Cyber Threat Intelligence (CTI) Technical Committee approved a Committee Specification Draft for STIX 2.0 [OASIS 2017]; a specification for STIX 2.1 is in process. Organizations can use STIX and TAXII™ (Trusted Automated eXchange of Indicator Information) to share threat intelligence.

The STIX domain model defines data structures to characterize or describe an adversary and adversary activities. STIX Domain Objects include Threat Actor; Malware; Tools; Attack Pattern (which can reference the Common Attack Pattern Enumeration [CAPEC™], discussed in Section 3.1.2); Campaign (i.e., a grouping of adversarial behaviors, using attack patterns, malware, and/or tools); and Intrusion Set. The Threat Actor object has several optional associated properties, including goals, sophistication, resource level, primary motivation, secondary motivations, and personal motivations. Attack patterns, malware, and tools are all forms of TTPs. Information about adversary reasons for acting and how they organize themselves is described via the threat actor, intrusion set, and campaign domain objects. Other portions of the STIX domain model include observables, indicators, and courses of action. Kill chain phases are an optional property of Attack Pattern, Indicator, Malware, and Tool. STIX does not specify a set of kill chain phases, instead allowing its users to specify which kill chain model they are using.

A white paper by Payments UK recommends STIX and its transport protocol TAXII as formats for Standard Technical Reports Using Modules (STRUM) [Payments UK 2014].

[12] The STIX standards are available at github (https://stixproject.github.io/).

2.3.2 OMG Threat / Risk Standards Initiative

The Object Management Group (OMG) has developed a request for proposal (RFP) for an operational threat and risk model [OMG 2014], which can be used to federate existing risk models or partial models. The conceptual model will have an information exchange format based on the National Information Exchange Model (NIEM) and an explicit mapping to STIX. The Threat and Risk Community created at http://threatrisk.org/drupal/ during the development of the RFP continues to refine the requirements for this model. The RFP defines operational risk as follows:

> "Operational risks are situations having a negative impact on an organization or company due to uncertainties related to possible breakdowns in a system or its environment via supply chain, injury to a person or failure of a process resulting from intentional/malicious as well as unintentional/natural operational threats. One of the main impacts of operational risks is inability to conduct operations as planned."

Cyber risks are a key class of operational risks. The RFP identifies a number of terms related to threat modeling, including threat, threat source, threat actor, undesired event, tactics, techniques, procedures, exploit target, goal, and campaign. The draft expansion provides more details, including taxonomic and attribute relationships. These are expressed in diagram form in slides 60-65 of https://slideplayer.com/slide/9121179/.

Compatibility with STIX is a required feature of any model that meets the RFP.

2.3.3 PRE-ATT&CK™

PRE-ATT&CK™ (Adversarial Tactics, Techniques & Common Knowledge [ATT&CK[13]] for Left-of-Exploit) is an emerging framework for categorizing and characterizing adversary activities in the early stages of the cyber attack lifecycle [MITRE 2016b]. Seventeen categories of high-level tactics are currently defined, primarily covering techniques external to the enterprise. Tactics can be technical, human, or organizational; examples include People Information Gathering, Adversary OPSEC (Operations Security), Persona Development, and Test Capabilities. PRE-ATT&CK can be used by cyber defenders to prioritize cyber threat intelligence data acquisition and analysis.

Pre-exploit adversary activities, such as gathering information from the Internet about potential targets of attack, are largely executed outside of a potential victim's purview, making it significantly more difficult for defenders to detect. However, PRE-ATT&CK could provide a common lexicon to allow cyber defense to understand, detect, mitigate, and share information about adversary activities across the FSS. This could then be used to shift to a more proactive/predictive analytic capability to support elements of attribution and defensive responses.

2.3.4 Cyber Threat Framework

In March 2017, the ODNI published its Cyber Threat Framework (CTF) [ODNI 2017], including use guidance and a lexicon. The CTF was initially constructed to support threat information sharing by providing a common structure for information in published threat reports. However,

[13] ATT&CK is discussed in Section 3.1.1.

its approach to characterizing and categorizing adversary activities also supports analysis, senior-level decision making, and trend and gap analysis. As illustrated in Table 1, the CTF defines four broad stages of adversary actions: Preparation, Engagement, Presence, and Effect / Consequence. Actions in each stage have defined objectives. Each action has one or more Indicators. Objectives and representative examples of actions are included in the published lexicon. Other terms used in CTF materials include threat actor and threat actor resources.

Table 1. ODNI Cyber Threat Framework

Layer	External Actions		Internal Actions	
1: Stages	Preparation	Engagement	Presence	Effect / Consequence
2: Objectives	Plan activity Conduct research & analysis *Develop resources & capabilities* Acquire victim-specific knowledge Complete preparations	Deploy capability *Interact with intended victim* Exploit vulnerabilities Deliver malicious capability	Establish controlled access Hide *Expand presence* Refine focus of activity Establish persistence	*Enable other operations* Deny access Extract data Alter data and/or computer, network, or system behavior Destroy hardware / software / data
3: Actions (examples of *italicized* objectives)	Dedicate resources Create capabilities Establish partnerships	Persuade people to act on the threat actor's behalf (e.g., conduct social engineering)	Increase user privileges Move laterally	Establish command and control node Add victim system capabilities to botnet
4: Indicators	[to be populated by analytic users]			

Stages in the CAL described in Figure 9 correspond either to objectives or to stages in the CTF. Recon corresponds to Conduct research & analysis and Acquire victim-specific knowledge. Deliver corresponds to Engagement. Control corresponds to Presence. Execute corresponds to Deny access, Extract data, Alter data, and Destroy hardware / software / data. Maintain corresponds to Enable other operations. Categories in PRE-ATT&CK correspond either to objectives or to action in the CTF.

In March 2018, the National Security Agency published version 1 of the NSA/CSS Technical Cyber Threat Framework [NSA 2018]. This report is intended to provide "a baseline of standard definitions to be used as a reference for U.S. government collaboration with partners and stakeholders in discussing adversary activities throughout the adversary lifecycle." The NSA/CSS CTF integrates the ODNI CTF with ATT&CK. It defines five stages (administer, engagement, presence, effect, and ongoing presence), objectives for each stage, and multiple actions related to each objective. More than 200 actions are described.

3 Specific Threat Models

This section describes several specific threat models, populated with representations of adversary tactics, techniques, and procedures (TTPs). Section 3.1 deals with those that are focused purely on the specific technical patterns that adversaries might employ, while Section 3.2 describes those that explicitly incorporate a model of the enterprise or system against which adversary TTPs may be applied.

Threat models may be developed via one of the modeling frameworks described in Section 2, but often are not. The threat models in this section, indeed, are shaped according to their varying purposes and do not instantiate the methodologies from Section 2. Some are enterprise-oriented, while others instead describe the techniques threat actors may employ against a technological environment in general. For enterprises, while the guidance in NIST SP 800-30R1 is frequently referred to and provides useful threat information in its extensive appendices, organizations often follow hybrid or internally developed approaches suited to their particular organizational processes and modeling goals.

3.1 Enterprise-Neutral, Technology-Focused

Enterprise-neutral, technology-focused threat models are models of adversary capabilities and attack techniques within a general technological environment. These models do not incorporate information about a specific enterprise, its network and system architecture, data assets, or goals that a threat actor might undertake against that enterprise in particular.

3.1.1 Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK™)

Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK™, [MITRE 2015]) is a framework for describing the actions an adversary may take while operating within an enterprise network. It provides a detailed characterization of adversary behavior post-access, i.e., after initially gaining entry via a successful exploit. ATT&CK has been populated for adversaries operating in a Microsoft Windows environment; future expansion for additional operating system environments is planned. ATT&CK is intended to assist in prioritizing network defense by detailing the post-initial access (post exploit and implant) TTPs that advanced persistent threat (APT) actors use to execute their objectives while operating inside a network.

The ten tactics categories for ATT&CK, listed in Table 2, were derived from the later stages (control, maintain, and execute) of the seven-stage Cyber Attack Lifecycle [MITRE 2012] or the Cyber Kill Chain [Hutchens 2010]. Each category contains a listing of techniques that an adversary could use to perform that tactic, including technical description, indicators, useful defensive sensor data, detection analytics, and potential mitigations. Some techniques can be used for different purposes and therefore appear in more than one category.

ATT&CK continues to be populated and updated as new techniques are reported. As noted in Section 2.3.4, portions of the NSA/CSS CTF were derived from ATT&CK.

Table 2. ATT&CK Categories of Tactics

Tactic	Number	Description
Persistence	51	Any access, action, or configuration change to a system that gives an adversary a persistent presence on that system Examples: Bootkit, Hypervisor
Privilege Escalation	27	The result of actions that allow an adversary to obtain a higher level of permissions on a system or network Examples: DLL injection, Web shell
Defense Evasion	34	Techniques an adversary may use to evade detection or avoid other defenses Examples: Binary padding, File deletion
Credential Access	18	Techniques resulting in access to or control over system, domain, or service credentials that are used within an enterprise environment Examples: Credential dumping, Input capture
Discovery	17	Techniques that allow the adversary to gain knowledge about the system and internal network Examples: Network service scanning, Query registry
Lateral Movement	17	Techniques that enable an adversary to access and control remote systems on a network and could, but do not necessarily, include execution of tools on remote systems Examples: Pass the hash, Windows Remote Management (WinRM)
Execution	25	Techniques that result in execution of adversary-controlled code on a local or remote system Examples: PowerShell, Windows Management Instrumentation (WMI)
Collection	13	Techniques used to identify and gather information, such as sensitive files, from a target network prior to exfiltration Examples: Audio capture, Clipboard data
Exfiltration	9	Techniques and attributes that result or aid in the adversary removing files and information from a target network Examples: Data encrypted, Scheduled transfer
Command and Control	19	Represents how adversaries communicate with systems under their control within a target network Examples: Data encoding, Uncommonly used port

3.1.2 Common Attack Pattern Enumeration and Classification (CAPEC™)

The Common Attack Pattern Enumeration and Classification (CAPEC™) effort provides a publicly available catalog of attack patterns along with a comprehensive schema and classification taxonomy (https://capec.mitre.org). Attack patterns are "descriptions of the common elements and techniques used in attacks against vulnerable cyber-enabled capabilities." Each pattern defines a challenge that an attacker may face, provides a description of the common technique(s) used to meet the challenge, and presents recommended methods for mitigating an actual attack. Attack patterns help categorize attacks in a meaningful way in an effort to provide a coherent way of teaching designers and developers how their systems may be attacked and how they can effectively defend them. Figure 10 illustrates the attack pattern elements in CAPEC.

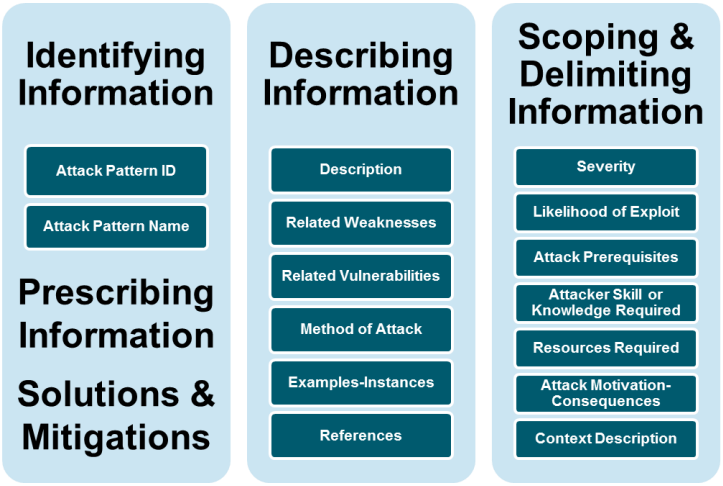

Figure 10. CAPEC™ Model

3.1.3 Web Application Threat Models

The Web Application Security Consortium (WASC) developed a classification of weaknesses in and threats against web applications [WASC 2010]. Its 34 classes of attacks include, for example, buffer overflow, cross-site scripting, and denial of service Classes of weaknesses include improper input handling and abuse of functionality. While the WASC classification effort is dormant, these classes are used in the Open Web Application Security Project (OWASP) WASC Web Hacking Incidents Database, which continues to be updated.[14] OWASP identified 12 categories of web application attacks, which distill the WASC attack classes.[15] The OWASP effort is reflected in the Process for Attack Simulation & Threat Analysis (PASTA) threat modeling methodology [UcedaVelez 2015].

In November 2016, OWASP published an ontology of automated threats against web applications [OWASP 2016]. The OWASP Automated Threat Handbook currently describes 20 threat events. For each threat event, the following information is included: sectors targeted (e.g., financial, health), parties affected, data commonly misused, related threat events, description, other names and examples, CAPEC category, WASC threat identifiers, Common Weakness Enumeration (CWE) identifiers, OWASP attack category, possible symptoms, and suggested countermeasures. OWASP is currently working on its planned Top 10 publication, describing the ten most significant classes of application vulnerabilities [OWASP 2017]. In that publication, the description of each vulnerability includes two threat modeling constructs: threat agents (the types of threat actors which could exploit the vulnerability) and attack vectors (descriptions of how the vulnerability could be exploited – in effect, descriptions of either threat events or fragments of threat scenarios).

3.1.4 Invincea Threat Modeling

Invincea has developed an approach to modeling threats to enterprise IT which enables adversary playbooks to be developed [Invincea 2015]. This approach is complemented by the development

[14] See https://www.owasp.org/index.php/OWASP_WASC_Web_Hacking_Incidents_Database_Project.

[15] See https://www.owasp.org/index.php/Category:Attack.

of defender playbooks in which cybersecurity products are mapped to CSF functions. The two playbooks can then be used to run a notional game, and to identify gaps in the defender's playbook. Key threat modeling constructs are adversary type, target organization type, campaign objective, campaign vehicle, campaign weapon (e.g., Adobe Flash exploit), payload delivery, and payload capabilities; a set of values is defined for each construct.

3.1.5 Other Taxonomies and Attack Pattern Catalogs

Several attack taxonomies are cited in the DRDC [Magar 2016] and Payments UK [Payments UK 2014] white papers, notably AVOIDIT (Attack Vector, Operational Impact, Defense, Information Impact, and Target, [Simmons 2014]) and a proposed cyber conflict taxonomy [Applegate 2013]. Those two papers also survey previous attack taxonomies. AVOIDIT defines six key constructs: attack vector (e.g., design flaw), operational impact (e.g., misuse of resources), defense (mitigation or remediation), informational impact (distort, disrupt, destroy, disclose, and discover), and target (e.g., operating system, network, user, application). Attacks are classified using a cause, action, defense, analysis, and target (CADAT) process. The proposed cyber conflict taxonomy defines two categories (action and actor) and two types of subjects (entity and event). Two types of action are defined: defense and intrusion. An intrusion has four attributes: vector, operational impact, systems impact, and informational impact. Representative values are defined for each of the attributes.

ENISA (the European Union Agency for Network and Information Security) has published an initial taxonomy of cyber threats – i.e., "threats applying to assets related to information and communication technology" [ENISA 2016]. That taxonomy identifies non-adversarial as well as adversarial threats; threat classes are legal, nefarious activity / abuse, eavesdropping / interception / hijacking, outages, failures / malfunctions, damage / loss (IT assets), disasters, accidents, and physical attacks. An open threat taxonomy published by Enclave Security defines and provides an initial set of entries in four categories: physical threats (14 entries), resource threats (13), personnel threats (7), and technical threats (41) [Tarala 2015]. A taxonomy of semantic attacks – i.e., manipulations of user-computer interfaces intended to breach a system's security by deceiving the user – provides examples of 30 types of attacks [Heartfield 2015]. The top level of the taxonomy uses a three-phase attack lifecycle (orchestration, exploitation, and execution). A survey of definitions together with analysis of ten high-profile cyber attacks identified 11 attributes: Actors, Assets targeted, Motivation, Effect on targeted assets, Duration, Attack vector, Vulnerability, Malicious software, Botnet reliance, Origin, and Destination (or region affected) [Kadivar 2014].

Additional attack catalogs have been developed for supply chain threats and for attacks against cyber-physical systems. A catalog of 41 supply chain attack patterns was developed from CAPEC, TARA (see Section 3.2.1), and NIST SP 800-30R1 [Miller 2013] [Reed 2014]. Characteristics of attack patterns include the attack point (organization or physical location in the supply chain), attack act, attack vector, attack type (what is inserted or modified, e.g., hardware, software), attack goal (e.g., disruption, corruption, disclosure, destruction), and attack impact.

NIST, under the auspices of the Cyber-Physical Systems Public Working Group (CPS PWG), has assembled an initial catalog of threats (i.e., attack patterns or threat events) against mobile information systems [NIST 2016b]. Categories of attack patterns include application, authentication, cellular, ecosystem, enterprise mobility management, Global Positioning System (GPS), local area network and personal area network, payment, physical access, stack, and

supply chain. A version of ATT&CK for mobile devices, building on the NIST Mobile Threats Catalog, has been developed [MITRE 2017].

3.1.6 Threat Modeling for Cloud Computing

For cloud computing, one way of categorizing attacks is: data breach and data loss, evading provenance, malicious service attacks, malicious administrator attacks, virtual machine (VM) threats, and network threats [Kazim 2016]. In addition, several "man-in-the-cloud" attacks have been identified [Imperva 2015]. A variety of modeling approaches are discussed in [Amini 2015], which cites prior work by [Fernandez 2014]. These two references cite work by the Cloud Security Alliance [CSA 2013]. However, no set of attacks or modeling approach has emerged as a consensus.

Cloud computing relies on, but is not identical to, virtualization, since VMs can be used in non-cloud architectures. A threat model related to virtual desktop environments for financial services is presented by Dell in [Lewis 2012]. Examples of attacks include data leakage and data tampering at rest. Surveys of cloud and virtualization threat models highlight colocation DoS attacks, colocation breach of confidentiality attacks, attacks on data availability and integrity, attacks on data confidentiality, and infrastructure compromises [Booth 2013][McCall 2014]. A recent survey also identifies a variety of attacks, threat models, and solutions for virtualization as well as cloud computing [Sgandurra 2016]. Categories of attacks include attacks on applications or OSs, VM escape, attacks from the hypervisor, attacks on the hypervisor, and lower-level attacks.

3.2 Enterprise-Oriented, Technology-Focused

Enterprise-oriented, technology-focused threat models or methodologies incorporate information about the specific enterprise for which a cyber threat assessment is being done. Specific threat models for particular enterprises are typically not shared broadly, as they encapsulate sensitive information about the ways in which the enterprise could be attacked. The first two models included here are thus somewhat generic. The first is really a modeling methodology and toolset; however, it is populated with adversary TTP information that is filtered for applicability to a particular enterprise or network's architecture and data flows. The second is a model that represents a financial services sector-specific view of cyber threats within the context of a notional financial institution. The third model demonstrates how ATT&CK and other approaches can be pulled together into a single enterprise-specific approach for the DoD enterprise.

3.2.1 MITRE's Threat Assessment and Remediation Analysis (TARA)

Threat Assessment and Remediation Analysis (TARA) is a methodology developed by The MITRE Corporation for identifying threats to a system and determining appropriate countermeasures [Wynn 2011, Wynn 2014]. It is designed to work in tandem with a related methodology known as Crown Jewels Analysis. Cyber Threat Susceptibility Analysis, a component of TARA, deals with the identification and ranking of potential cyber attack events or patterns that could be mounted by sophisticated adversaries.

Cyber Threat Susceptibility Analysis constructs and uses a threat catalog, which can draw from many sources, such as CAPEC (http://capec.mitre.org/), the Common Weakness Enumeration (CWE, https://cwe.mitre.org/), Common Vulnerabilities and Exposures (CVE,

https://cve.mitre.org/), NIST publications, reported details of security incidents, and other published security research. The key modeling construct is an *attack vector* – a sequence of steps performed by an adversary in the course of conducting a cyber attack [Wynn 2017]. A TARA catalog consists of vector groups (named collections of attack vectors), organized in a taxonomy. TARA also includes tools for matching a specified system environment and its technologies to attack vectors in the catalog and for scoring the resulting list of applicable attack vectors.

A threat analysis of a particular system or environment begins by establishing its scope, architecture, and technology components, as well as the types of adversaries and range of attack techniques to be considered. (For instance, attacks on the supply chain might be considered within scope or excluded.) Security perimeters, interfaces, and flows are examined to characterize the attack surface.

Candidate attack vectors applicable to system components within that scope are then identified from the catalog. Implausible attack vectors are eliminated through a narrowing process, which might observe preconditions that are not met or configurations that can be assumed based on a system's prior conformance to specified hardening requirements. The remaining attack vectors are ranked via a scoring model that considers a variety of factors such as proximity, skills, and resources required for an attacker to carry out the attack vector, locality of its effects, stealth of the attack vector, and time to recover. A threat matrix is constructed from the attack vectors and their scores; a simple example, taken from [Wynn 2017], is illustrated in Figure 11.

Attack Vectors		Risk Score	Shopping cart			
AV ID	AV Name		Browser	Database	Web Server	Email App
T000049	Buffer Overflow	High	X	X	X	X
T000014	Accessing, Intercepting, and Modifying HTTP Cookies	Moderate	X			X
T000050	Forced Integer Overflow	Moderate		X		
T000071	SOAP Array Overflow	Moderate			X	
T000052	Inducing buffer overflow to disable input validation	Low		X		X
T000170	Attack through shared data	Low	X		X	

Figure 11. Example TARA Threat Matrix

3.2.2 NIPRNet/SIPRNet Cyber Security Architecture Review (NSCSAR)

NSCSAR is a Department of Defense (DoD) program to continually evolve and further strengthen the cybersecurity architectures of the NIPRNet and SIPRNet, which are the DoD's Unclassified and Secret-level Internet Protocol (IP) networks, respectively [Dinsmore 2016]. As part of NSCSAR, a threat model and risk framework to assess and prioritize new cybersecurity capabilities have been developed and populated. The contents of the threat model include information from both classified and unclassified sources, and thus cannot be shared. However, the structure of the model illustrates an alternative or complement to the CART's Cyber Defense Matrix and other such matrices, as described in Section 1.2.3. The threat model uses a four-phase cyber attack lifecycle: pre-event, get in, stay in, and act. Tactics and techniques are mapped to these phases, drawing from the ATT&CK model [MITRE 2015] as well as other threat models. The threat framework expands beyond ATT&CK by including both preparatory (pre-event) and attack effects phases in addition to post-exploit TTPs.

The main architectural elements of the network are characterized within a cybersecurity reference architecture, and significant traffic flow paths identified. The cybersecurity capabilities

associated with each of these are then evaluated against the threat techniques in the threat model. The results of the analysis enable identification of areas for improvement, to support technology foraging.

DHS is building on NSCSAR to define the .Gov Cybersecurity Architecture Review (.GovCAR) [Naegele 2018].

3.2.3 Notional Threat Model for a Large Financial Institution

Figure 12 depicts, in mind map format, a threat model representing threats against a hypothetical or representative large financial institution [Fox 2016]. Its objective is to support an observed threat model mapped to deployed mitigations (products and process) to assess residual risk levels as described in NIST SP 800-30 and the FFIEC Information Security Handbook. This model was developed by beginning with an open source browser attack tree [Franz 2005] and evolving and extending it to focus on the enterprise infrastructure of a financial institution. Significantly, it states the objectives of threats in terms of their effect on business-specific functions, rather than in a generic technology-oriented context.

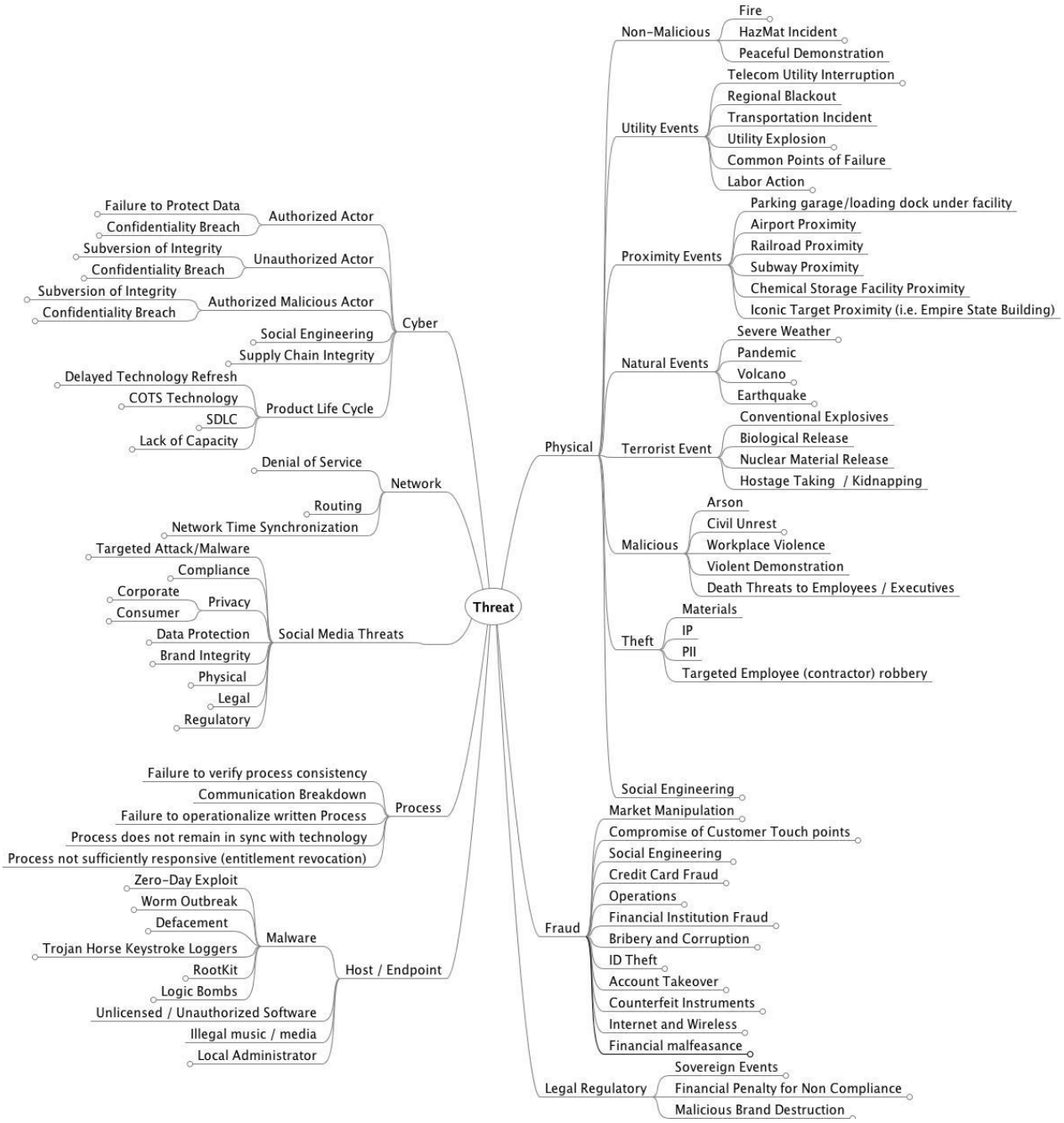

Figure 12. Large Financial Institution Notional Threat Model

4 Analysis and Assessment

This section presents analysis and assessment of the results of the literature survey presented in Sections 2 and 3. In Section 4.1, the models and frameworks are characterized by a structured set of attributes for descriptive purposes and comparison. Attributes both of models in general and of models for the cyber threat modeling domain are identified. The threat models and frameworks described in Sections 2 and 3 are then characterized in light of these attributes.

Section 4.2 describes how models and frameworks with different attributes interrelate and can be combined to represent and share information about the threat environment more comprehensively. In Section 4.3, the models and frameworks are assessed for use within the NGCI Apex program. While this assessment is specific to NGCI Apex, the assessment criteria and the summary assessment are expected to be more broadly useful.

4.1 Characterizing Threat Models

To help clarify the roles and scope of the different threat frameworks and models, it is useful to characterize them in a more structured way. A variety of dimensions can be considered when characterizing models in general, and threat models in particular. Section 4.1.1 reviews characteristics for general comparison of models. Section 4.1.2 considers characteristics of threat models specifically, in relation to how they can be applied to support the NGCI Apex goals. Based on these, several key aspects of cyber threat models relevant to NGCI Apex are identified. The models, frameworks, and methodologies described in Sections 2 and 3 are then characterized in terms of these aspects in Section 4.1.3.

4.1.1 Characterizing Models in General

As the financial sector has come to rely on models to support decision-making, the need to manage the risks associated with such models has increasingly been recognized. OCC guidance on model risk management (MRM) – i.e., the risk associated with depending on a model – provides representative examples of different attributes of model quality: *precision, accuracy, discriminatory power, robustness, stability, and reliability* [OCC 2011]. To provide more structure for understanding these characteristics, MRM frameworks have been defined. The factors or dimensions identified in the OCC guidance and in those frameworks can be used to inform the characterization and assessment of cyber risk and cyber threat models. Two representative MRM frameworks are described, to highlight representative factors or characteristics which can be used to assess or characterize cyber threat models.

PricewaterhouseCoopers (PwC) defines four categories of models: simple factor, complex single scenario, constrained multi-scenario, and unconstrained enterprise-specific [PwC 2015]. PwC identifies seven attributes which can be compared across these categories: *accuracy* (how well does the model reflect reality), *conservatism* (how easily can conservatism be built into the model), *scope* (how many values need to be considered when evaluating the model), *buffer* (how much of a buffer must be included in model-supported decisions in order to manage model risk), *longevity* (how long can a model survive, given changes in the domain it represents), *gaming* (how easy is it to "game" the model to get specific results), and *comparability* (how easy is it to compare model results across different enterprises).

Management Solutions indicates three sources of model risk: data deficiencies in terms of both availability and quality, estimation uncertainty or model error, and model misuse [Management Solutions 2014]. Management Solutions identifies three factors that can be used to categorize model risk: *materiality* (severity of the consequences of misuse of or error in the model), sophistication or *complexity*, and *impact on decisions* (specifically including the scope of the decisions to be informed by the model – department, institution, or external). Based on these factors, models can be characterized as high, medium, or low risk.

The model risk perspective can be applied to cyber risk models and to cyber threat models. A cyber risk model enables an organization, sector, or Federal Department or Agency to identify, prioritize, and compare the relative effectiveness of alternative mitigations on cyber risks. Model risks relate primarily to (1) ignoring or failing to represent classes of risks, (2) underestimating classes of cyber risks, or (3) overestimating classes of cyber risks. These model risks result in increased risk exposure or misallocation of resources. A cyber threat model enables an organization, sector, or Federal Department or Agency to identify, prioritize, share information about, and define courses of action specific to classes of cyber threat actors, events, or scenarios. Model risks relate primarily to (1) failing to identify classes of threats, (2) mischaracterizing or underestimating likelihoods associated with classes of threats, or (3) overestimating likelihoods associated with classes of risks. These model risks result in failures to share threat intelligence (or to make effective use of it), and contribute to the model risks for cyber risk models.

The attributes of model quality defined in the context of MRM inform the criteria used to characterize and assess cyber threat models as described in Sections 4.1.2 and 4.3.1. For example, precision and accuracy inform specification. Comparability informs scalability.

4.1.2 Characteristics of Cyber Threat Models

Eleven characteristics of cyber threat models, frameworks, and methodologies were developed by taking into consideration the factors identified for characterizing models in general, together with the goals of the NGCI Apex program and the role of this Cyber Threat Modeling Survey and Assessment. The first three relate to the applicability of the models: In what settings could they be used? The next five relate to the structure of the models: What is included, at what level of detail? The final three capture considerations for potential organizational use of the models. These characteristics are defined in Table 3; values that will be used to characterize the surveyed frameworks and models are indicated in **bold**.

Table 3. Characteristics of Threat Models and Frameworks

Characteristic	Discussion
Tier(s) or level(s) of risk management addressed	As discussed in Sections 1.2.1 and 2.1.1, cybersecurity risk can be managed at the **national** or transnational tier, the **sector** or community-of-interest tier, the **organizational** tier (or executive level), the **mission/business function** tier (or business/process level), and the **system** tier (also referred to as the implementation/operations level).
Sector or business environment addressed	Some threat models and frameworks are oriented toward a **specific critical infrastructure sector** or business sector. Others are **sector-neutral**. Still others are oriented toward identifying threats and managing risks in the context of a **specific activity** or process, such as software development.

Characteristic	Discussion
Technology environment addressed	Some threat models or frameworks assume a **specific technical environment** (e.g., enterprise IT, software in development, Windows). Others are **technology-neutral**. Note, however, that to the extent that a threat model includes all or portions of a cyber attack lifecycle, it is likely to be oriented toward enterprise IT.
Threat domain coverage	This characteristic has several aspects, including the portion of the attack lifecycle addressed, as well as whether insider threats, supply chain attacks, and non-cyber attacks are considered. Some threat models or frameworks **explicitly** define stages in a cyber attack lifecycle; others **implicitly** refer or apply to specific stages; while still others make **no reference** to a cyber attack lifecycle model. While insider threat behaviors can be represented using a cyber attack lifecycle model, some modeling constructs specific to **insider** threats can be explicitly included. Some threat models applicable to systems focus on an **existing**, as-used system (in the O&M stage), others on a system in **development**, and others to **multiple** stages in the SDLC. Finally, some threat models consider **supply chain** attacks, and some consider **non-cyber** or hybrid attacks.
Key terms defined	As noted in Section 1, a number of terms related to cyber threats are in common use. Some threat models define many of these terms; others use terms without definition. The terms a model defines or uses determine, implicitly or explicitly, how much of the cyber threat modeling domain it covers. (Note that some of the surveyed threat models and frameworks are part of risk models; only the terms related to threat are identified in Section 4.2.2).
Level of detail or granularity	Some threat models or frameworks define only a few key terms or attributes, emphasizing expository value over support for analysis (**Low** level of detail). In practical use, such models are intended to be extensible, with additional terms, concepts, relationships, and algorithms to be defined when used. Others define more modeling constructs (typically supported by representative values), but favor extensibility over completeness (**Medium** level of detail, with or without explicit support for extensibility). Such models emphasize longevity and robustness. Still others define many terms and values, organizing them in a many-layered taxonomy or ontology, emphasizing precision, accuracy, and discriminatory power (**High** level of detail, frequently not extensible). For some frameworks or modeling approaches, the level of detail depends on how the framework or approach is used; these are denoted with **D**.
Complexity	Some threat models or frameworks represent relationships among key terms and concepts in general terms (**Low** complexity). Others (typically those with medium-to-high levels of detail) define or describe dependency and functional relationships among the key terms and concepts, and offer general algorithms for combining values, often in table form (**Medium** complexity). Still others (typically those with a high level of detail) define many dependency and functional relationships and specify computational algorithms in detail (**High** complexity). Use of highly complex models generally relies on modeling and simulation (M&S) tools.

Characteristic	Discussion
Rigor	The extent to which a model is rigorous or well-founded depends on such factors as how well-defined its terms are, how clearly and completely the relationships among its terms are specified, and how completely it specifies the computational algorithms it uses and the possible values for its terms. For purposes of characterizing models, three values can be used: **Low** (vague and incomplete; intended primarily for expository purposes); **Medium** (defined and partially specified; intended for qualitative analysis); and **High** (well-defined, specified clearly and – in the view of subject matter experts – completely with respect to the domain it is intended to address; intended for quantitative analysis).[16]
Degree of population	A threat modeling framework can be **unpopulated**, i.e., key terms are defined but no representative values are given. Most threat modeling frameworks are populated with **representative** values for attributes, or with representative examples. Some threat modeling frameworks are **heavily** populated with values, so that users of the model only need to select values.
Degree of adoption	Some threat models, frameworks, or modeling approaches fill a **niche**, and are adopted only by a small user base. Some are used as points of **reference**. Others are **widely used**, and have an "installed base" of analysts with expertise and published worked examples or lessons learned.
Compatibility with other frameworks or standards	Some threat models are **highly** compatible with the de facto standards offered by STIX and NIST SP 800-30, using the same terms and relationships while adding further detail. Others are **moderately** compatible: they can be used with one or more of the de facto standards, but can also be used stand-alone. Still others have **low** compatibility: they were designed to be used stand-alone.

A twelfth characteristic could be defined: dependence on analyst quality. This determines the extent to which the results of using a threat model are reliably reproducible. In general, dependence on analyst quality is determined by such factors as rigor, complexity, and population, and relates to the uncertainty inherent in the assignment of values. Given the way that adversary TTPs and goals change over time, uncertainty is inherent in the cyber threat domain. All the models surveyed have a high degree of dependence on analyst quality.

4.1.3 Cyber Threat Frameworks, Methodologies, and General Models

Table 4 summarizes how these characteristics apply to the threat frameworks and models surveyed in Sections 2 and 3. One observation can be made immediately: Except for the DSB 6-tier threat hierarchy and DACS, none of the surveyed threat models is intended for use beyond a single organization. Threats are assumed to target an organization, its assets, or its missions or business functions, rather than a sector. Some models accommodate representation of threats to missions or business functions, which conceptually can transcend or span organizations. However, application of such models at the sector level entails tailoring and extension.

[16] Rigor can also be an attribute of the process or methodology that uses a model, such as threat modeling, risk assessment, or red teaming. When applied to processes, rigor (together with level of detail) is a key attribute of depth of analysis or assessment. In NIST SP 800-53A [NIST 2014b], representative values given for depth of analysis are basic, focused, and comprehensive.

Table 4. Profiles of Surveyed Threat Models and Frameworks

Model or Framework	Characteristics		
NIST SP 800-30R1	***Applicability*:**	***Intended Use:* Risk assessment**	
	Scope: Organization, Mission, System	**Business Environment:** Neutral, but created for Federal organizations under Joint Transformation Initiative	**Technical Environment:** Neutral
	***Structure*:**		
	Threat Domain Coverage: Representative examples of threat events for seven stages in cyber attack lifecycle. Identifies insider threats, supply chain attacks, non-cyber attacks as of concern. Applies to multiple SDLC stages.	**Key Terms:** Threat source; adversary capabilities, intent, and targeting; threat event, threat scenario, and cyber campaign	
	Level of Detail / Granularity: M; extensible. Explicitly accommodates attack trees as additional level of detail.	**Complexity:** M	**Rigor:** M
	***Usage Considerations*:**		
	Population: Representative values	**Adoption:** H within and beyond Federal organizations	**Compatibility:** H (de facto standard)
CBEST	***Applicability*:**	***Intended Use:* Penetration testing**	
	Scope: Organization, Mission, System	**Business Environment:** Neutral, but created for financial sector in UK	**Technical Environment:** Neutral
	***Structure*:**		
	Threat Domain Coverage: Defines six stages in cyber attack lifecycle. Identifies insider threats, supply chain attacks as of concern. Applies to multiple SDLC stages.	**Key Terms:** Threat entity goal orientation (including identity, motivation, and intention), capabilities, and modus operandi	
	Level of Detail / Granularity: H	**Complexity:** M	**Rigor:** M
	***Usage Considerations*:**		
	Population: Representative values	**Adoption:** H within financial sector in UK	**Compatibility:** H (NIST SP 800-30, reference list of 50+ sources)
	***Applicability*:**	***Intended Use:* Risk assessment**	

Model or Framework	Characteristics		
COBIT and Risk IT	**Scope:** Organization, Mission, System	**Business Environment:** Neutral	**Technical Environment:** Neutral
	***Structure*:**		
	Threat Domain Coverage: No mention of cyber attack lifecycle. Risk IT process can be used to analyze insider threats, supply chain attacks, and non-cyber, across the SDLC.	**Key Terms:** Threat actor, threat target, threat vector, affected asset or resource, time, risk scenario	
	Level of Detail / Granularity: L	**Complexity:** L	**Rigor:** L
	***Usage Considerations*:**		
	Population: A few examples in open publications; 60 representative scenarios in commercial report	**Adoption:** M	**Compatibility:** M (NIST SP 800-30)
DSB Six-Tier Threat Hierarchy	***Applicability*:**	***Intended Use:* Risk framing**	
	Scope: Sector, Organization, Mission, System	**Business Environment:** Military	**Technical Environment:** Neutral
	***Structure*:**		
	Threat Domain Coverage: Does not use cyber attack lifecycle. Insider and supply chain threats considered at higher tiers.	**Key Terms:** Cyber threat, threat actor, sophistication, scale of operation, timeframe	
	Level of Detail / Granularity: L	**Complexity:** L	**Rigor:** L
	***Usage Considerations*:**		
	Population: L	**Adoption:** M (frequently cited, not solely for military)	**Compatibility:** H (NIST SP 800-30)
Cyber Prep (CP) and DACS	***Applicability*:**	***Intended Use:* Risk framing**	
	Scope: Organization (all scopes for DACS)	**Business Environment:** Neutral	**Technical Environment:** Neutral
	***Structure*:**		
	Threat Domain Coverage: Uses cyber attack lifecycle phases to characterize adversary. Does not use insider or supply chain attack lifecycles.	**Key Terms:** Goals, scope or scale of operations, timeframe of operations, persistence, concern for stealth, stages of the cyber attack lifecycle used, cyber effects sought or produced, and capabilities.	
	Level of Detail / Granularity: M	**Complexity:** L	**Rigor:** L
	***Usage Considerations*:**		

Model or Framework	Characteristics		
	Population: Representative values or scales for adversary characteristics.	**Adoption:** L	**Compatibility:** H (NIST SP 800-30)
NIST SP 800-154 (DRAFT)	***Applicability*:**	***Intended Use:* Design analysis**	
	Scope: System	**Business Environment:** Neutral	**Technical Environment:** Neutral
	***Structure*:**		
	Threat Domain Coverage: Does not discuss cyber attack lifecycle.	**Key Terms:** Threat; attack vector	
	Level of Detail / Granularity: M; extensible	**Complexity:** M	**Rigor:** M
	***Usage Considerations*:**		
	Population: Representative examples	**Adoption:** L (draft)	**Compatibility:** M (NIST SP 800-30R1)
STRIDE	***Applicability*:**	***Intended Use:* Design analysis**	
	Scope: System	**Business Environment:** Neutral. Created for software development, but has been applied more broadly	**Technical Environment:** Software
	***Structure*:**		
	Threat Domain Coverage: Implicit use of cyber attack lifecycle: defines classes of threat actions, corresponding to Control and Execute. Does not address insider, supply chain, non-cyber.	**Key Terms:** Threat classes	
	Level of Detail / Granularity: L	**Complexity:** L	**Rigor:** L
	***Usage Considerations*:**		
	Population: Representative examples	**Adoption:** M	**Compatibility:** M; can be used with NIST SP 800-30
DREAD	***Applicability*:**	***Intended Use:* Design analysis**	
	Scope: System	**Business Environment:** Neutral, but created for software development	**Technical Environment:** Software
	***Structure*:**		
	Threat Domain Coverage: Implicit use of cyber attack lifecycle, by incorporating STRIDE. Does not address insider, supply chain, non-cyber.	**Key Terms:** [Not a threat model; method for assessing risk associated with a threat exploit] Threat Exploit	
	Level of Detail / Granularity: L	**Complexity:** L	**Rigor:** L
	***Usage Considerations*:**		
	Population: Representative examples	**Adoption:** L	**Compatibility:** M
	***Applicability*:**	***Intended Use:* Risk assessment**	

Model or Framework	Characteristics			
OCTAVE / Allegro	**Scope:** Organization, Mission, System	**Business Environment:** Neutral	**Technical Environment:** Neutral	
	***Structure*:** **Threat Domain Coverage:** No use of cyber attack lifecycle. Process can be used to analyze insider threats, supply chain attacks, and non-cyber.		**Key Terms:** Threat scenario, attack tree, means, outcome (cyber effects)	
	Level of Detail / Granularity: M; extensible		**Complexity:** M	**Rigor:** M
	***Usage Considerations*:** **Population:** Representative values: Four classes of threats (top nodes of attack trees)	**Adoption:** M	**Compatibility:** L	
Intel's TARA and TAL	***Applicability*:**		***Intended Use:* Risk assessment (TARA), risk framing (TAL)**	
	Scope: Organization, Mission, System	**Business Environment:** Neutral	**Technical Environment:** Neutral	
	***Structure*:** **Threat Domain Coverage:** No mention of cyber attack lifecycle. Process can be used to analyze insider threats, supply chain attacks, and non-cyber.		**Key Terms:** Threat agent, Motivation, Objective (cyber effect), Resources (personnel), Skills, Method, Attack, Visibility (concern for stealth)	
	Level of Detail / Granularity: L		**Complexity:** M	**Rigor:** M
	***Usage Considerations*:** **Population:** Representative values: eight attributes, 22 threat archetypes	**Adoption:** L (but aspects incorporated into OWASP)	**Compatibility:** H (NIST SP 800-30, ATT&CK, OWASP)	
IDDIL/ATC	***Applicability*:**		***Intended Use:* Risk assessment**	
	Scope: System	**Business Environment:** Neutral	**Technical Environment:** Neutral	
	***Structure*:** **Threat Domain Coverage:** Uses Lockheed Martin Cyber Kill Chain.		**Key Terms:** Asset, threat actor, attack vector, threat profile, threat type, attack surface	
	Level of Detail / Granularity: M; extensible		**Complexity:**	**Rigor:**

Model or Framework	Characteristics			
	***Usage Considerations*:**			
	Population: Representative values in published materials	**Adoption:** L	**Compatibility:** H (NIST SP 800-30, STRIDE)	
STIX	***Applicability*:**	***Intended Use:* Threat information sharing**		
	Scope: Organization, Mission, System	**Business Environment:** Neutral	**Technical Environment:** Neutral	
	***Structure*:**			
	Threat Domain Coverage: Defines seven stages in cyber attack lifecycle. Includes insider threats; does not address supply chain or non-cyber.	**Key Terms:** Threat Actor (goals, sophistication, resource level, primary motivation, secondary motivations, and personal motivations); Malware; Tools; Attack Pattern; Campaign; Intrusion Set		
	Level of Detail / Granularity: D	**Complexity:** M	**Rigor:** M	
	***Usage Considerations*:**			
	Population: Depends on community of organizational users	**Adoption:** H	**Compatibility:** H (de facto standard)	
OMG Threat / Risk Model	***Applicability*:**	***Intended Use:* Threat information sharing**		
	Scope: Organization, Mission, System	**Business Environment:** Neutral	**Technical Environment:** Neutral	
	***Structure*:**			
	Threat Domain Coverage: Provides a structure in which a wide variety of adversaries and attacks can be defined.	**Key Terms:** Operational risk, threat, threat source, threat actor, undesired event, tactics, techniques, procedures, exploit target, goal, and campaign		
	Level of Detail / Granularity: H	**Complexity:** H	**Rigor:** M	
	***Usage Considerations*:**			
	Population: Will depend on community of users	**Adoption:** To be determined (intended for H, but new effort)	**Compatibility:** H (STIX)	
ATT&CK	***Applicability*:**	***Intended Use:* Threat information sharing**		
	Scope: System	**Business Environment:** Neutral	**Technical Environment:** Windows	
	***Structure*:**			
	Threat Domain Coverage: Applies to cyber attack lifecycle right of Exploit. Does not address insider, supply chain, non-cyber.	**Key Terms:** Adversary TTP		
	Level of Detail / Granularity: H	**Complexity:** L	**Rigor:** M	
	***Usage Considerations*:**			

Model or Framework	Characteristics			
	Population: Currently 230 entries; extensible	**Adoption:** M	**Compatibility:** H (STIX)	
CAPEC™	***Applicability*:**	***Intended Use:* Threat information sharing**		
	Scope: System	**Business Environment:** Neutral	**Technical Environment:** Neutral; emphasis on Windows and *nix	
	***Structure*:**			
	Threat Domain Coverage: Defines three phases: "Explore", "Experiment", or "Exploit." Some entries represent insider threats, supply chain attacks, and non-cyber attacks.	**Key Terms:** Attack pattern, mechanism of attack, domain of attack		
	Level of Detail / Granularity: H	**Complexity:** M	**Rigor:** M	
	***Usage Considerations*:**			
	Population: 508 entries in v. 2.11	**Adoption:** H	**Compatibility:** M (NIST SP 800-30)	
OWASP	***Applicability*:**	***Intended Use:* Design analysis**		
	Scope: System	**Business Environment:** Neutral	**Technical Environment:** Web applications	
	***Structure*:**			
	Threat Domain Coverage: Does not use cyber attack lifecycle, insider threats, or supply chain attacks.	**Key Terms:** Threat event, attack class		
	Level of Detail / Granularity: M	**Complexity:** L	**Rigor:** L	
	***Usage Considerations*:**			
	Population: 20 threat events in OWASP handbook	**Adoption:** M (OWASP community)	**Compatibility:** M (NIST SP 800-30)	
Cyber Threat Framework (ODNI, NSA/CSS)	***Applicability*:**	***Intended Use:* Threat information sharing**		
	Scope: System, Mission, Organization	**Business Environment:** Neutral	**Technical Environment:** Neutral	
	***Structure*:**			
	Threat Domain Coverage: Uses cyber attack lifecycle. Does not address insider threats.	**Key Terms:** Threat actor, attack stage, objective of action, action, indicator		
	Level of Detail / Granularity: M; extensible	**Complexity:** M	**Rigor:** M	
	***Usage Considerations*:**			
	Population: 200+ threat events in NSA/CSS CTF	**Adoption:** M (well adopted in the Intelligence community)	**Compatibility:** M (STIX for ODNI, ATT&CK for NSA/CSS)	
Invincea	***Applicability*:**	***Intended Use:* Design analysis**		
	Scope: Organization	**Business Environment:** Neutral	**Technical Environment:** Neutral	

<table>
<tr><th>Model or Framework</th><th colspan="4">Characteristics</th></tr>
<tr><td></td><td colspan="4">Structure:</td></tr>
<tr><td></td><td colspan="2">Threat Domain Coverage:
Defines eight stages in cyber attack lifecycle. Does not address supply chain or non-cyber; treats insider threat as a campaign vehicle (attack vector).</td><td colspan="2">Key Terms:
Adversary Type, Campaign Objective, Campaign Vehicle, Campaign Weapon, Payload Delivery, Payload Capabilities</td></tr>
<tr><td></td><td colspan="2">Level of Detail / Granularity:
L</td><td>Complexity:
M</td><td>Rigor:
M</td></tr>
<tr><td></td><td colspan="4">Usage Considerations:</td></tr>
<tr><td></td><td>Population:
Small number of values for each term.</td><td colspan="2">Adoption:
L</td><td>Compatibility:
M</td></tr>
</table>

4.2 Assessment of Cyber Threat Models

Many of the cyber threat models surveyed in Sections 2 and 3 could serve as a starting point for credible threat models that the NGCI Apex Program could use. Each model has both strengths and weaknesses, and models vary in their relevance to the financial services sector (or other critical infrastructure sectors). In this section, assessment criteria for NGCI Apex Program adoption or tailoring of cyber threat models are defined; and an assessment of the surveyed threat models against those criteria is given.

4.2.1 Assessment Criteria

Figure 13 illustrates three broad dimensions that can be used to characterize a model and assess its suitability for a given use:

- **Specification**: How fully specified is the model, in terms of taxonomy, relationships, and algorithms? This determines the extent to which its uses can be repeatable and reproducible. This dimension relates to such characteristics as level of detail or granularity, complexity, and rigor.
- **Coverage**: What does the model cover? This determines the circumstances in which the model can be used meaningfully. Coverage includes completeness: How completely does the model cover the domain it represents? For example, does the threat model represent the cyber attack lifecycle, insider threats, supply chain attacks, or non-cyber attacks? In addition, coverage includes applicability: Does the model assume a specific scope, business environment, technical environment, or threat environment?
  Note that completeness is with respect to the current state of knowledge, and applicability is with respect to current practice and technology. Thus, a model which is currently comprehensive can, over time, come to represent selected sub-domains.
- **Concreteness**: How concrete is the model? This relates to how well it is populated.

For a cyber threat model, Adoption and Extensibility relate to Specification. Scalability relates to one aspect of Coverage.

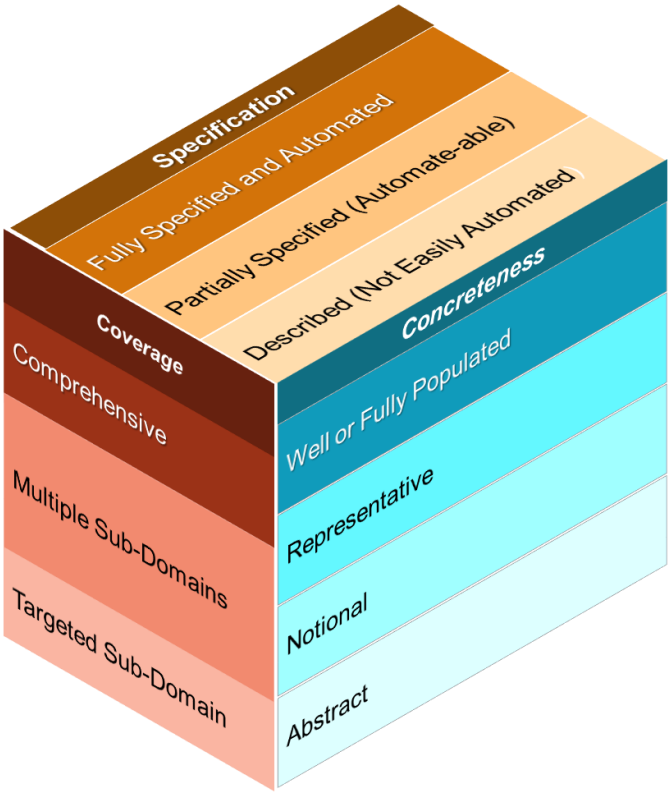

Figure 13. Characterizing a Model for Use in Evaluating Effectiveness

As noted in Section 1, threat models (including frameworks and methodologies) are important to NGCI Apex in three ways:

- A threat model can be used as an input to risk modeling processes (in particular, to definition, evaluation, and sharing of risk metrics).
- A threat model can motivate and be used in the development of scenarios for cyber wargaming.
- A threat model can be used to support the identification and evaluation of cyber defense technologies, by helping to indicate which technologies are relevant and suggesting test cases and scenarios in which the technologies' effectiveness can be assessed.

These possible uses can be considered with varying scopes, as illustrated in Figure 2. As the survey of published models presented in Table 4 illustrates, no widely accepted model currently addresses all possible scopes.

In the following subsections, assessment criteria related to these possible uses are identified. It must be noted that no single model can meet all the criteria, particularly when the different scopes at which effectiveness could be evaluated or risk could be measured are considered. Even in the context of a single use (e.g., evaluation of cyber defense technologies for a representative large financial institution), trade-offs among the criteria can be identified.

4.2.1.1 Support Definition and Evaluation of Risk Metrics

As noted in Section 1, a threat model is a component of a risk model, which is used to produce risk metrics. The following characteristics of risk models and risk metrics (and thus of cyber threat models and metrics, which are constituents of risk models and risk metrics) relate to supporting the risk assessment, tracking, and prioritization goals of NGCI Apex:

- **Adaptability and extensibility**: How easily can the model be adapted, for example to represent evolving threat capabilities? How easily can the model be extended to include additional concepts, attributes, factors, or algorithms?
- **Feasibility**: How practical is it to use the model and/or evaluate the metrics, in real-world environments?
  - Can the requisite data be obtained (e.g., using existing products and processes)?
  - Can the data be analyzed in a reasonable time period (i.e., quickly enough to support decisions), with a reasonable level of effort (taking into consideration the size of the entity performing the analysis)?
  - How well do evaluation and use of the model and/or set of metrics fit into existing governance? In particular, how well does the model or set of metrics support cybersecurity risk management as an integral aspect of enterprise risk management (ERM)?
- **Adoptability**: How easily can the model and/or set of metrics be adopted? In particular, how consistent is the model or set of metrics with those currently used by sector institutions?
- **Scalability**: What is the scope of the model? Can the metrics be aggregated, rolled up, or otherwise combined to produce broader-scale metrics (e.g., from system to mission, from system or mission to organization, from organization to sector or to some cross-sector business function)?
- **Information sharing**: How compatible is the model with models or standards used to share information about threats or risks?

4.2.1.2 Provide a Foundation for Cyber Wargaming

NGCI Apex has identified potential uses for a variety of forms of cyber wargaming to identify gaps in technologies, practices, and supporting policies and standards, and to evaluate the relative effectiveness of proposed or as-implemented solutions to cybersecurity issues across a critical infrastructure sector, focusing on the financial services sector. Forms of cyber wargaming include tabletop exercises (with varying degrees of automated support), Red Team exercises, and hybrid exercises.

Tabletop, and to a lesser extent hybrid, exercises can range in scope from the system level to the national or transnational level. Red Team exercises are oriented to systems, missions, or portions of organizations. The level of detail needed in a threat model for specific modeling constructs depends on the scope of the exercise. For example, an exercise might assume a single adversary goal; alternately, as a scenario plays out, secondary or tertiary goals might be considered.

A threat model is used to develop threat scenarios for an exercise, or for a family of related exercises. Any wargaming exercise will be limited to a small number of threat scenarios. Some aspects of specification are less important for some forms of cyber wargaming; for example, complexity and rigor are important when a wargame involves considerable automated support, but could lead to distractions for participants in many tabletop exercises. Completeness is less of a consideration for threat models for cyber wargaming than for other purposes. Coverage depends on the purpose of the exercise.

4.2.1.3 Support Profiling and Evaluation of Cyber Defense Technologies

In terms of the Cyber Defense Matrix (Figure 4), NGCI Apex seeks to provide well-founded answers to such questions as:

- How well does a given technology improve an organization's ability to identify resources that are part of or are connected to its network? (Network-Identify)
- How well does a given technology improve an organization's ability to protect sensitive or critical data? (Data-Protect)
- How well does a given technology improve an organization's ability to detect exfiltration, modification, or fabrication of sensitive or critical data? (Data-Detect)
- How well does a given technology at the network layer improve an organization's ability to detect adversary-created degradation, interruption, modification, or misdirection of services, or modification of data? (Network-Detect)

These questions can be made more precise by using a threat model which represents adversary activities (e.g., which includes a cyber attack lifecycle model) and a vocabulary for describing possible effects on adversary activities (e.g., as described in [NIST 2018]).

Beyond the benefits to individual organizations, NGCI Apex seeks to provide well-founded answers to questions of the form: If a given technology were widely deployed across a sector, how much better off would the sector be, in terms of ability to:

- Correlate attack information across sector institutions, so that multi-organizational responses can be developed and implemented? (Note that participation in multi-organizational responses can range from a pair of partner institutions, to a handful of affected institutions, together with law enforcement and US-CERT, to a sector-wide response.)
- Detect new or emerging adversary TTPs?
- Determine the most effective defender TTPs to address adversary activities?
- Disseminate knowledge of new or emerging adversary TTPs and/or effective defender TTPs?
- Adapt systems and networks to protect cyber resources against anticipated new adversary TTPs?
- Identify new or emerging technologies as they become capable of connecting to systems and networks operated by sector institutions?

Claims about the effectiveness of cyber defense technologies can be evaluated in a variety of settings, including abstract or conceptual models, modsims (i.e., modeling and simulation events) or M&S environments, cyber ranges, tabletop exercises, simulation experiments (SIMEX, [MITRE 2009]), operational experiments, and deception environments. Each setting instantiates a model of the threats, the technical environment(s), and the operational environment(s) in which the effectiveness claims are expected to hold [Bodeau 2013b], thereby representing aspects of system-centric and asset-centric threat modeling views [NIST 2018b]. When an evaluation environment (a setting for evaluating claims about effectiveness) is constructed, trade-offs must be made between these characteristics. For example, a modsim can be fully specified and fully populated, but typically makes assumptions which restrict its coverage to a limited or targeted sub-domain.

4.2.2 Assessment of Surveyed Models, Frameworks, and Methodologies

The considerations described above apply to all models, including risk models as well as threat models. For cyber threat models, these considerations can be recast, taking into consideration the questions which NGCI Apex seeks to answer and the goal of defining a set of realistic and threat-informed cyber attack test scenarios. In characterizing a cyber threat model using the framework illustrated in Figure 12, the following more detailed questions can be taken into consideration:

- **Specification**: Specification in the context of a cyber threat model refers to the set of terms it defines, the relationships it defines among those terms, the qualitative or quantitative values that it allows to be assigned to those terms, and the algorithms it defines based on the identified relationships, to compute values for higher-level terms based on values assigned or measured for lower-level terms. Defined terms: How fully does the cyber threat model represent the terms used in standard or commonly used threat models (e.g., NIST SP 800-30R1, STIX)? Does the model define these terms, or simply use them? Is the set of terms extensible? Relationships: How, and how fully, does the model define relationships (e.g., dependencies, subset or superset) among the terms it uses? For example, does the model define a taxonomy or an ontology, or does it express relationships solely in the form of text discussion? Values: Does the model define a range of values explicitly (e.g., a list of qualitative or nominative values, a quantitative range), or implicitly (e.g., via anchoring examples in definitions or discussions of terms)? If the model provides qualitative values, is the set of qualitative values extensible? Algorithms: Does the model define rules or algorithms for assigning values? For example, does the model include tables to combine qualitative values? If the model defines rules or algorithms, are these tailorable?
- **Coverage**: Coverage in the context of a cyber threat model refers to the range of threat sources, threat scenarios, and intended or expected threat consequences it can represent. Coverage also refers to the range of scopes over which threats can be represented. Threat sources: Does the threat model cover solely attacks from an external adversary, or does it also cover insider threats? Does it consider human error or structural failure as primary threat sources, as contributing factors to adversarial threats, or not at all? Threat scenarios: Does the threat model restrict attention to threat scenarios involving as-deployed, as-used systems, or does it include threat scenarios throughout the system lifecycle? In particular, does it include supply chain attacks? Does the threat model

assume a specific technical or operational environment (e.g., Microsoft vs. *nix; consumer-oriented institutions vs. back-end institutions)? Threat consequences: Does the threat model identify consequences of threat events or threat scenarios in terms of cyber consequences, mission or organizational consequences, or benefits to or achievements experienced by the adversary? Scope: Is the threat model intended for use solely at the system level (e.g., to inform systems engineering decisions), or can it be used with broader scopes? Does the threat model enable threat scenarios to be developed which span organizations? Does the threat model assume a specific business environment or critical infrastructure sector, or can it be used to develop threat scenarios which span sectors?

- **Concreteness**: Concreteness in the context of a cyber threat model refers to how well it is populated and how easily it can support development of scenarios, test cases, or use cases. Population: How well populated is the model, in terms of representative values for key terms? Have the values been validated in terms of realism? For example, are there real-world case studies which provide examples? Is the population fixed or extensible? Is the population maintained as current? Scenario development: How easily can the cyber threat model be used to construct test cases and motivating examples? How well does the model support scenario development? For example, does it include sample attack scenarios to serve as a starting point?

In this section, the models, frameworks, and methodologies surveyed in Sections 2 and 3 are assessed with respect to the criteria identified above. The assessment is presented in Table 6, using the key in Table 5.

Table 5. Evaluation Attributes

	Value		
Attribute	**L**	**M**	**H**
Specification (Definitions, Relationships, Values, Algorithms)	Described (i.e., verbal descriptions)	Partially Specified (e.g., using representative values)	Fully Specified (e.g., providing a relatively complete set)
Coverage (Scope, Threat Sources, Threat Scenarios, Threat Consequences) [Note: a "+" indicates that the threat model includes non-adversarial threats; an "*" indicates coverage specific to the FSS]	Targeted (i.e., focused on a specific sub-domain with a specific scope)	Broad (i.e., covering multiple sub-domains and/or covering multiple scopes)	Comprehensive (i.e., covering all sub-domains for a given scope and/or covering multiple sub-domains at multiple scopes)
Concreteness (Population, Scenario Development)	Abstract or Notional (i.e., few if any examples are given)	Representative (i.e., at least one example is given for every modeling construct)	Well or Fully Populated (i.e., multiple examples or values are given for every modeling construct)
Adaptability & Extensibility	Static or Fixed	Modifiable or Tailorable	Highly Flexible
Feasibility in Operational Environments	Infeasible (i.e., data must be supplied by SMEs)	Supported by some tools (i.e., limited automated support for data gathering)	Supported by tools and information sharing mechanisms
Adoptability	Not consistent with models in use	Consistent with models in use	Reference point for models in use

Attribute	Value		
	L	M	H
Scalability	Aggregation limited to frequency counts	Limited computation of aggregate metrics	Designed to enable aggregation at multiple scales
Information Sharing (Standards Compatibility)	Independent of and possibly incompatible with standards	Compatible with one or more standards	Constitutes a standard

Table 6. Summary Assessment of Threat Models and Frameworks

	Specification				Coverage				Concreteness						
Framework, Methodology, or Model	Definitions	Relationships	Values	Algorithms	Scope	Threat Sources	Threat Scenarios	Threat Consequences	Population	Scenario Development	Adaptability & Extensibility	Feasibility in Operational Environments	Adoptability	Scalability	Information Sharing (Standards Compatibility)
NIST SP 800-30R1	H	M	M	M	M	H +	H +	M	M	M	H	L	H	H	L
CBEST	H	M	M	M	M *	M *	M *	M *	L	M	M	L	M	M	L
COBIT 5 & Risk IT	L	L	L	L	M	M +	L	M	L	L	H	L	M	L	L
Proposed DRDC	M	M	L	-	L	M	L	M	L	L	M	L	M	L	L
DSB 6-Tier Threat Hierarchy	L	L	M	-	L	M	L	L	L	-	M	L	M	M	L
Cyber Prep / DACS	H	H	M	L	M	H	L	M	M	L	M	L	H	H	L
Attack Tree Modeling	•[17]	M	•	◦[18]	M	◦	◦	•	L	◦	H	L	M	L	L
NIST SP 800-154 (DRAFT)	M	M	M	M	M	M	M	M	L	M	M	L	M	L	L
STRIDE	L	L	L	L	L	TL	M	L	L	M	M	L	M	L	L
DREAD	L	L	L	L	L	TL	L	M	L	M	M	L	M	L	L
OCTAVE / Allegro	M	M	L	L	M	M +	M +	M	L	M	H	L	M	L	L
Intel's TARA / TAL	M	L	M	L	M	M	M	L	M	L	L	L	L	L	L
IDDIL/ACT	M	M	M	L	M	M	M	M	L	M	M	L	M	L	M
STIX	H	H	M	L	L	M	M	M	•[19]	M	M	M	H	M	H
OMG Threat / Risk Model	H	H	M	L	H +	H +	H	H +	L	L	M	L	L	L	•[20]
ATT&CK	H	H	H	L	L	M	L	L	H	M	M	L	M	M	H
CAPEC	H	H	H	L	L	M	M	L	H	M	H	L	M	L	H
OWASP	M	M	L	L	L	M	M	L	M	L	L	L	M	L	M
CTF	H	H	M	-	M	H	H	M	-	-	H	H	M	H	M

[17] Low-to-Medium, depending on specific modeling technique.

[18] Medium-to-High, depending on specific modeling technique.

[19] Depends on organizational users. Within some communities, High.

[20] Intended to be High.

	Specification				Coverage				Concreteness						
Framework, Methodology, or Model	Definitions	Relationships	Values	Algorithms	Scope	Threat Sources	Threat Scenarios	Threat Consequences	Population	Scenario Development	Adaptability & Extensibility	Feasibility in Operational Environments	Adoptability	Scalability	Information Sharing (Standards Compatibility)
MITRE's TARA	M	M	M	H	M	M	M	L	M	L	M	L	M		L
Invincea	L	L	M	L	M	M	M	M	M	L	M	L	M	L	M
NSCSAR	L	L	L	L	M	M	M	M	L	M	M	L	M	L	M
Large Financial Institution Notional Threat Model	L	M	L	L	M *	M *	M *	M *	L	L	M	L	M	L	L

Table 7 presents profiles of the desired characteristics of threat models or modeling frameworks with respect to some of the purposes identified by the NGCI Apex program. A dash (-) indicates that the characteristic is not applicable.

Table 7. Profiles of Desired Characteristics of Threat Models for Different Purposes

	Specification				Coverage				Concreteness						
Purpose	Definitions	Relationships	Values	Algorithms	Scope	Threat Sources	Threat Scenarios	Threat Consequences	Population	Scenario Development	Adaptability & Extensibility	Feasibility in Operational Environments	Adoptability	Scalability	Information Sharing (Standards Compatibility)
Risk framing	L	L	M	-	M	M	M	M	M	M	H	-	M	-	-
Risk assessment (expert-driven)	M	M	M	M	M	M-H	M	M-H	M-H	M	M	L-M	M	M	-
Risk assessment (automated tool)	H	H	H	H	M	M-H	M-H	H	H	M-H	H	M-H	M	M	M
Cyber wargaming (expert-driven)	M	M	M	-	L-M	M	M	M	M	M	M-H	L-M	M	L	-
Cyber wargaming (automated generation)	H	H	H	H	L-M	M-H	M-H	H	M	M-H	M	M-H	M	M	-
Portfolio Management	L-M	L-M	L-M	L	M	M-H	M-H	M-H	L-M	M	M	L-M	M	L	M
Technology profiling and foraging	M	L	M	-	L-M	M	M	M	M	L-M	M	-	M	-	-

	Specification				Coverage				Concreteness							
Purpose	Definitions	Relationships	Values	Algorithms	Scope	Threat Sources	Threat Scenarios	Threat Consequences	Population	Scenario Development	Adaptability & Extensibility	Feasibility in Operational Environments	Adoptability	Scalability	Information Sharing (Standards Compatibility)	
Technology evaluation (functional testing)	M	L	M	-	L-M	M	M	M	M-H	M	-	M-H	-	-	-	
Penetration testing	M	M	M	M	M	M-H	M-H	M-H	M-H	M	M	M-H	M	M	-	
Operations	M	M	M	L	L-M	L-M	-	H	M-H	-	H	H	M	-	-	
High-water mark (all uses)	H	H	H	H	M	M-H	M-H	H	H	M-H	H	M-H	M	M	M	

A comparison of Tables 6 and 7 indicates that many of the surveyed models and frameworks share characteristics making them suitable for risk framing, risk assessments by expert practitioners, cyber wargaming when defined and directed by experts, and technology profiling. Few if any are suitable for automated generation of risk assessments or cyber wargames, reflecting the state of the practice. Some may be suitable for technology evaluation or penetration testing; however, suitability for those uses depends on the technical environment, since no model or modeling framework represents all possible technologies. The last line of Table 7 represents the high-water mark of all the uses identified in that table, and indicates that simultaneous suitability for all uses raises the bar very high.

4.3 Relevance of Cyber Threat Modeling Constructs

One observation from the discussion of different modeling frameworks in Sections 2 and 3 is that different frameworks use different modeling constructs or terminology. When analysts seek to decide which framework to use to develop a cyber threat model for a specific purpose, they consider whether the framework provides them with the vocabulary they need to answer the questions that purpose raises. They also may consider whether the framework requires them to represent aspects of cyber threats which are not relevant to that purpose, since such a requirement involves wasted effort and possible distraction. Table 8 characterizes terms or modeling constructs from the frameworks discussed in Sections 2 and 3 with respect to the purposes identified in Section 1.[21] Where one modeling construct is commonly accepted as an

[21] Because the NGCI Apex program is specifically interested in risk metrics, the risk management purpose is broken into two purposes: risk assessment and risk framing. In risk assessment, some adversary characteristics can be used either to assess the likelihood that an adversary will initiate a threat scenario or to classify a threat scenario as relevant or irrelevant to an adversary with that characteristic; other characteristics are used to assess the likelihood that the adversary will succeed in executing a threat event or attack event.

attribute of another, that higher-level construct is identified in parentheses. A term or modeling construct can be used for characterization or classification (indicated by C), in which case alternative values are nominal; such constructs generally are used in the development of threat scenarios to support the intended purpose. Alternatively, qualitative or semi-quantitative values (S) or quantitative values (Q) can be associated with a modeling construct to represent a measurable or evaluable property.

The purposes are relevant at different scales or scopes. *Risk framing* and *risk assessment* (by supporting the definition of risk metrics) are relevant at all scopes. Some purposes – *cyber wargaming* and *threat information sharing* – are relevant to efforts with broad scopes (organization or enterprise; sector, region, or COI; national or transnational) as illustrated in Figure 1; *security operations* as informed by threat information sharing is relevant primarily at the organization level. *Design analysis and testing* is primarily relevant at the system or implementation / operations level; however, since a mission or business function is typically supported by a system of systems (SoS), design analysis and testing can be relevant at that level as well.

Technology profiling and technology foraging efforts are situated in an assumed technical environment, i.e., in a context of assumptions about the architectures, technical standards, or product suites with which technologies to be identified and profiled must interoperate. Thus, such efforts can be relevant to a community of interest or critical infrastructure sector, defined by or characterized in terms of its shared technical environment. Such efforts can also be specific to an organization (characterized by its enterprise architecture), a mission or business function, or an individual system. In general, technology profiling and foraging efforts focus on the threat events for which technologies might reduce the likelihood of success or the severity of consequences.

Modeling constructs which support a purpose at one scope may be irrelevant at another scope. Therefore, Table 8 identifies the scope(s) at which a given construct is relevant to a purpose with the following values: 1 for system, implementation, or operations; 2 for mission or business function (and/or supporting SoS); 3 for organization or enterprise; 4 for sector, region, or COI; and 5 for national or transnational.

Table 8. Uses of Cyber Threat Modeling Constructs

Term	Sources	Risk Assess-ment	Risk Framing	Cyber War-gaming	Technology Profiling & Foraging	Design Analysis & Testing	Security Operations & Threat Information Sharing
Adversary, Threat Actor, Threat Agent, or Threat Entity	NIST SP 800-30R1 CBEST, Risk IT, DRDC, DSB, CP/DACS, TARA/TAL, IDDIL/ATC, STIX, OMG, ODNI CTF	1-5: C	1-5: C	2-4: C		1-2: C	1, 4: C

Term	Sources	Risk Assess-ment	Risk Framing	Cyber War-gaming	Technology Profiling & Foraging	Design Analysis & Testing	Security Operations & Threat Information Sharing
(Adversary or Threat) Type or Source	NIST SP 800-30R1 CBEST, Risk IT, DRDC, OCTAVE/Allegro, TARA/TAL, Invincea, IDDIL/ATC, OMG	1-5: C	1-5: C	2-4: C		1-2: C	1, 4: C
(Adversary) Capability	NIST SP 800-30R1 CBEST, CP/DACS	1-3: S	1-5: C	2-4: C, S		1-2: C	1, 4: C
(Adversary Capabilities) Resources	CBEST, DRDC, CP/DACS, STIX, ODNI CTF	1-5: S	1-5: C	2-4: C		1-2: C	1, 4: C
(Adversary Resources) Technological Resources or Sophistication	CBEST, DRDC, DSB, CP/DACS, TARA/TAL, STIX	1-5: C, S	1-5: C	2-4: C		1-2: C	1, 4: C
(Adversary Resources) Information Resources or Intelligence	CBEST, DRDC, CP/DACS	1-5: C, S	1-5: C	2-4: C		1-2: C	1, 4: C
(Adversary Resources) Financial Resources	CBEST, CP/DACS	1-5: C, S	1-5: C	2-4: C		1-2: C	1, 4: C
(Adversary Resources) Personnel	CBEST, DRDC, CP/DACS, TARA/TAL	1-5: C, S	1-5: C	2-4: C		1-2: C	1, 4: C
(Adversary Capabilities) Relationships	CBEST, CP/DACS	1-5: C		2-4: C		1-2: C	1, 4: C
(Adversary) Intent	NIST SP 800-30R1		1-3: C				
(Adversary Intent) Motivation	CBEST, DRDC, CP/DACS, TARA/TAL, STIX, Invincea	1-5: C	1-5: C	2-4: C		1-2: C	1, 4: C
(Adversary Intent) Additional Motivation	CBEST, TARA/TAL, STIX	1-5: C	1-5: C	2-4: C		1-2: C	1, 4: C
(Adversary Motivation) Goal (non-cyber)	DRDC, TARA/TAL, OMG, ODNI CTF	1-5: C	1-5: C	2-4: C			

Term	Sources	Risk Assess-ment	Risk Framing	Cyber War-gaming	Technology Profiling & Foraging	Design Analysis & Testing	Security Operations & Threat Information Sharing
(Adversary Non-Cyber Goal) Scope or Scale	DSB, CP/DACS		1-5: C	2-4: C			
(Adversary Motivation) Intended Cyber Effect	Risk IT, DRDC, CP/DACS, OCTAVE/Allegro, TARA/TAL	3: C		2-4: C	1-2: C	1-2: C	
(Adversary Intent) Persistence, Commitment, or Resolve	CBEST, DRDC, CP/DACS	1-5: C		2-4: C		1-2: C	1, 4: C
(Adversary Intent) Concern for Stealth or Risk Sensitivity	CBEST, DRDC, CP/DACS, TARA/TAL	1-5: C		2-4: C		1-2: C	1, 4: C
(Adversary Intent) Timeframe	DRDC, DSB, CP/DACS			2-4: C			
(Adversary) Targeting	NIST SP 800-30R1	1-3: C					
Attack Phase or Stage (of Cyber Attack Lifecycle or Cyber Kill Chain)	NIST SP 800-30R1 CBEST, CP/DACS, ODNI CTF	1-5: C		2-4: C		1-2: C	1, 4: C
(Adversary) TTP, Method, Means, Modus Operandi, or Attack Pattern	CBEST, OCTAVE/Allegro, STIX, OMG, ATT&CK, CAPEC, ODNI CTF, Invincea	1-5: C		2-4: C	1-4: C	1-2: C	1, 4: C
(Adversary Method) Operational Tempo	CBEST	1-5: C		2-4: C		1-2: C	1, 4: C
Threat Event	NIST SP 800-30R1 Risk IT, OWASP, CTF	1-5: C; 1-2: S		2-4: C	1-4: C	1-2: C	
(Adversary, Attack Pattern, or Threat Event) Attack Vector or Delivery Mechanism	DRDC, NIST SP 800-154 (Draft), IDDIL/ATC, CAPEC	1-2: C		2-4: C	1-4: C	1-2: C	

Term	Sources	Risk Assess-ment	Risk Framing	Cyber War-gaming	Technology Profiling & Foraging	Design Analysis & Testing	Security Operations & Threat Information Sharing
(Adversary, Attack Pattern, or Threat Event) Mechanism of Attack or Attack Category	DRDC, STRIDE, DREAD, IDDIL/ATC, CAPEC OWASP	1-3: C		2-4: C	1-4: C	1-2: C	1, 4: C
Threat Scenario	NIST SP 800-30R1, CBEST, Risk IT, OCTAVE/Allegro	1-3: C; 1-2: S		1-4: C		1-2: C	

4.4 Combining Cyber Threat Models for NGCI Apex

As Tables 6, 7, and 8 indicate, cyber threat models can differ in a variety of ways. The desired uses draw upon different concepts, and the NGCI Apex program considers a range of scopes, from system to sector. Therefore, it is unsurprising that no single model or modeling framework surveyed covers all the concepts needed for the full range of uses or scopes identified by the NGCI Apex program. This observation does not imply criticism of any of the models surveyed. Instead, it points to the need for a threat modeling framework which can be used at multiple scales and tailored to different purposes. As shown in Figure 14, threat models inform two threads of NGCI Apex activities:

- Transitioning innovative cyber technologies into use in the FSS. The initial threat model provided in Section 5.2 of this report can help with high-level profiling of technologies of potential interest by providing a basis for characterizing which threat events they may address. More detailed threat models, which specify attack techniques and patterns, can be used to help define test cases for testing of candidate products.
- Enhanced cyber wargaming. Threat models at varying degrees of detail can feed the development of wargame scenarios at corresponding levels of detail. Cyber wargames can be developed and conducted for use cases including assessing risk in various circumstances and identifying gap areas in which additional cyber technologies could be helpful. Cyber wargames also provide a means of developing playbooks for how to manage the situation in various cyber attack what-if scenarios.

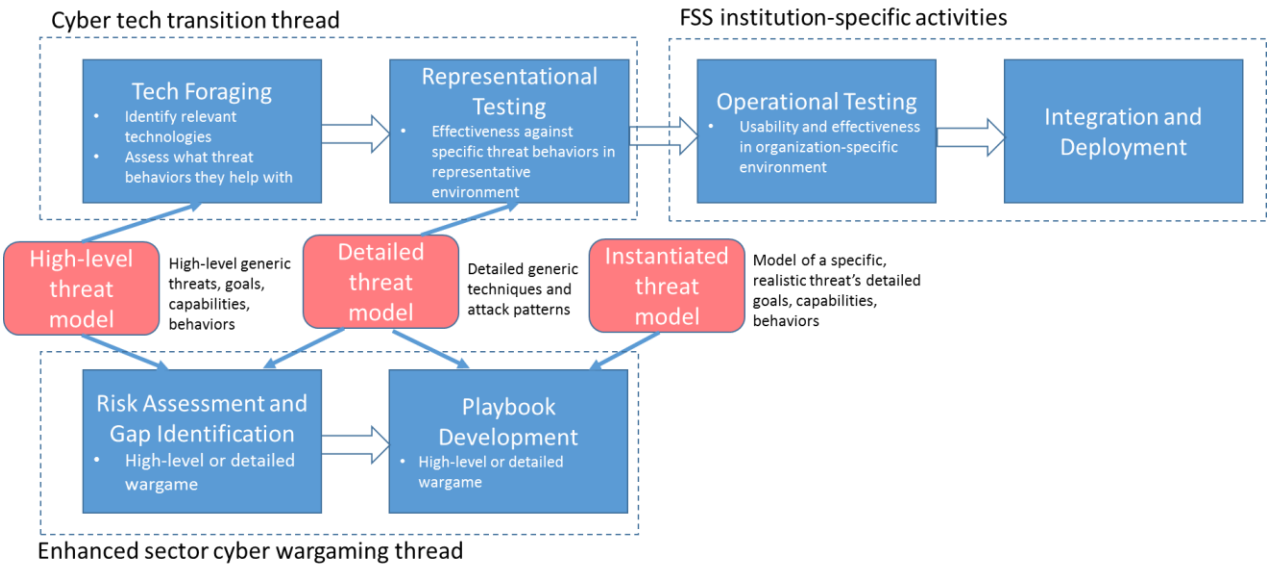

Figure 14. Uses of Cyber Threat Models in NGCI Apex

Therefore, the threat modeling framework for NGCI Apex needs to support the development of a suite of consistent models:

- High-level models. These support technology foraging and profiling, high-level or sector-wide risk assessment, and cyber wargames in which events are described in general terms.
- Detailed threat models. These support technology evaluation, risk assessments for systems (or for missions as supported by defined systems-of-systems), cyber wargaming in which events are described in terms of specific systems, technologies, and targets; and development of high-level cyber playbooks in which types of actions are recommended for types of threat events.
- Instantiated threat models. These can be developed either by NGCI Apex or by an individual FSS institution. NGCI Apex can use instantiated threat models to support development of detailed cyber playbooks in which actions involving specific technology are recommended for threat events based on indicators. An individual FSS institution can instantiate a threat model with details specific to its technologies, operating environments, and business functions.

Level of detail should not be confused with degree of population. For example, an instantiated threat model used to evaluate a technology can include highly specific information about only a few threat events, against which the technology is hypothesized to have specific effects on the activities of a representative threat actor directing those events. By contrast, a high-level or a detailed threat model used in a modsim can be fully populated. The level of detail in a threat model depends in part on the extent to which accompanying models of the system and assets affected by the threat are specified. This is illustrated in Figure 15.

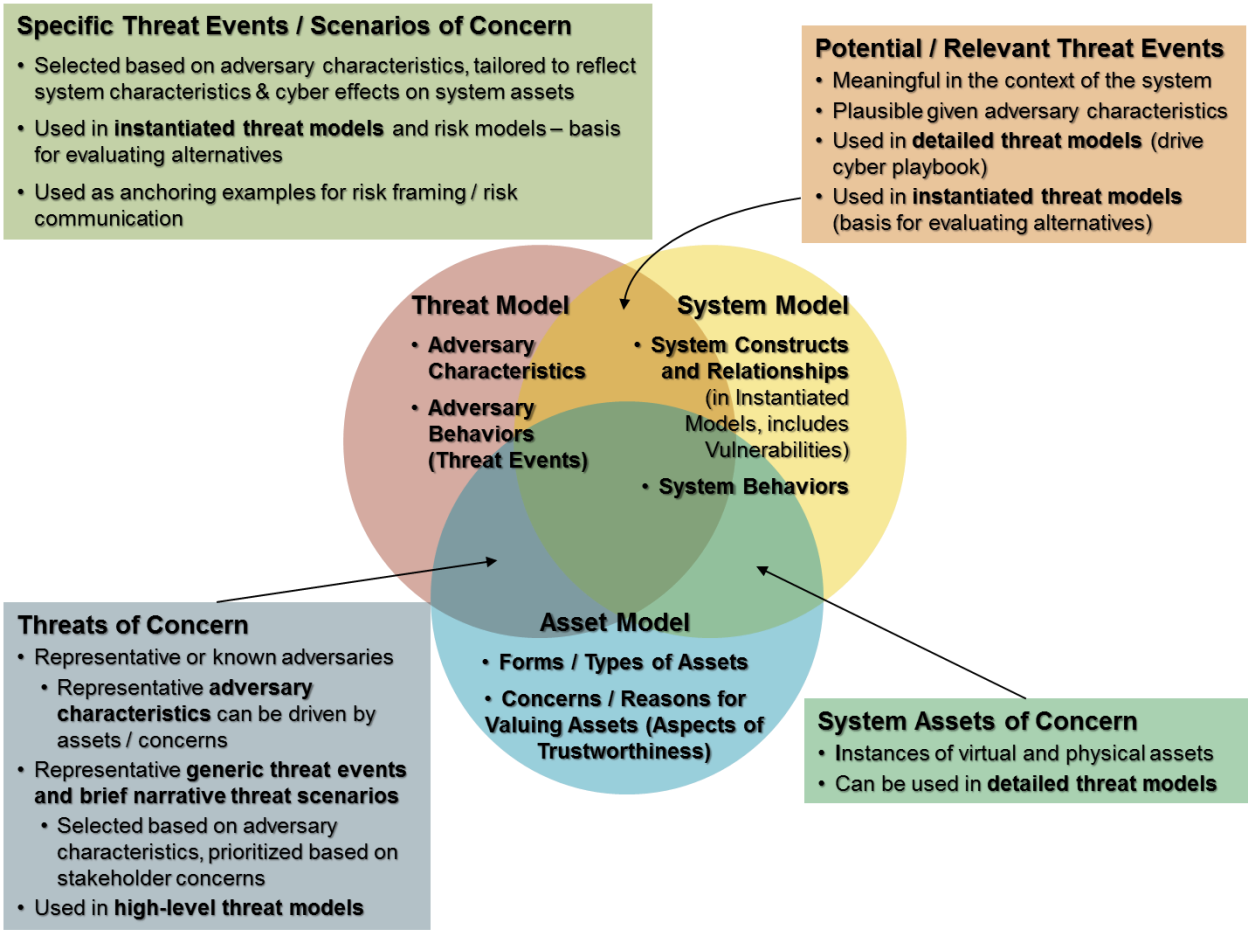

Figure 15. Threat Modeling Level of Detail Depends on Whether and How Assets and Systems Are Modeled

The NIST SP 800-30R1 model identifies several aspects of threat to consider in the course of an analysis:

- The threat source (in the case of adversarial threats, the threat actor), which has multiple characteristics. For a threat actor, these include capability, intent, and targeting. Capability, intent, and targeting need not be specified in exactly these terms, however. To take advantage of other sources of information or models, they can be provided via some other set of characteristics which can be mapped to them.
- What the threat source might do to produce adverse consequences. Actions a threat source might perform are described using a threat scenario representing the adversary's behavior.
- The consequences or impacts of adversary activities. Consequences that are important to recognize include those that are unintended as well as intended.

While the NIST model provides some suggested examples of threat events (which can be supplemented by entries from other taxonomies as discussed in Sections 3.1.3 and 3.1.4), it does not determine those that apply to a specific organization and its environment, or combine them into threat scenarios. Threat scenarios can be developed using various approaches: an attack tree

modeling technique, a cyber attack lifecycle model, or some less structured approach. In any case, the building blocks of a threat scenario are individual threat events or attack patterns consisting of sets of threat events. Information provided in ATT&CK (identifying specific attacker techniques – in Windows environments, initially) and CAPEC (specifying known patterns of threat events) can be used to populate threat scenarios in a repeatable way, using the same names for the same events or patterns. Threat events might also be expressed in or mapped to a sector-specific model, such as the generic Large Financial Institution Notional Threat Model described in Section 3.2.2, to provide a link to business functions affected.

STIX and TAXII provide a common, structured representation of multiple aspects of threat. STIX defines how threat information is described, and TAXII provides the protocol for conveying it from one organization to another. Conforming to (or mapping to) these common representations allows an organization to continue populating and updating portions of the NIST model, by consuming new information about threats as it is shared by others, or to share its own new locally observed information about threats with them in turn.

5 Initial Cyber Threat Model

This section presents an initial cyber threat model for use by the NGCI Apex program and by organizations in critical infrastructure sectors. First, in Section 5.1, a high-level cyber threat modeling framework is described. It identifies the key constructs and relationships, provides representative values for key constructs and examples of relationships, and describes how threat scenarios can be generated from the framework. The threat modeling framework is based on the NIST 800-30R1 framework, elaborated and fusing in material from other frameworks to meet the needs of NGCI Apex. Key constructs are illustrated in Figure 16; characteristics of threat types and the relationships between these characteristics and other modeling constructs are discussed in Section 5.1. (Constructs and relationships in dotted lines are included to indicate linkages to risk modeling; these constructs are used in risk assessment, and relate to the system model or the asset model in Figure 15.) In each case, the verb should be modified with "one or more;" for example, a threat scenario has one or more consequences.

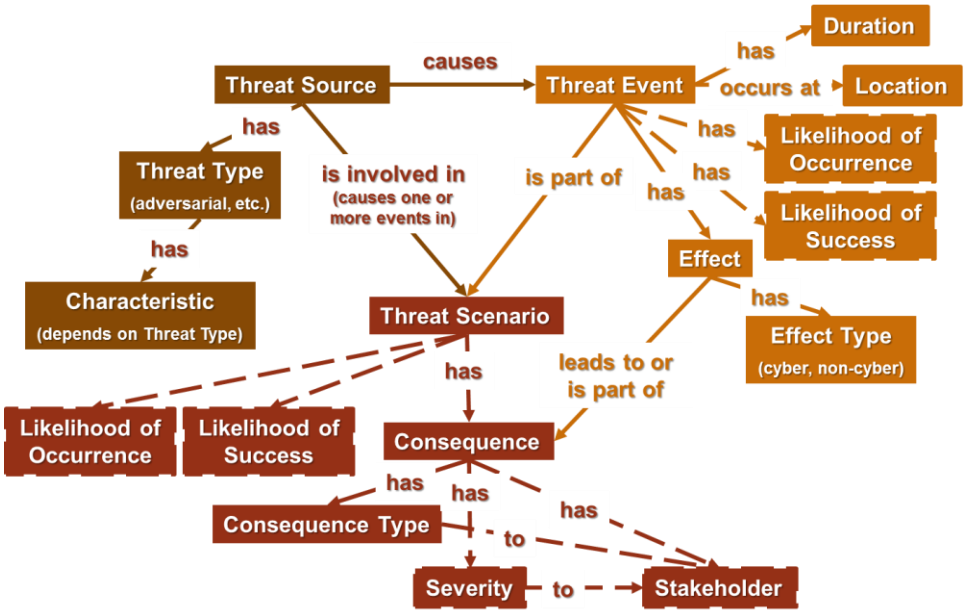

Figure 16. Key Constructs in Cyber Threat Modeling (Details for Adversarial Threats Not Shown)

Section 5.1 presents this framework in discursive form, with a few representative examples. Additional detail can be found in Appendix A, which presents definitions of terms, relationships, and values or references in which sets of values can be found.

In Section 5.2, an initial high-level threat model built using the framework is described. This threat model instance is populated notionally, as an indication of what more fully fleshed-out models will look like. The initial model assigns values to some but not all constructs from the framework.

Section 5.3 provides some high-level examples of threat scenarios representative of cyber attacks and campaigns. Based on an assumed enterprise IT and operational environment, these examples describe attack vectors, attack targets, a few representative attack events, their cyber effects, and how those cyber effects relate to the adversary goals.

5.1 Modeling Framework

A modeling framework for a problem domain defines the key constructs and relationships that should be included in a model, in order for that model to be meaningful and useful in that domain. A meaningful model uses, or can easily be translated into, terms which stakeholders understand. It is not solely the province of subject matter experts. A useful model is one which can be used in processes or activities that produce results that stakeholders value.

For NGCI Apex, the problem domain is adversarial threats that exploit dependence on cyberspace to produce consequences to financial services sector (FSS) entities. A cyber threat modeling framework for the FSS therefore must consider adversary goals and potential side effects of cyber attacks that are relevant to FSS entities. It must also support development of models that can be used in the evaluation of alternative technologies, architectures, processes, and procedures, particularly in the context of cyber wargaming. In addition, the framework must accommodate ways in which adversarial threats can leverage or emulate non-adversarial threats. For example, the disruption to normal business processes resulting from a natural disaster can be exploited by cyber adversaries. Adversaries frequently take advantage of human error, and adversaries can also make their activities appear to be the effects of human errors or of errors in external systems and infrastructures.

The initial set of key constructs (indicated in ***bold italics*** and defined in Appendix A) are:

- ***Types*** of ***threat sources***: adversarial, non-adversarial (structural failure, human error, natural disaster). The characteristics of the threat depend on its type:
    - For adversarial threats, key characteristics are ***intent***, ***targeting***, and ***capabilities***. Each of these has multiple sub-characteristics, as described in the following subsections.
    - For classes of threat source other than adversarial, characteristics include ***scope or scale of effects***, ***timeframe***, and ***types of assets*** affected. (Types of non-adversarial threat sources and their characteristics are described briefly in this section, below.)
- ***Threat events***. These are caused by threat sources. The possibility and likelihood that a given threat source will cause a threat event is based on the threat source's characteristics. Many adversarial threat events can be categorized in terms of stages in a cyber attack lifecycle or cyber kill chain model, and can be related to adversary capabilities and types of resources affected.

In more detail, characteristics of non-adversarial threat sources, which are closely related to behavior, are as follows. Non-adversarial threat sources are outside the scope of the initial threat model in Section 5.2 but are included in the framework to support the development of cyber wargaming scenarios in which an adversary treats events caused by such sources as opportunities.

- Human error. Characteristics of a threat event of this type include:
    - Role (of threat actor): privileged user, normal user, individual with physical access to facility, external actor, maintainer, developer / integrator
    - Form of error: physical / kinetic error (e.g., cut power to a component), system configuration error, user input error, erroneous value transmitted, software

development error resulting in vulnerability, integration error resulting in vulnerability

- ***Location***: See ***scope or scale of effects*** (Table 11) and ***types of assets*** (Section 5.1.2).
- Historical frequency (if available)

- Structural failure. Note that threat events are typically described in terms of the types of effects they have (e.g., power failure, loss of DNS services).
  - Scope or scale of effects: See Table 11.
  - Duration
  - Historical frequency (if available)
- Natural or widespread disaster
  - Scope or scale of effects. See Table 11.
  - Duration
  - Historical frequency (if available)

5.1.1 Adversary Intent

For adversarial threats, key sub-characteristics of intent include:

- ***Goal(s) or motivation(s)***. Depending on the intended use of the threat model, primary, secondary, and additional goals might be identified. In addition, typical organizational consequences of the adversary achieving a goal might be identified.
- ***Intended cyber effect(s)***
- ***Scope or scale of intended effects***
- ***Timeframe***
- ***Persistence*** (or ease with which adversary can be discouraged)
- ***Concern for stealth***
- ***Opportunism*** or synergies with non-adversarial threat events (e.g., deception via phishing after a natural disaster)

Figure 17 illustrates how these aspects of intent relate to other constructs. For a threat event a given threat actor could cause, the likelihood of occurrence (i.e., the likelihood that the threat actor will choose to cause the event) is affected by the adversary's timeframe and the duration associated with the event (event duration or duration of exposure), the adversary's concern for stealth, and (insofar as the threat event is part of a larger threat scenario in which non-adversarial events have occurred) the adversary's opportunism. The likelihood of occurrence is strongly conditioned on the adversary's knowledge of (or beliefs about) the resources which could be affected by the threat event. Note that a threat scenario can have multiple consequences, of different types and affecting different stakeholders. To the extent that a consequence is intended by the adversary, it can be identified with an adversary goal or motivation.

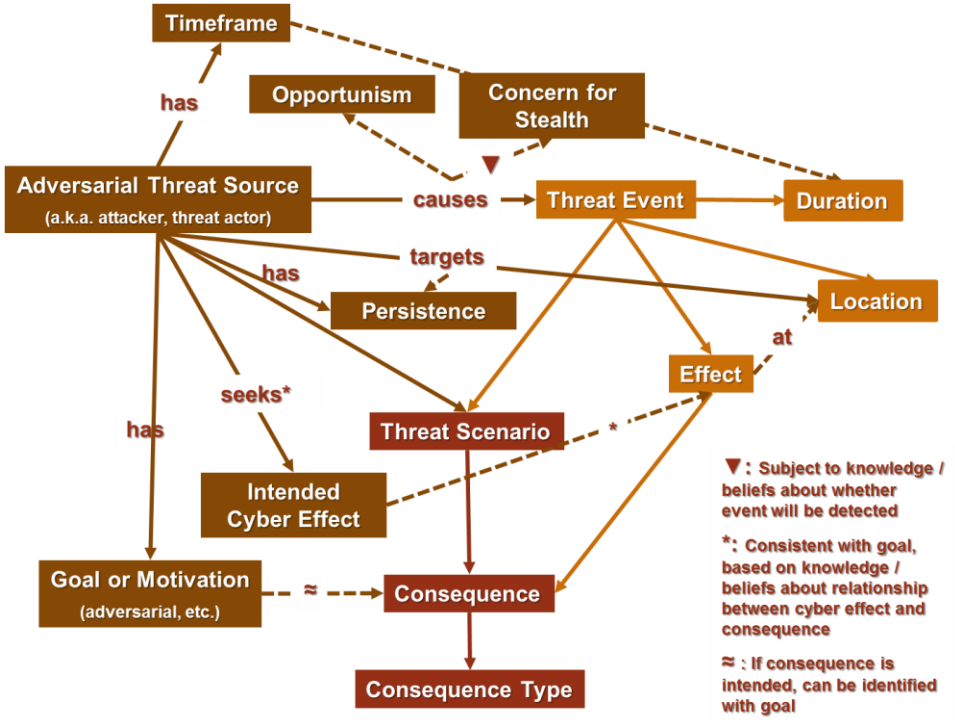

Figure 17. Relationships Between Aspects of Adversary's Intent and Other Key Constructs

Representative values of these intent-related characteristics are shown in the following tables. Table 9 describes the linked characteristics of adversary goals, cyber effects (defined in Table 13), and organizational consequences. Table 10 defines representative values for the adversary's timeframe, persistence, and concern for stealth, and links these to stages of the cyber attack lifecycle.

Table 9. Characteristics Related to Adversary Intent: Goals, Cyber Effects, and Organizational Consequences

Adversary Goal	Typical Cyber Effects	Typical Organizational Consequences
Financial gain		
• Fraud against or theft from the organization	Corruption, Modification, or Insertion	Financial loss, Reputation damage
• Acquire salable / usable personally identifiable information (PII) (e.g., credit card numbers)	Exfiltration, Interception	Liability due to non-physical harm to individuals, Reputation damage
• Acquire salable / usable competitive information	Exfiltration, Interception	Liability due to failure to meet contractual obligations, Loss of future competitive advantage
• Extortion	Degradation or Interruption Corruption, Modification, or Insertion Exfiltration	Financial loss (ransom paid to avert denial-of-service, destructive malware such as ransomware or wipers, adversary release of sensitive information)

Adversary Goal	Typical Cyber Effects	Typical Organizational Consequences
• Fraud against or theft from the organization's customers, suppliers, or partners	Unauthorized use	Financial loss (indirect, through theft of services), Reputation damage, Liability
Personal motives		
• Attention	Degradation, Interruption Corruption, Modification, or Insertion	Reputation damage
• Malice / resentment	Degradation, Interruption Corruption, Modification, or Insertion	Reputation damage, Liability due to physical or non-physical harm to individuals
• Acquire PII about targeted individuals	Exfiltration, Interception	Reputation damage, Liability due to non-physical harm to individuals
Geopolitical advantage		
• Undermine public confidence in government or critical infrastructure sector	Degradation, Interruption Corruption, Modification, or Insertion Exfiltration, Interception	Physical or non-physical harm to individuals, Reputation loss
• Cause economic or political instability	Degradation, Interruption Corruption, Modification, or Insertion Exfiltration, Interception	Reputation damage, Financial loss to multiple individuals or organizations
• Terrorism	Degradation, Interruption	Physical or non-physical harm to individuals, Reputation loss
• Acquire information that improves another nation's economic advantage	Exfiltration, Interception	Loss of future competitive advantage
• Acquire / use military advantage	Degradation, Interruption Corruption, Modification, or Insertion	Military mission failure, Loss of future military advantage
• Acquire / use ability to threaten homeland security	Degradation, Interruption Corruption, Modification, or Insertion	Homeland security mission failure, Loss of future capabilities
Positional / Stepping-Stone		
• Acquire a launching point for targeted attacks	Corruption, Modification, or Insertion Unauthorized use	Reputation damage, Liability due to harm to other entities
• Acquire resources that can be used in targeted attacks (e.g., DDoS)	Unauthorized use	Reputation damage, Liability due to harm to other entities
• Acquire intelligence about other entities	Exfiltration, Interception	Liability due to harm to other entities

Table 10. Characteristics Related to Adversary Intent: Timeframe, Persistence, Stealth, CAL Stages

Timeframe	Persistence	Stealth	CAL Stages
One-time or Episodic. Episodic adversary activities are limited in duration, in order to achieve a specific effect or goal – or to determine that the intended effect cannot be achieved without sustained effort. Episodic operations can be one-time attacks, or the adversary can perform them periodically or in response to triggering events.	None	No concern for stealth, although some concern for attribution is possible	Deliver, Exploit, Execute
Episodic or Sustained. Sustained adversary activities occur over an extended time period (e.g., months to a couple of years), requiring the adversary to make sustained investments of time, effort, or other resources.	Limited, with near-term (tactical) planning	Limited concern, focused on concealing evidence of presence	Recon, Deliver, Exploit, Execute
Sustained	Persistent, with planning for a cyber campaign	Moderate concern, focused on concealing evidence of presence, TTPs, and capabilities	All, but Weaponize is limited
Sustained or Enduring	Strategically Persistent, with long-term planning for multiple campaigns	High concern, focused on concealment and deception; may use OPSEC	All
Enduring. Enduring adversary activities occur over a significant time period (several years, or into the future without bounds) and with a scope that requires the adversary to define an investment strategy and a strategic plan for achieving goals.	Strategically Persistent, with long-term planning for multiple coordinated campaigns	Very high concern; may use OPSEC, counterintelligence, and partnerships or other relationships	All, including multiple CALs (e.g., cyber, supply chain, physical or kinetic)

5.1.2 Adversary Targeting

As illustrated in Figure 15, an adversary selects a threat event with the intention of causing an effect at a location; targeting thus can be identified with location selection. Two major sub-characteristics of adversary targeting are ***scope or scale of intended effects*** and type of ***assets*** targeted. Scope/scale relates strongly to the timeframe aspect of intent. Representative values of scope/scale are identified in Table 11.

Table 11. Scope or Scale of Effects

Scope or Scale of Effects	Scope or Scale of Adversarial Targeting
Very Narrow: A small and well-defined set of organizational assets	**Organizational Subset**: The adversary targets a subset of the organization's systems or business functions (e.g., public-facing Web services), resulting in a *localized engagement* with the adversary.
Narrow: A set of organizational assets sharing a common property or set of properties (e.g., physical location, type of OS)	**Critical Organizational Operations or Targeted Information**: The adversary targets those of the organization's systems, infrastructure, or business functions that are critical to its operations or that handle specific information, in the form of *structured campaigns*.

Scope or Scale of Effects	Scope or Scale of Adversarial Targeting
Broad: Any or all assets belonging to or reachable from an organization	**Organizational Operations and Associates**: The adversary targets any of the organization's systems, infrastructure, or business functions, as well as the organization's customers, users, or partners, in the form of *structured campaigns, including campaigns that span organizational elements or multiple organizations*.
Strategic: Assets across a critical infrastructure sector, sub-sector, or geographic region	**Sector or Community**: The adversary targets interdependent critical infrastructure or financial services sector systems, or set of systems spanning multiple organizations to accomplish a collective mission. Note that the Quantum Dawn exercises [Deloitte 2015] have focused on this scale.
Broadly Strategic: Assets across a nation or across multiple critical infrastructure sectors	**National or Transnational**: The adversary targets systems and organizations critical to the nation or to interrelated infrastructure or industry entities.

Note that scope/scale also applies on the defensive side: technical and operational decisions can be made and executed at different scales.

Types of assets targeted can use the five asset classes in the Cyber Defense Matrix (devices, applications, network, data, and people), or can add classes and sub-classes based on (1) the enterprise architecture of a specific institution or on a generic architecture such as the Open Systems Architecture (OSA) developed for the NGCI Apex program and/or (2) functionality or mission role. In particular, the following initial set of sub-classes can be defined for FSS organizations:

- Device: enterprise endpoint clients (e.g., laptops, desktops used by organizational staff), special-purpose endpoints (e.g., automated teller machines or ATMs), customer endpoint mobile devices (e.g., smartphones, tablets, customer laptops)
- Network:
  - Network components
    - Networking devices (e.g., routers, switches, firewalls)
    - Network servers (e.g., domain name service or DNS servers, directory servers, dynamic host configuration protocol or DHCP servers)
    - Other network-discoverable devices
  - Enterprise services (e.g., identity and access management or IdAM services)
- Application: financial transaction applications, financial transaction monitoring applications, trend/historical analysis and forecasting, customer interaction applications (e.g., Web, mobile), customer relationship management (CRM) applications
- Data: financial service (FS) databases (e.g., account databases); databases or other knowledge stores about partners, suppliers, or customers
- People: enterprise staff, customers, staff at partner organizations, general public

These subclasses are a starting point and are not exhaustive. In the case of devices, network, or application, the asset is identified with the services it provides (e.g., making information accessible).

5.1.3 Adversary Capabilities

Adversary ***capabilities*** can be characterized in terms of ***resources*** (e.g., expertise, financial resources, technical resources), ***methods***, and ***attack vectors***. Representative values for five broad classes of adversary capabilities are shown in Table 12.

Table 12. Characteristics of Adversary Capabilities: Resources, Methods, and Attack Vectors

Capability	Resources	Methods and Attack Vectors
Acquired	The adversary has very limited resources or expertise of their own.	The adversary tends to employ malware, tools, delivery mechanisms and strategies developed by others. The adversary focuses on cyber attack vectors, specific to the organization and its systems, or to service providers. The adversary also uses limited human attack vectors for reconnaissance and deception (e.g., email, social media).
Augmented	The adversary some expertise and limited resources of their own.	The adversary builds upon known vulnerabilities and publicly available malware, to develop their own new malware (e.g., zero day attacks). The adversary focuses on cyber attack vectors, specific to the organization and its systems, or to service providers. The adversary also uses limited human attack vectors for reconnaissance and deception (e.g., email, social media).
Developed	The adversary has a moderate degree of resources and expertise.	The adversary discovers unknown vulnerabilities, and develops their own malware (e.g., zero day) utilizing those vulnerabilities, and their own delivery mechanism. Alternately, the adversary purchases vulnerability information and tailored malware. The adversary focuses on cyber attack vectors, specific to the organization and its systems, or to service providers. The adversary also uses human attack vectors for reconnaissance, deception, subversion, and coercion.
Advanced	The adversary has a significant degree of resources and expertise.	The adversary "influences" commercial products and services (or free and open source software) during design, development, manufacturing, or acquisition (supply chain), allowing them to introduce vulnerabilities into such products. The adversary uses a wide range of attack vectors, not only against the organization, but also against its suppliers, system integrators, maintainers, partners, and service providers – non-cyber (e.g., power) as well as cyber.
Integrated	The adversary is sophisticated and very well resourced.	The adversary generates their own opportunities to successfully execute attacks that combine cyber and non-cyber threads in support of a larger, non-cyber goal. The adversary seeks out, and fosters vulnerabilities in, a wide range of attack surfaces. The adversary uses a wide range of attack vectors, not only against the organization, but also against its suppliers, system integrators, maintainers, partners, and service providers – non-cyber (e.g., power) as well as cyber.

As indicated in Table 12, methods use – and can be categorized in terms of – attack vectors. An ***attack vector*** is a general approach to achieving a cyber effect, and takes advantage of the exposure of a type of, or a region in, an attack surface.[22] Attack vectors can be categorized as

[22] At a minimum, the term "attack surface" refers to "accessible areas where weaknesses or deficiencies in information systems (including the hardware, software, and firmware components) provide opportunities for adversaries to exploit vulnerabilities." [NIST 2013] While some uses of the term focus on externally exposed vulnerabilities, the assumption that an adversary will

cyber, physical, and human; are closely related to targeting; and are characteristic of behaviors. I.e., a given behavior, attack event, or threat event uses a given attack vector. Representative values of attack vectors include:

- Cyber attack vectors: supply chain, maintenance environment, external network connection, external shared or infrastructure services, trusted or partner network connection, internal network, internal shared or infrastructure services, internal system, mobile or transiently connected devices[23], authorized actions of non-privileged user, authorized actions of privileged user, device port (e.g., removable media), data
- Physical attack vectors: immediate physical proximity, cyber-physical interface, indirect attack (e.g., kinetic attack on building, tampering with heating, ventilation, and air conditioning [HVAC])
- Human attack vectors have multiple attributes:
  - Role of attacked individual(s): privileged user, normal user, external actor, maintainer, developer / integrator
  - Intended effect on attacked individual(s): coercion, subversion, deception, incapacitation
  - Method for achieving intended effects on attacked individual(s): physical threats, social media interactions, in-person interactions, email

5.1.4 Behaviors or Threat Events

Depending on the level of detail needed, threat events can be drawn from different resources. More general threat events can be taken from NIST SP 800-30R1; more specific adversarial threat events or behaviors can be drawn from ATT&CK and CAPEC. Threat events and behaviors relate to characteristics of threat sources. For example, threat events associated with a CAL stage are relevant only to adversaries whose attacks include that stage; threat events associated with a given attack vector are only included in a threat model if that attack vector is included in the model of or set of assumptions about the technical and operational environment in which the attack occurs. A threat event occurs at one or more ***locations*** (see Section 5.1.2) and may have a ***duration***. A threat event has one or more ***effects***, which may be cyber or non-cyber. One set of possible cyber effects, adapted from [Temin 2010], is shown in Table 13.[24] Note that a given event can have multiple effects, depending on the architectural view from which the effect is described. For example, the introduction of ransomware into an OS is insertion from an OS view, but modification from a system view; the subsequent triggering of the ransomware has the cyber effect of interruption.

penetrate an organization's systems means that internal exposures – vulnerabilities which can be reached by lateral movement within a system or infrastructure – are also part of the attack surface. Conceptually, the term can also cover aspects of the operational, development, and maintenance environments that an adversary can reach and that could contain vulnerabilities.

[23] These include, for example, personal devices allowed under a bring-your-own-device (BYOD) policy.

[24] Table 13 differs from [Temin 2010] in several ways: Insertion is offered as an alternative to Fabrication; Usurpation is offered as an alternative to Unauthorized use; Accountability is offered as a security objective corresponding to Unauthorized use; and Corruption and Exfiltration are added.

Table 13. Cyber Effects

Cyber Effect	Description	Related Security Objective
Degradation	A reduction in the performance or effectiveness of a system or component	Availability
Interruption	Loss of any ability to use a cyber asset	Availability
Corruption	Change in the quality of existing information, data, protocol, or software, to make it unusable or undependable	Availability / Integrity
Modification	Change in existing information, data, protocol, or software	Integrity
Fabrication (or Insertion)	Introduction of new information, data, or software into a system	Integrity
Unauthorized use (or Usurpation)	Use of system resources in violation of policies	Accountability
Interception	Obtaining of access to information within or transmitted to or from a system	Confidentiality
Exfiltration	Unauthorized transmission or removal of information from a system	Confidentiality

5.1.5 Threat Scenarios

Threat scenarios for cyber wargaming, risk assessment, or technology evaluation can be developed in a variety of ways, depending on such factors as the scale of the wargaming exercise, the scope of the risk assessment, or the assumed environment for the technology to be evaluated. Starting points for scenario development include:

- Historical events. A real-world incident can be generalized or recapitulated in terms specific to the exercise environment (e.g., selecting attack events specific to the system environment). Real-world incidents can be drawn from another sector (e.g., the attack on the Target Corporation, the DDoS attack on Dyn), as well as from the financial services sector (e.g., the attacks on Society for Worldwide Interbank Financial Telecommunication [SWIFT] customers). Scenarios based on historical events can range in scale from very narrow to strategic.
- Postulated sector-wide attacks, as in the case of some large-scale exercises. These can focus on attacks on shared infrastructures or services (e.g., SWIFT for the FSS), exploitation of zero-days in widely deployed technologies, or attacks on specific key institutions (e.g., DDoS attack on a large financial institution, with ripple effects across the FSS). Scenarios of this type focus on the strategic scale, and can also include a broad scope (a given institution and its partners, customers, and suppliers).
- Adverse cyber effects on specific assets (services, databases), to serve as the starting point for a fault tree analysis. Scenarios of this type can be very narrow or narrow in scope.

The level of detail in the threat scenario depends on the level of detail provided or assumed for such attributes of the wargaming exercise as business functions, system environment, and defensive cyber technologies and posture.

5.2 Initial Representative Threat Model

This section describes a high-level threat model developed for the NGCI Apex program, using the framework in Section 5.1. This initial representative threat model is restricted to adversarial threats. (If desired or needed, future versions could look at interactions between adversarial and non-adversarial threats.)

5.2.1 Adversary Characteristics

A key assumption of this threat model is that FSS institutions must be prepared for these threats. Threats that must be addressed by government entities are not included. In particular, this threat model does not include nation-state-sponsored military groups or terrorist groups, whether aligned with nation-state or not. Note that when a terrorist group actively seeks financial gain, it is operating as a criminal enterprise rather than committing terrorism. Table 14 selects adversary goals from Table 9, identifies typical actors, and identifies typical targets of adversarial activities.

Table 14. Adversary Goals, Typical Actors, and Targets

Adversary Goal	Typical Actors	Typical Targets
Financial gain		
• Fraud against or theft from the organization	Insider, criminal (individual or organized group)	Financial service (FS) databases (modify or insert data); Identity and Access Management (IdAM) services (acquire / elevate privileges)
• Acquire salable / usable PII (e.g., credit card numbers)	Insider, criminal (individual or organized group)	FS databases, IdAM services
• Acquire salable / usable competitive information	Subverted / suborned insider, criminal (individual or organized group) seeking such information on behalf of or for sale to competitors or insider trading customers	FS databases, forecasting applications and databases, strategic planning data stores
• Extortion	Insider, criminal (individual or organized group)	Network components (denial-of-service [DoS] threats); FS databases and applications (threats to destroy / encrypt data, via ransomware)
• Fraud against or theft from the organization's customers, suppliers, or partners	Insider, criminal (individual or organized group)	FS databases (for information about customers); databases or other data stores used in partnership or purchase transactions
Personal motives		
• Attention	Hackers, taggers, and "script kiddies;" small disaffected groups of the above	Network components (DoS); outward-facing services and data (DoS, fabrication)
• Malice / resentment	Disgruntled insider or former insider; Hackers, taggers, and "script kiddies;" small disaffected groups of the above	Network components (DoS); outward-facing services and data (DoS, fabrication)

Adversary Goal	Typical Actors	Typical Targets
• Acquire PII about targeted individuals (e.g., wealth, sources or allocation of wealth)	Suborned insider; criminal (individual or organized group); stalker	FS databases (for information about customers); HR databases (for information about staff which can be exploited to masquerade as or to influence them)
Geopolitical advantage		
• Undermine public confidence in financial services sector	Political or ideological activists; Nation-state-aligned professional criminal enterprise	Network components (DoS); outward-facing services and data (DoS, fabrication); FS databases and services (DoS, corruption); FS transaction data
• Cause economic or political instability	Political or ideological activists; Nation-state-aligned professional criminal enterprise	Network components (DoS); outward-facing services and data (DoS, fabrication); FS databases and services (DoS, corruption); FS transaction data (DoS, corruption) – particularly for sector infrastructure or shared services
• Acquire information that improves another nation's economic advantage	Nation-state-aligned professional criminal enterprise	FS databases, forecasting applications and databases, strategic planning data stores
Positional		
• Acquire a launching point for targeted attacks on other entities	Insider, criminal (individual or organized group)	Network components
• Acquire intelligence about other entities (e.g., business partners)	Insider, criminal (individual or organized group)	Databases or other data stores used in partnership or purchase transactions

With respect to timeframe, persistence, stealth, and stages of the cyber attack lifecycle, the threat model is restricted to the top four rows of Table 10. Scope / scale ranges from very narrow through strategic (sector-wide effects, particularly via attacks on financial infrastructure services such as joint clearing), but excludes broadly strategic. Capabilities include acquired, augmented, and developed, and also include advanced resources; advanced methods might be considered in the future. Physical and human attack vectors are excluded; cyber attack vectors include maintenance environment, external network connection, trusted or partner network connection, internal network, actions of non-privileged user, actions of privileged user, device port (e.g., removable media), and data.

5.2.2 Adversary Behaviors and Threat Events

Table 15 presents an initial set of adversary behaviors and adversary-related threat events. These are drawn primarily from NIST SP 800-30R1 but have been tailored for adversaries with the characteristics identified above. Information about attack vectors and cyber effects is added to the NIST SP 800-30R1 event descriptions. (Shading indicates that the event is drawn from NIST SP 800-30R1. A few additional events based on other frameworks, particularly the ODNI CTF

and ATT&CK, are included; these rows are unshaded.) Additional tailoring could make these descriptions more meaningful to FSS environments.

The final column illustrates how identification of events can be used for technology profiling and foraging using a matrix approach. As discussed in Section 1.2.3, the CART identified four cells in the Cyber Defense Matrix as of particular importance: Network-Identify (N-I), Network-Detect (N-D), Data-Protect (D-P), and Data-Detect (D-D). Table 15 indicates whether capabilities could reduce the likelihood of success or the consequence severity of the threat events, by identifying network-discoverable resources which could be targeted, protecting data resources, or detecting malicious activity against network or data resources.

Table 15. Adversary Behaviors and Threat Events

CAL Stage	Adversary Behavior or Threat Event	Attack Vector(s)	Cyber Effect(s)	Selected Matrix Cells
Recon	Perform perimeter network reconnaissance/scanning.	External network connection	Interception	N-I
Recon	Perform network sniffing of exposed networks.	External network connection Internal network (when CAL is applied recursively)	Interception	N-I
Recon	Perform network sniffing of external networks (e.g., ISPs) to which organizational networks are connected.	External network connection	Interception	N-I
Recon	Analyze network traffic based on network sniffing.	External network connection Internal network (when CAL is applied recursively)	Interception	N-I
Recon	Gather information using open source discovery of organizational information.	Publicly available information, social media interactions	Interception	
Recon	Perform reconnaissance and surveillance of targeted organizations.	Physical observation, social media interactions, in-person interactions, email, location tracking	Interception	
Recon	Perform malware-directed internal reconnaissance.	Maintenance environment, actions of privileged user, trusted or partner network connection	Interception	N-I, N-D
Weaponize	Craft phishing attacks.	External network connection, email	(no immediate effects)	
Weaponize	Craft spear phishing attacks.	External network connection, email	(no immediate effects)	
Weaponize	Craft psychological manipulation attacks on key staff.	Social media interactions	(no immediate effects)	

CAL Stage	Adversary Behavior or Threat Event	Attack Vector(s)	Cyber Effect(s)	Selected Matrix Cells
Weaponize	Craft attacks specifically based on deployed information technology environment.	External network connection, trusted or partner network connection	(no immediate effects)	
Weaponize	Create counterfeit/spoof web site.	External network connection	(no immediate effects)	N-D
Weaponize	Craft counterfeit certificates.	External network connection, trusted or partner network connection	(no immediate effects)	N-D
Weaponize	Create and operate false front organizations to inject malicious components into the supply chain.	Supply chain	(no immediate effects)	
Weaponize	Compromise systems in another organization to establish a presence in the supply chain.	Supply chain	(no immediate effects)	
Deliver	Establish or use a communications channel to the enterprise as a whole or to a targeted system.	External network connection, trusted or partner network connection	(no immediate effects)	N-D
Deliver	Deliver commands to a targeted system (e.g., login).	(no immediate effects)	Unauthorized use	N-D
Deliver	Deliver known malware to internal organizational information systems (e.g., virus via email). [See CTF: Interact with intended victim]	External network connection, email	Corruption, Modification, or Insertion	N-D
Deliver	Deliver modified malware to internal organizational information systems. [See CTF: Interact with intended victim]	Internal network, authorized actions of non-privileged user, authorized actions of privileged user, device port (e.g., removable media)	Corruption, Modification, or Insertion	N-D
Deliver	Deliver targeted malware for control of internal systems and exfiltration of data.	Internal network, authorized actions of non-privileged user, authorized actions of privileged user, device port (e.g., removable media)	Corruption, Modification, or Insertion	N-D

CAL Stage	Adversary Behavior or Threat Event	Attack Vector(s)	Cyber Effect(s)	Selected Matrix Cells
Deliver	Deliver malware by providing removable media.	Authorized actions of non-privileged user, authorized actions of privileged user, device port (e.g., removable media)	Corruption, Modification, or Insertion	
Deliver	Insert untargeted malware into downloadable software and/or into commercial information technology products.	Supply chain	Corruption, Modification, or Insertion	
Deliver	Insert targeted malware into organizational information systems and information system components.	Supply chain, maintenance environment	Corruption, Modification, or Insertion	
Deliver	Insert specialized malware into organizational information systems based on system configurations.	Supply chain, maintenance environment	Corruption, Modification, or Insertion	
Deliver	Insert counterfeit or tampered hardware into the supply chain.	Supply chain	Corruption, Modification, or Insertion	
Deliver	Insert tampered critical components into organizational systems.	Supply chain, maintenance environment	Corruption, Modification, or Insertion	
Deliver	Compromise information systems or devices used externally and reintroduced into the enterprise.	Mobile or transiently connected devices	Corruption, Modification, or Insertion Unauthorized use	N-D
Deliver / Exploit	Install general-purpose sniffers on organization-controlled information systems or networks.	Internal network, authorized actions of privileged user, device port (e.g., removable media)	Modification or Insertion	N-D
Deliver / Exploit	Install persistent and targeted sniffers on organizational information systems and networks.	Internal network, authorized actions of privileged user, device port (e.g., removable media)	Modification or Insertion	N-D
Deliver / Exploit	Insert malicious scanning devices (e.g., wireless sniffers) inside facilities.	Immediate physical proximity	Modification or Insertion	N-D
Exploit	Exploit physical access of authorized staff to gain access to organizational facilities.	Immediate physical proximity	(no immediate effects)	

CAL Stage	Adversary Behavior or Threat Event	Attack Vector(s)	Cyber Effect(s)	Selected Matrix Cells
Exploit	Exploit poorly configured or unauthorized information systems exposed to the Internet.	External network connection	Corruption, Modification, or Insertion	N-D
Exploit	Exploit split tunneling on an end-user system to gain access to enterprise systems.	External network connection, end-user system	Exfiltration, Interception	N-D
Exploit	Obtain a legitimate account. [See CTF]	External network connection	(no immediate effects)	
Exploit	Exploit known vulnerabilities in mobile systems (e.g., laptops, PDAs, smart phones). [See CTF: Establish illicit user access]	Mobile or transiently connected devices	Corruption, Interception	N-D
Exploit or Control	Exploit recently discovered vulnerabilities. [See ATT&CK: Lateral Movement]	External network connection, trusted or partner network connection, internal network	Corruption, Modification, or Insertion Unauthorized use	N-D
Control	Acquire privileges associated with a user account, process, service, or domain. [See ATT&CK: Credential Access]	Internal network, internal shared or infrastructure services	Unauthorized use	
Control	Modify or increase privileges associated with a user account, process, service, or domain. [See ATT&CK: Privilege Escalation]	Internal network, internal shared or infrastructure services	Modification or Insertion	
Control	Perform internal reconnaissance. [See ATT&CK: Discovery; enabled by Install sniffer, Acquire privileges, or Modify privileges]	Internal network, internal shared or infrastructure services	Interception	N-D
Control	Exploit multi-tenancy in a cloud environment. [See ATT&CK: Lateral Movement; enabled by Obtain a legitimate account]	Internal shared or infrastructure services	Corruption, Interception	
Control	Exploit vulnerabilities on internal organizational information systems. [See ATT&CK: Lateral Movement]	External network connection, trusted or partner network connection, internal network	Corruption, Modification, or Insertion Unauthorized use	N-D
Control	Exploit vulnerabilities using zero-day attacks. [See ATT&CK: Lateral Movement]	External network connection, trusted or partner network connection, internal network, mobile or transiently connected devices	Corruption, Modification, or Insertion Unauthorized use	N-D

CAL Stage	Adversary Behavior or Threat Event	Attack Vector(s)	Cyber Effect(s)	Selected Matrix Cells
Control or Execute	Exploit vulnerabilities in information systems timed with organizational mission/business operations tempo.	External network connection, trusted or partner network connection, internal network	Degradation, Interruption Corruption, Modification, or Insertion Unauthorized use	N-D
Control	Exploit insecure or incomplete data deletion in multi-tenant environment.	External network connection, trusted or partner network connection, internal network, internal shared or infrastructure services	Exfiltration, Interception	D-P
Control	Violate isolation in multi-tenant environment.	Internal shared or infrastructure services	Degradation, Interruption Exfiltration, Interception	D-P
Control	Establish command and control (C2) channels to malware or compromised components. [See ATT&CK: Command and Control]	External network connection, trusted or partner network connection, internal network, internal shared or infrastructure services	Corruption, Modification, or Insertion Unauthorized use Exfiltration	N-D
Control	Employ anti-IDS measures. [See CTF; see ATT&CK: Defense Evasion]	Internal network, internal shared or infrastructure services	Modification, Insertion	N-D
Control	Employ anti-forensics measures. [See CTF; see ATT&CK: Defense Evasion]	Internal network, internal shared or infrastructure services, internal system	Modification, Insertion	N-D
Control	Compromise critical information systems via physical access.	Immediate physical proximity	Degradation, Interruption Corruption, Modification, or Insertion Unauthorized use	
Control	Compromise software of organizational critical information systems.	Maintenance environment, internal network, internal shared or infrastructure services, authorized action of privileged user, device port	Corruption, Modification, or Insertion Unauthorized use	N-D

CAL Stage	Adversary Behavior or Threat Event	Attack Vector(s)	Cyber Effect(s)	Selected Matrix Cells
Control	Compromise organizational information systems to facilitate exfiltration of data/information. [See CTF: Relocate and store data on victim's computer, information system(s), network(s), and/or data stores]	Maintenance environment, internal network, internal shared or infrastructure services, authorized action of privileged user, device port	Corruption, Modification, or Insertion Unauthorized use Exfiltration, Interception	N-D
Control	Stage data for exfiltration. [See CTF: Relocate and store data on victim's computer, information system(s), network(s), and/or data stores; see ATT&CK: Collection]	Internal network, internal shared or infrastructure services, internal system	Insertion	D-P, D-D
Control	Compromise information critical to mission / business functions.	Internal network, internal shared or infrastructure services, authorized action of non-privileged user, authorized action of privileged user, device port, data	Corruption, Modification, or Insertion	D-P, D-D
Execute	Obtain sensitive information through network sniffing of external networks. [See ATT&CK: Collection]	External network connection, trusted or partner network connection	Interception	D-P
Execute	Cause degradation or denial of attacker-selected services or capabilities. [See CTF: Deny access]	Internal network, internal shared or infrastructure services, authorized action of privileged user	Degradation, Interruption	N-D
Execute	Cause deterioration/ destruction of critical information system components and functions. [See CTF: Destroy hardware / software / data]	Internal network, internal shared or infrastructure services, authorized action of privileged user	Degradation, Interruption	N-D
Execute	Cause integrity loss by creating, deleting, and/or modifying data on publicly accessible information systems (e.g., web defacement).	External network	Corruption, Modification, or Insertion	D-P, D-D
Execute	Cause integrity loss by polluting or corrupting critical data. [See CTF: Alter data on the victim's system(s)]	Internal network, internal shared or infrastructure services, authorized action of privileged user, authorized action of non-privileged user, data	Corruption, Modification	D-P, D-D

CAL Stage	Adversary Behavior or Threat Event	Attack Vector(s)	Cyber Effect(s)	Selected Matrix Cells
Execute	Cause integrity loss by injecting false but believable data into organizational information systems.	Internal network, internal shared or infrastructure services, authorized action of privileged user, authorized action of non-privileged user, data	Insertion	D-P, D-D
Execute	Reduce or deny availability by jamming communications.	External network, trusted or partner network connection, internal network	Degradation, Interruption	N-D
Execute	Cause disclosure of critical and/or sensitive information by authorized users.	Internal network, internal shared or infrastructure services, authorized action of privileged user, social engineering	Exfiltration, Interception	N-D
Execute	Cause unauthorized disclosure and/or unavailability by spilling sensitive information.	Internal network, internal shared or infrastructure services, authorized action of privileged user, social engineering	Exfiltration, Interception	N-D
Execute	Transmit sensitive information from the internal network to an external destination covertly. [See CTF: Exfiltrate data / information and ATT&CK: Exfiltration]	External network, trusted or partner network connection, internal network	Exfiltration	N-D
Execute	Inject crafted network traffic.	External network, trusted or partner network connection, internal network	Corruption, Modification, or Insertion	N-D
Execute	Transmit messages to a targeted range of perimeter network addresses to deny service.	External network, trusted or partner network connection	Degradation, Interruption	N-D
Execute	Download sensitive information to information systems or devices used externally and reintroduced into the enterprise.	Internal network	Exfiltration, Interception	D-P
Execute	Obtain information by externally-located interception of wireless network traffic.	Internal network	Interception	

CAL Stage	Adversary Behavior or Threat Event	Attack Vector(s)	Cyber Effect(s)	Selected Matrix Cells
Execute	Obtain unauthorized access.	Internal network, internal shared or infrastructure services, authorized action of privileged user, authorized action of non-privileged user, social engineering	Unauthorized use	N-D
Execute	Obtain sensitive data/information from publicly accessible information systems.	External network	Exfiltration, Interception	
Execute	Obtain information by opportunistically stealing or scavenging information systems/components.	Supply chain, maintenance environment	Exfiltration, Interception	
Maintain	Obfuscate adversary actions. [See ATT&CK: Defense Evasion]	Internal network, internal shared or infrastructure services, authorized action of privileged user	Corruption, Modification	N-D

Threat models at the next level of detail will be based on stated assumptions about the operational and technical environments. Assumptions about the operational environment can include identification of critical mission or business functions, supporting tasks, and cyber resources needed to accomplish those tasks; the scope or scale at which defensive actions or technological changes can be made; and the management or governance structure for cyber decision making (in particular, which decisions are centralized). Assumptions about the technical environment can include identification of products, product suites, or standards for the classes and sub-classes of resources which are considered as targets.

At the next level of detail, a different taxonomy of threat events than the one offered by the CAL and NIST SP 800-30R1 in Table 15 may be more useful. See, for example, CAPEC, ATT&CK, and the CAL models for insider threats and supply chain threats discussed in Section 2.1.5.3.

5.3 Structuring Representative Threat Scenarios

A small set of highly general threat scenarios can serve as a starting point for development of more detailed, but still institution-independent, scenarios. These are:[25]

1. *Breach: An adversary obtains sensitive information from the institution's systems.* This scenario includes data breaches of personally identifiable information (PII), as well as large-scale exfiltration of proprietary information, trade secrets, or other highly sensitive information.
2. *Fraud: An adversary modifies or fabricates information on the institution's systems so that the institution will disburse money or transfer other assets at the adversary's*

[25] This list is adapted from [Bodeau 2017].

direction. This scenario focuses on fraudulent transactions resulting from cyber attack, and excludes fraud resulting from non-cyber methods.

3. *Misuse: An adversary modifies or fabricates software or configuration data on the institution's systems so that the adversary can direct their use (typically to resell capacity, as with botnet farms or cryptocurrency mining).* This scenario focuses on usurpation of resources, which is typically highly surreptitious.
4. *Destruction: An adversary modifies or destroys institutional assets in order to prevent the institution from accomplishing its primary business functions.* This scenario includes adversary denial, disruption, or subversion of business operations.
5. *Friendly Fire: An adversary deceives business area managers or cyber defense staff into taking operationally-disruptive actions.* This scenario focuses on modification or fabrication of business or configuration data, as well as on modification or disruption of business functions.
6. *Upstream Attack: An adversary compromises a supplier or partner in order to increase the institution's vulnerability to attack.* This scenario includes attacks on partner institutions as well as those in the institution's supply chain.
7. *Reputation Damage: An adversary disrupts institutional operations or fabricates information the institution presents to its constituency, damaging its reputation and the trust of its constituency.* This scenario is closely related to those involving disruption or denial of mission functions, but also includes modification of inessential but externally visible information or services in ways that undermine confidence in the institution.
8. *Stepping-Stone Attack: An adversary compromises the institution's systems in order to attack downstream entities (e.g., customers, customers of customers).* Like the preceding scenario, this scenario is related to those involving disruption of mission functions. However, it is also related to scenarios involving acquisition of sensitive information, or fraudulent transactions.
9. *Extortion: An adversary modifies or incapacitates business assets for financial gain (e.g., ransomware, distributed denial-of-service (DDoS) attack).* This scenario is closely related to those involving modification for purposes of fraud and for disruption or denial of business functions.

For each generic scenario, typical threat actors and their ultimate targets can be identified, as well as typical intermediate targets which must be compromised in the course of the attack.

The following table identifies representative building blocks for attacks or campaigns, derived from NIST SP 800-30R1. These summaries can be elaborated by selecting and tailoring the attack events identified in Table 15 as illustrated, and adding details related to targeting for FSS organizations. The next level of detail can leverage material from CAPEC and ATT&CK.

Table 16. Building Blocks for Threat Scenarios

Type	Approach	Typical Events or Behaviors	Cyber Effects
Conduct attack	Conduct communications interception attacks.	Perform perimeter network reconnaissance/scanning. Perform network sniffing of exposed networks.	Interception
Conduct attack	Conduct wireless jamming attacks.	Perform perimeter network reconnaissance/scanning. Perform network sniffing of exposed networks. Reduce or deny availability by jamming communications.	Degradation, Interruption
Conduct attack	Conduct attacks using unauthorized ports, protocols and services.	Perform perimeter network reconnaissance/scanning. Perform network sniffing of exposed networks. Exploit poorly configured or unauthorized information systems exposed to the Internet.	Degradation, Interruption
Conduct attack	Conduct attacks leveraging traffic / data movement allowed across perimeter.	Establish command and control (C2) channels to malware or compromised components. Compromise organizational information systems to facilitate exfiltration of data/information. Cause disclosure of critical and/or sensitive information by authorized users. *Or* Cause unauthorized disclosure and/or unavailability by spilling sensitive information. *Or* Transmit sensitive information from the internal network to an external destination covertly.	Degradation, Interruption Exfiltration, Interception
Conduct attack	Conduct simple Denial of Service (DoS) attack.	Perform perimeter network reconnaissance/scanning.	Degradation, Interruption
Conduct attack	Conduct Distributed Denial of Service (DDoS) attacks.	Perform perimeter network reconnaissance/scanning. Transmit messages to a targeted range of perimeter network addresses to deny service.	Degradation, Interruption
Conduct attack	Conduct targeted Denial of Service (DoS) attacks.	Install persistent and targeted sniffers on organizational information systems and networks. Cause degradation or denial of attacker-selected services or capabilities.	Degradation, Interruption
Conduct attack	Conduct physical attacks on organizational facilities.	(depends on physical characteristics of organizational facilities)	Degradation, Interruption
Conduct attack	Conduct physical attacks on infrastructures supporting organizational facilities.	(depends on physical characteristics of supporting infrastructures)	Degradation, Interruption

Type	Approach	Typical Events or Behaviors	Cyber Effects
Conduct attack	Conduct cyber-physical attacks on organizational facilities.	(depends on cyber-physical characteristics of organizational facilities)	Degradation, Interruption
Conduct attack	Conduct data scavenging attacks in a cloud environment.	Establish command and control (C2) channels to malware or compromised components. Exploit insecure or incomplete data deletion in multi-tenant environment. *Or* Violate isolation in multi-tenant environment.	Exfiltration, Interception
Conduct attack	Conduct brute force login attempts/password guessing attacks.	Establish or use a communications channel to the enterprise as a whole or to a targeted system. Deliver commands to a targeted system (e.g., login).	Unauthorized use
Conduct attack	Conduct non-targeted zero-day attacks.	(Depends on the enterprise architecture)	All
Conduct attack	Conduct externally-based session hijacking.	Perform network sniffing of exposed networks.	Interception
Conduct attack	Conduct internally-based session hijacking.	Perform network sniffing of exposed networks. *Or* Perform malware-directed internal reconnaissance.	Interception
Conduct attack	Conduct externally-based network traffic modification (man in the middle) attacks.	Perform network sniffing of external networks (e.g., ISPs) to which organizational networks are connected. Analyze network traffic based on network sniffing. Inject crafted network traffic.	Degradation, Interruption Corruption, Modification, or Insertion
Conduct attack	Conduct internally-based network traffic modification (man in the middle) attacks.	Analyze network traffic based on network sniffing. Inject crafted network traffic.	Degradation, Interruption Corruption, Modification, or Insertion
Conduct attack	Conduct outsider-based social engineering to obtain information.	Gather information using open source discovery of organizational information. Craft psychological manipulation attacks on key staff.	Exfiltration, Interception
Conduct attack	Conduct insider-based social engineering to obtain information.	Craft psychological manipulation attacks on key staff.	Exfiltration, Interception

Type	Approach	Typical Events or Behaviors	Cyber Effects
Conduct attack	Conduct attacks targeting and compromising personal devices of critical employees.	Gather information using open source discovery of organizational information. Craft spear phishing attacks. *Or* Create counterfeit/spoof web site. Exploit known vulnerabilities in mobile systems (e.g., laptops, PDAs, smart phones). Compromise information systems or devices used externally and reintroduced into the enterprise. Compromise organizational information systems to facilitate exfiltration of data/information. *Or* Download sensitive information to information systems or devices used externally and reintroduced into the enterprise.	Corruption, Modification, or Insertion Exfiltration, Interception
Conduct attack	Conduct supply chain attacks targeting and exploiting critical hardware, software, or firmware.	Gather information using open source discovery of organizational information. Create and operate false front organizations to inject malicious components into the supply chain. *Or* Compromise systems in another organization to establish a presence in the supply chain. Insert counterfeit or tampered hardware into the supply chain.	Corruption, Modification, or Insertion
Coordinate campaign	Coordinate a campaign of multi-staged attacks (e.g., hopping).	Insert targeted malware into organizational information systems and information system components. Exploit vulnerabilities on internal organizational information systems.	All
Coordinate campaign	Coordinate a campaign that combines internal and external attacks across multiple information systems and information technologies.	[Other scenarios can be used as building blocks]	All
Coordinate campaign	Coordinate campaigns across multiple organizations to acquire specific information or achieve desired outcome.	Compromise systems in a partner organization. *Or* Compromise information systems or devices used externally and reintroduced into the enterprise. *Or* Compromise systems in another organization to establish a presence in the supply chain. Establish or use a communications channel to the enterprise as a whole or to a targeted system. Insert targeted malware into organizational information systems and information system components.	All

Type	Approach	Typical Events or Behaviors	Cyber Effects
Coordinate campaign	Coordinate a campaign that spreads attacks across organizational systems from existing presence.	Establish command and control (C2) channels to malware or compromised components. Violate isolation in multi-tenant environment. *Or* Exploit vulnerabilities on internal organizational information systems.	All
Coordinate campaign	Coordinate a campaign of continuous, adaptive and changing cyber attacks based on detailed surveillance.	[Other scenarios can be used as building blocks]	All
Coordinate campaign	Coordinate cyber attacks using external (outsider), internal (insider), and supply chain (supplier) attack vectors.	[Other scenarios can be used as building blocks]	All

6 Conclusion

This report presents a survey and assessment of cyber threat modeling frameworks and methodologies. The assessment was driven by the scope of desired uses for a cyber threat model identified by the NGCI Apex program – risk management, cyber wargaming within an organization and across a sector or sub-sector, technology foraging, and technology evaluation. The focus was on the financial services sector (FSS), and on cyber threats targeting or exploiting enterprise IT, since the FSS depends so heavily on it. The desired uses draw upon different concepts, and the NGCI Apex program considers a range of scopes, from information system to critical infrastructure sector. Therefore, it is unsurprising that no single model or modeling framework surveyed covers all the concepts needed for all the uses or the full range of scopes. This report has presented an initial framework and high-level model, tailored from NIST SP 800-30R1 and drawing from numerous other surveyed sources, for use by the NGCI Apex program. The initial framework is designed to support the development of models for a variety of purposes, and at levels of detail ranging from high-level to instantiated.

The initial framework and model presented in this report may serve as a resource for other critical infrastructure sectors, as well as for the FSS. However, other critical infrastructure sectors depend heavily on operational technology. Even organizations in the FSS depend – or will increasingly depend – on cyber-physical systems (e.g., automated teller machines) and operational technology; for example, convergence between Enterprise IT and building access and control systems can increase efficiency and decrease operating costs. Therefore, cyber threat modeling for cyber-physical systems, operational technology, and the Internet of Things is an area of future work.

Appendix A Modeling Constructs

Table 17 presents the threat modeling constructs discussed in Section 5. For some of the constructs, whether the construct is included in a threat model and the set of possible values will depend on other aspects of the context in which the threat model will be used, in particular the technical context (e.g., architecture, technical standards, products). For others, whether the construct is included in a threat model and the set of possible values will depend on the scope or scale to be represented by the threat model, and the purpose the threat model is intended to serve.

As discussed in Section 4.3, the threat modeling framework needs to support the development of three levels of models:

- *high-level* to support risk assessment, gap identification, and high-level wargaming, as well as technology foraging and profiling
- *detailed* to support more nuanced risk assessment and gap identification, more detailed cyber wargaming, and high-level playbook development, as well as representational testing
- *instantiated* to support detailed cyber wargaming and playbook development, as well as operational testing.

Table 17. Threat Modeling Constructs

Term	Definition	Relationships	Values	Use(s)
Adversary	An adversarial **threat source**	Is a **threat source**. Attributes include capabilities, intent, targeting, and sub-attributes of these.	Scope-dependent. Sector or nation: [DSB 2013] System, mission, or organization: [Intel 2015]	High-level
Asset	Something of value	Has an **asset type**.	Depends on system model.	Detailed Instantiated
Asset type	Class of **asset**	Has a **location**.	Scope-dependent; also depends on system model. For an organization, asset classes are defined in the Cyber Defense Matrix or Section 5.1.2	Detailed Instantiated
Attack phase	A category of **threat events** with a common intended effect	A stage in a campaign or an attack lifecycle (not necessarily cyber). Used in developing or describing a **threat scenario** or characterizing a **threat event**.	Reconnaissance, weaponize, deliver, exploit, control, execute, maintain. See Section 2.1.5.3 for a discussion of other cyber attack lifecycles or cyber kill chains.	High-level Detailed

Term	Definition	Relationships	Values	Use(s)
Attack surface	An area (in a representation of a system, organization, sector or region) where vulnerabilities or weaknesses are exposed	Is exposed to a **threat source**. Different attack surfaces can be identified with **attack vectors**.	Scope dependent (for a system, can include development and maintenance environments; for an organization, can include partner, customer, or supplier organizations or the interfaces with these). For a system, attack surfaces can be categorized as human, physical, and technical; technical attack surfaces can be categorized in terms of interfaces between architectural layers in the system.	Detailed Instantiated
Attack vector	A general approach to achieving an effect	Used by a **method**. Used in a **threat event**. Takes advantage of the exposure of a type of, or a region in, an attack surface.	Can be categorized as cyber, physical, or human. See Section 5.1.3.	All
Behavior	Activity or set of activities of a system, organization, group, or individual	Can be a **threat event**; if so, typically modified by "adverse."	Scope-dependent. Malicious cyber activities [NSTC 2016] are a class of behavior.	High-level
Capability	The factor or set of factors which enable an adversary to cause a threat event	Attribute of **adversary**. Sub-attributes include **resources** and **methods**.	For an adversary targeting a system, mission, or organization, [NIST 2012] defines five levels. Cyber Prep also defines five levels; [DSB 2013] defines six.	High-level (Detailed uses sub-attributes.)
Concern for Stealth	Consideration given to the avoidance of discovery or exposure	Attribute of **intent**.	None, limited, moderate, high, or very high. See Table 8. [Intel 2007]: Overt, covert, clandestine, don't care	All
Consequence	The ultimate result of an event	When modified by "adverse" or "undesirable," refers to a form of harm; thus, result of a **threat** or a **threat event**. Has a **consequence type**. May also have a stakeholder and a severity.	Scope-dependent. In the context of security, undesirable consequences can be categorized in terms of security objectives not met (confidentiality, integrity, availability).	High-level Detailed (Instantiated may specify cyber effects.)

Term	Definition	Relationships	Values	Use(s)
Consequence type	The general class or characteristic of a **consequence**	Attribute of **consequence**	Financial loss, reputation damage, liability, physical or non-physical harm to individuals. See Table 9.	High-level Detailed
Cyber effect	An effect of a **threat event** in cyberspace	Attribute of adversary **intent** (intended cyber effects) or result of a **threat event**.	Degradation, interruption, modification, fabrication / insertion, unauthorized use / usurpation, or interception / observation [Temin 2010]. Can be categorized using STRIDE [Kohnfelder 1999], [Shostack 2014]. [Intel 2007]: copy, destroy, injure, take, don't care	Detailed Instantiated (may identify individual assets targeted or affected)
Duration	Period of time over which a condition exists, or over which a **threat event**, **attack phase**, or **threat scenario** occurs	Attribute of **exposure** (condition). Attribute of **threat event**. Attribute of **threat source** (**structural failure** or **environmental**), when identified with **threat event**.	Draw from historical data where possible.	All
Effect	The immediate result of a **threat event**	Caused by a **threat event**. Has an **effect type**. Can be detected or experienced at a **location**. Has a **scope or scale**.	See effect type and cyber effect.	All
Effect type	The class of an **effect**	Attribute of **effect**.	Cyber effect, non-cyber effect. Non-cyber effects can be categorized as physical, social (e.g., privacy-related, reputation-related), economic, or political.	All
Exposure	Accessibility to a **threat event** or a **threat actor**	Attribute of a vulnerability, weakness, or **attack surface**.	None, low, moderate, high. Meaningful in the context of a system model. Can be used to screen out threat events.	Detailed Instantiated
Financial resources	Money an **adversary** can use to improve other capabilities	Sub-type of **resource**. Can be used to improve **technological resources**, **informational resources**, increase the number of **personnel**, or build **relationships**.	Levels can be defined, but are dependent on assumptions about adversary tier [DSB 2013] or type [Intel 2007]. [Bodeau 2014]: Can have an associated scope.	High-level

Term	Definition	Relationships	Values	Use(s)
Form of error	Category of **threat events** caused by human error	Equivalent of **attack vector**, for human error threat source.	Physical / kinetic error, system configuration error, user input error, erroneous value transmitted, software development error resulting in vulnerability, integration error resulting in vulnerability	All (if human error, or adversary taking opportunistic advantage of human error, is in scope)
Frequency	Number of times an event or circumstance occurs per unit time	Attribute of **threat event**; attribute of **form of error**, **type of structural failure**, or **type of environmental threat**.	Draw from historical data where possible.	All (risk assessment)
Goal or Motivation	The type of benefit or harm an **adversary** seeks to achieve	Attribute of an **adversary** or of **intent**. Can have attributes of level or degree of motivation and motivational aspects. Can be identified with **consequence type**.	Financial gain, personal motives, geopolitical advantage, stepping-stone. See Table 9. [Intel 2015]: ideology, dominance, accidental, disgruntlement, unpredictable, personal financial gain, organizational gain, personal satisfaction, notoriety, and coercion. Also defines motivational aspects (defining motivation, co-motivation, subordinate motivation, binding motivation, and personal motivation).	High-level Detailed
Informational resources	Information an **adversary** can use to cause a **threat event**	Sub-type of **resource**, used in a **threat event**. Can include intelligence requiring skill to analyze; thus, informational resources are related to adversary **personnel**.	[Bodeau 2014]: Can have an associated scope.	High-level Detailed
Intent	The factor or set of factors which lead an **adversary** to act or not to act	Attribute of an **adversary**. Has attributes of **goal or motivation**, intended **cyber effects**, **scope of scale**, timeframe, persistence, concern for stealth, opportunism.	For an adversary targeting a system, mission, or organization, [NIST 2012] defines five levels.	High-level Detailed

Term	Definition	Relationships	Values	Use(s)
Location	Where a **threat event** occurs	For adversarial threats, may be identified with **attack vector**.	Depends on the scope and purpose of the threat model. For a detailed or instantiated model, also depends on the system model.	All
Method	A type of activity an **adversary** performs	Attribute of **capability**. Use **attack vectors**. Can have an intended **scope**.	Five levels defined in Table 9. Can be categorized using STRIDE. [Bodeau 2014]: Can be characterized as cyber, non-cyber, or partially cyber; can have an intended scope. [OWASP 2016]: Attack Category	High-level Detailed (Instantiated uses descriptions of specific TTPs.)
Opportunism	Ability or desire to take advantage of opportunities created by events not caused by the **adversary**	Attribute of **intent**. Used in the development of a **threat scenario** involving multiple threat sources.	Levels can be defined.	High-level Detailed
Persistence	Commitment to continue activities	Attribute of **intent**. Conversely, ease with which an adversary can be discouraged.	None, limited, persistent, or strategically persistent. See Table 10.	High-level Detailed
Personnel	The individuals an **adversary** can use to cause **threat events**	Sub-type of **resource**. Personnel require expertise to use **technological and informational resources**.	[Intel 2007]: Defines skill levels (none, minimal, operational, adept).	Detailed
Relationship	An affiliation or conflict with another entity which can affect an **adversary**'s ability to cause a **threat event**	Sub-type of **resource**. Can be used when defining a **threat scenario** involving multiple actors.	[Bodeau 2014]: Defines spectrum of relationships (collaboration, coordination, cooperation, friction avoidance, communication, mutual indifference, observation, frictional conflict, competition, contention, and coercion). [Intel 2007]: Defines level of organization (individual, club, contest, team, organization, government).	High-level Detailed
Resources	A set of assets which can be used to achieve a goal. As an attribute of **adversary capability**, what an **adversary** can use to cause a **threat event**	Attribute of **capability**. Sub-types include technological resources, information resources, financial resources, personnel, and relationships.	Five levels defined in Table 12.	High-level

Term	Definition	Relationships	Values	Use(s)
Scope or Scale of Effects	Range over which **effects** are experienced or evidenced	Attribute of **effect**, for all **effect types**. Attribute of **threat source**, of **structural failure** and **environmental threat** directly, and of adversary **targeting**.	Five values defined in Table 11. Derived from [Bodeau 2014, 2017].	High-level Detailed
Stage of Cyber Attack Lifecycle	See **attack phase**			
Targeting	The factor or set of factors which lead an **adversary** to select a target or **target type**	Attribute of **adversary**. Sub-types include **scope** and **target types**.	For an adversary targeting a system, mission, or organization, [NIST 2012] defines five levels.	High-level Detailed
Target Type	Type of **resources** targeted by an adversary	Attribute of **targeting**.	Scope-dependent and dependent on technical and operational contexts. For NGCI Apex, includes devices, network components, enterprise services, applications, data, and people. Can also include facilities and suppliers.	High-level Detailed
Technological resources	Tools, technologies, and malware an **adversary** can use to cause a **threat event**	Sub-type of **resource**, used in a **threat event**. Note that a given adversary may lack the skill to use a given tool; thus, technological resources are related to **personnel**. Can identify specific tools or malware.	Levels can be defined, or verbal characterizations can be used. STIX: Identify specific tools or malware. [Bodeau 2014]: Can have an associated scope.	High-level Detailed
Threat	Potential cause of harm	Refers to either a **threat source** or a **threat event**. Assumes an entity (e.g., an individual, group, organization, system, mission, sector, region, or nation) which could be harmed.	Context should make clear whether usage refers to a threat event, a threat source, a set of threat events which produce the same cyber effect(s) or consequence(s), or a set of similar threat sources (e.g., a DSB tier).	All

Term	Definition	Relationships	Values	Use(s)
Threat actor	An individual or group whose action or behavior produces a **threat event**	Is a **threat source**. Can be of either adversarial or human error type; if type is unspecified, assume adversarial.	For human error, can be defined in terms of role; e.g., privileged user, normal user, individual with physical access to facility, external actor, maintainer, developer / integrator. For adversarial, see Adversary.	All
Threat event	An event which could result in adverse or undesired **consequences**	Caused or initiated by a **threat source**. For adversarial threat events, uses an **attack vector**, is intended to produce an effect (usually a **cyber effect**) on a target; often can be characterized by **attack phase**. For human error threat sources, can be characterized by **form of error**.	Scope-dependent and dependent on technical and operational contexts. ATT&CK, CAPEC, [Wynn 2011], [NIST 2012], [Miller 2013], [NIST 2016b], [OWASP 2016]	All
Threat scenario	A set of discrete **threat events**, associated with a specific **threat source** or multiple threat sources, partially ordered in time	Consists of **threat events**, caused by one or more **threat sources**, resulting in one or more **consequences**.	Constructed from selected or populated values of threat sources, threat events, and consequences, using values of attributes.	All
Threat source	An entity, agent, or circumstance which could cause or produce a **threat event**	Has a **threat type**. Causes or produces a **threat event**. Attributes depend on type. Is involved in (i.e., causes one or more threat events in) one or more **threat scenarios**.	May be listed, as in Intel TAL.	All
Threat type	Type of **threat source**	Has characteristics (types of attributes), depending on value. For non-adversarial**, scope or scale of effects**, **frequency**, and types of resources affected.	Adversarial, non-adversarial (structural failure, accidental / human error, environmental) [NIST 2012]	All (used to determine scope of threat model)

Term	Definition	Relationships	Values	Use(s)
Timeframe	Period of time over which an **adversary** plans and acts	Attribute of **intent**.	One-time, episodic, sustained, or enduring. See Table 10.	High-level Detailed
TTP	See **method**			
Type of environmental threat	Classes of **threat** inherent in the physical environment	Class of **threat source**; has **scope**, **frequency** and **duration**.	Scope-dependent and dependent on technical context. Can include natural or man-made disaster, unusual natural event, and infrastructure failure / outage; see Table D-2 of [NIST 2012]	High-level Detailed (if in scope)
Type of structural failure	(Self-explanatory)	Class of **threat source**; has **scope**, **frequency** and **duration**.	Scope-dependent and dependent on technical context. Can include IT equipment, environmental controls, and software; see Table D-2 of [NIST 2012]	High-level Detailed (if in scope)

List of Acronyms

Acronym	Definition
ABA	American Bankers Association
ACM	Association for Computing Machinery
AFCEA	Armed Forces Communications and Electronics Association
AO	Authorizing Official
APT	Advanced Persistent Threat
ARDA	Advanced Research and Development Activity
ATM	Automated Teller Machine
ATT&CK™	Adversarial Tactics, Techniques, and Common Knowledge
AVOIDIT	Attack Vector, Operational Impact, Defense, Information Impact, and Target
BACS	Building Access and Control System
BOE	Bank of England
BYOD	Bring Your Own Device
C2	Command and Control
CADAT	Cause, Action, Defense, Analysis, and Target
CAF	Canadian Armed Forces
CAL	Cyber Attack Lifecycle
CAPEC™	Common Attack Pattern Enumeration and Classification
CART	Cyber Apex Review Team
CC	Common Criteria
CCD	Cooperative Cyber Defense
CDM	Continuous Diagnostics and Mitigation
CERT	Computer Emergency Response Team
CI	Critical Infrastructure
CIS	Center for Internet Security
CKC	Cyber Kill Chain

Acronym	Definition
CNSS	Committee on National Security Systems
CNSSI	Committee on National Security Systems Instruction
COBIT	Control Objectives for Information and Related Technologies
COE	Center of Excellence
COI	Community of Interest
CP	Cyber Prep
CPS	Cyber-Physical System
CRM	Customer Relationship Management
CSA	Cloud Security Alliance
CS&C	DHS Office of Cybersecurity and Communications
CSF	(NIST) Cybersecurity Framework
CSS	(NSA) Central Security Service
CTF	Cyber Threat Framework
CTI	Cyber Threat Intelligence
CVE	Common Vulnerabilities and Exposures
CWE	Common Weakness Enumeration
DACS	Describing and Analyzing Cyber Strategies
DAG	Directed Acyclic Graph
DASD	Deputy Assistant Secretary of Defense
DDoS	Distributed Denial of Service
DHCP	Dynamic Host Configuration Protocol
DHS	Department of Homeland Security
DLL	Dynamic-Link Library
DNS	Domain Name System
DoD	Department of Defense
DoS	Denial of Service
DRDC	Defence Research and Development Canada

Acronym	Definition
DREAD	Damage, Reliability [of an attack – sometimes rendered as reproducibility], Exploitability, Affected Users, and Discoverability
DSB	Defense Science Board
DT&E	Developmental Test and Evaluation
EIT	Enterprise IT
ENISA	European Union Agency for Network and Information Security
ERM	Enterprise Risk Management
FAIR	Factor Analysis of Information Risk
FBI	Federal Bureau of Investigation
FFIEC	Federal Financial Institutions Examination Council
FFRDC	Federally Funded Research and Development Center
FIPS	Federal Information Processing Standards
FIRST	Forum of Incident Response and Security Teams
FS	Financial Service
FS-ISAC	Financial Sector Information Sharing and Analysis Center
FSS	Financial Services Sector
FSSCC	Financial Services Sector Coordinating Council
.GovCAR	.Gov Cybersecurity Architecture Review
GPS	Global Positioning System
HP	Hewlett Packard
HR	Human Resources
HSSEDI	Homeland Security Systems Engineering & Development Institute
HVAC	Heating, Ventilation, and Air Conditioning
IAEA	International Atomic Energy Agency
IC	Intelligence Community
ICS	Industrial Control System
IdAM	Identity and Access Management

Acronym	Definition
IDS	Intrusion Detection Systems
IEEE	Institute of Electrical and Electronics Engineers
IoT	Internet of Things
IP	Internet Protocol
IS	Information Security
ISACA	Information Systems Audit and Control Association
ISO	International Organization for Standardization
ISP	Internet Service Provider
IS	Information Security
IT	Information Technology
JTF	Joint Task Force
M&S	Modeling and Simulation
MITC	Man-in-the-Cloud
MORDA	Mission Oriented Risk and Design Analysis
MRM	Model Risk Management
N/A	Not Applicable
NATO	North Atlantic Treaty Organization
NCR	National Cyber Range
NCSC	National Cyber Security Centre
NGCI	Next Generation Cyber Infrastructure
NIAP	National Information Assurance Partnership
NIEM	National Information Exchange Model
NIST	National Institute of Standards and Technology
NISTIR	NIST Interagency Report
NSA	National Security Agency
NSCSAR	NIPRNet/SIPRNet Cyber Security Architecture Review
NSTC	National Science and Technology Council

Acronym	Definition
NUARI	Norwich University Applied Research Institutes
O&M	Operations and Maintenance
OASIS	Organization for the Advancement of Structured Information Standards
OCC	Office of the Comptroller of the Currency
OCTAVE	Operationally Critical Threat, Asset, and Vulnerability Evaluation
ODNI	Office of the Director of National Intelligence
OFR	Office of Financial Research
OMG	Object Management Group
OPSEC	Operations Security
OS	Operating System
OSA	Open Systems Architecture
OWASP	Open Web Application Security Project
OT	Operational Technology
PASTA	Process for Attack Simulation & Threat Analysis
PDA	Personal Digital Assistant
PII	Personally Identifiable Information
PMO	Program Management Office
PMP	Project Management Plan
PwC	PricewaterhouseCoopers
PWG	Public Working Group
QA	Quality Assurance
R&D	Research and Development
RCM	Research Coordination Meeting
RFP	Request for Proposals
RMF	Risk Management Framework
ROI	Return on Investment
S&T	Science and Technology Directorate

Acronym	Definition
SCADA	Supervisory Control and Data Acquisition
SDLC	System Development Lifecycle
SIMEX	Simulation Experiment
SLA	Service Level Agreement
SME	Subject Matter Expert
SoS	System-of-Systems
SP	Special Publication
STIX™	Structured Threat Information eXpression
STRIDE	Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege
STRUM	Standard Technical Reports Using Modules
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TAL	(Intel) Threat Agent Library
TARA	(Intel) Threat Agent Risk Assessment (MITRE) Threat Assessment and Remediation Analysis
TAXII™	Trusted Automated eXchange of Indicator Information
TTPs	Tactics, Techniques, and Procedures
TTX	Tabletop Exercise
VM	Virtual Machine
UK	United Kingdom
UML	Unified Modeling Language
US-CCU	U.S. Cyber Consequences Unit
WASC	Web Application Security Consortium

Glossary

Glossary Term	Glossary Definition
Advanced Persistent Threat (APT)	An adversary with sophisticated levels of expertise and significant resources, allowing it through the use of multiple different attack vectors (e.g., cyber, physical, and deception) to generate opportunities to achieve its objectives. Such objectives are typically (1) to establish and extend footholds within the information technology infrastructure of organizations for purposes of continually exfiltrating information, and/or (2) to undermine or impede critical aspects of a mission, program, or organization, or place itself in a position to do so in the future. Moreover, the advanced persistent threat pursues its objectives repeatedly over an extended period of time, adapting to a defender's efforts to resist it, and with determination to maintain the level of interaction needed to execute its objectives. [NIST 2011]
Adversarial threat	See Threat actor.
Adversary	Individual, group, organization, or government that conducts or has the intent to conduct detrimental activities. [NIST 2012] See Threat actor.
Attack	Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself. [NIST 2012] [CNSS 2015]
Attack surface	Accessible areas where weaknesses or deficiencies in information systems (including the hardware, software, and firmware components) provide opportunities for adversaries to exploit vulnerabilities. [NIST 2013] Aspects of systems, missions, or organizations (including operational, development, and maintenance environments) that an adversary can reach and that could contain vulnerabilities.
Attack tree	A branching, hierarchical data structure that represents a set of potential approaches to achieving an event in which system security is penetrated or compromised in a specified way. [CNSS 2015]
Attack vector	A segment of the entire pathway that an attack uses to access a vulnerability. Each attack vector can be thought of as comprising a *source* of malicious content, a potentially vulnerable *processor* of that malicious content, and the nature of the malicious *content* itself. [NIST 2016] A general approach to achieving cyber effects. Can include cyber, physical or kinetic, social engineering, and supply chain attacks. [Bodeau 2014]

Glossary Term	Glossary Definition
Campaign	A grouping of adversarial behaviors that describes a set of malicious activities or attacks (sometimes called waves) that occur over a period of time against a specific set of targets. [OASIS 2017]
Cyberspace	The interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries. [CNSS 2015]
Cyber attack	A deliberate effort to disrupt, steal, alter, or destroy data stored on IT systems. [OFR 2017]
Risk Management Framework (RMF)	(1) The six-step process for managing information system security risk defined in NIST SP 800-37. (2) The multi-tiered approach to information security risk management defined in NIST SP 800-39 and implemented using related standards (FIPS 199 and FIPS 200) and guidance (including NIST SP 800-37, NIST SP 800-53R4, NIST SP 800-53AR4, and NIST SP 800-160). Note: In this document, the broader definition – (2) – is used.
Supply chain	A system of organizations, people, activities, information, and resources, possibly international in scope, that provides products or services to consumers. [CNSS 2015]
Supply chain attacks	Attacks that allow the adversary to utilize implants or other vulnerabilities inserted prior to installation in order to infiltrate data, or manipulate information technology hardware, software, operating systems, peripherals (information technology products) or services at any point during the life cycle. [CNSS 2015] Attacks inserted or carried out after installation, by means of access granted to a supplier for diagnostic or maintenance purposes could also be considered supply chain attacks.
Tactics, Techniques, and Procedures (TTPs)	The behavior of an actor. A tactic is the highest-level description of this behavior, while techniques give a more detailed description of behavior in the context of a tactic, and procedures an even lower-level, highly detailed description in the context of a technique. [NIST 2016c]. In addition to behaviors actually used during particular cyber attacks, tactics, techniques, and procedures can refer to the methods known to be available to or within the capabilities of an actor.
Technology foraging	A process of identifying, locating and evaluating existing or developing technologies, products, services and emerging trends of interest (https://www.dhs.gov/science-and-technology/technology-foraging)

Glossary Term	Glossary Definition
Threat	Events that could cause harm to the confidentiality, integrity, or availability of information or information systems, through unauthorized disclosure, misuse, alteration, or destruction of information or information systems. [FFIEC 2016] Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service. [NIST 2012]
Threat actor	Individuals, groups, organizations, or states that seek to exploit the organization's dependence on cyber resources (i.e., information in electronic form, information and communications technologies, and the communications and information-handling capabilities provided by those technologies). [NIST 2012], Table D-2 An actual individual, group, or organization believed to be operating with malicious intent. [OASIS 2017] An individual or group posing a threat. [NIST 2016c]
Threat event	An event or situation that has the potential for causing undesirable consequences or impact. [NIST 2012]
Threat Scenario	A set of discrete threat events, associated with a specific threat source or multiple threat sources, partially ordered in time. Synonym for *Threat Campaign*. [NIST 2012]

List of References

1. Amini, A., Jamil, N., Ahmad, A.R., and Z'aba, M.R. 2015. "Threat Modeling Approaches for Securing Cloud Computing," July 25, 2015. Journal of Applied Sciences, 15: 953-967.

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

3. Applegate, S.D., and Stavrou, A. 2013. "Towards a Cyber Conflict Taxonomy," Proceedings of the 5th International Conference on Cyber Conflict, NATO CCD COE Publications, Tallinn. 2013. https://ccdcoe.org/cycon/2013/proceedings/d3r1s2_applegate.pdf

4. Assante, M. and Lee, R. 2015. "The Industrial Control System Cyber Kill Chain," October 2016. https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297

5. Bank of England. 2016. "CBEST Intelligence-Led Testing, An Introduction to Cyber Threat Modelling," Version 2.0, 2016. http://www.bankofengland.co.uk/financialstability/fsc/Documents/anintroductiontocbest.pdf

6. 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/

7. Bedell, C. 2016. "7 Steps to Enhance Your Cyber Defense," InfoSecurity Professional, July/August 2016, pp. 18-22.

8. Beyst, B. 2016. "Threat Modeling: Past, Present, and Future." April 15, 2016. https://threatmodeler.com/2016/04/15/application-threat-modeling-past-present-future/

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

10. Bodeau, D., Graubart, R. and Heinbockel, W. 2013b. "Mapping the Cyber Terrain: Enabling Cyber Defensibility Claims and Hypotheses to Be Stated and Evaluated with Greater Rigor and Utility (MTR130433)," November 2013, The MITRE Corporation, Bedford, MA. http://www.mitre.org/sites/default/files/publications/mapping-cyber-terrain-13-4175.pdf

11. Bodeau, D., and Graubart, R. 2014. "A Framework for Describing and Analyzing Cyber Strategies and Strategic Effects, MTR 140346, PR 14-3407," February 2014, The MITRE Corporation, Bedford, MA.

12. Bodeau, D., and Graubart, R. 2017. "Cyber Prep 2.0: Motivating Organizational Cyber Strategies in Terms of Threat Preparedness, MTR 150264, PR 16-0939," May 2017, The MITRE Corporation, Bedford, MA. https://www.mitre.org/sites/default/files/publications/16-0939-motivating-organizational-cyber-strategies.pdf

13. Booth, G., Soknack, A., and Somayaji, A. 2013. "Cloud Security: Attacks and Current Defenses," 8th Annual Symposium on Information Assurance (ASIA'13), June 4-5, 2013.

14. Buckshaw, D.L., et al. 2005. "Mission oriented risk and design analysis of critical systems," *Military Operations Research*, Vol. 10, Number 2.

15. Burns, S.F. 2005. "Threat Modeling: A Process to Ensure Application Security," SANS Institute Reading Room, January 5, 2005. https://www.sans.org/reading-room/whitepapers/securecode/threat-modeling-process-ensure-application-security-1646

16. Caralli, R.A., et al. 2007. Carnegie Mellon University - Software Engineering Institute, "OCTAVE Allegro: Improving the Information Security Risk Assessment Process," May 2007. http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=8419 or http://resources.sei.cmu.edu/asset_files/TechnicalReport/2007_005_001_14885.pdf

17. Center for Internet Security (CIS). 2016. "The CIS Community Attack Model." November 28, 2016. https://www.cisecurity.org/white-papers/cis-community-attack-model/

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

19. 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

20. Committee on National Security Systems (CNSS). 2014. "Security Categorization and Control Selection for National Security Systems (CNSSI No. 1253)." 27 March 2014. http://www.dss.mil/documents/CNSSI_No1253.pdf

21. Costa, D.L., et al. 2016. "An Insider Threat Indicator Ontology, CMU/SEI-2016-TR-007," May 2016. https://resources.sei.cmu.edu/asset_files/TechnicalReport/2016_005_001_454627.pdf

22. CNSS. "Committee on National Security Systems (CNSS) Glossary, CNSSI No. 4009," 26 April 2015. https://www.cnss.gov/CNSS/openDoc.cfm?+gFFwRcMwh5SYHeOUWSIiw==

23. Deloitte. 2015. "Quantum Dawn 3 After-Action Report." 2015. https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-risk-quantum-dawn-3-after-action-report.pdf

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

25. Department of Defense (DoD). 2013. Office of the DASD (DT&E), "Guidelines for Cybersecurity DT&E, version 1.0," April 19, 2013. https://www.hsdl.org/?view&did=736765

26. Department of Defense (DoD). 2018. "Cybersecurity Test and Evaluation Guidebook Version 2.0." April 25, 2018. https://www.acq.osd.mil/dte-trmc/docs/CSTE%20Guidebook%202.0_FINAL%20(25APR2018).pdf

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

28. DSB. 2017. "DSB Task Force on Cyber Supply Chain," February, 2017. https://insidedefense.com/sites/insidedefense.com/files/documents/mar2017/03132017_dsb.pdf

29. ENISA. 2016. "ENISA Threat Taxonomy: A tool for structuring threat information, Initial Version 1.0," January 2016. https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/etl2015/enisa-threat-taxonomy-a-tool-for-structuring-threat-information

30. Espenschied, J. and Gunn, A. 2012. "Threat Genomics," August 10, 2012. http://www.securitymetrics.org/attachments/Metricon-7-paper-Threat-Genomics-Espenschied-Gunn-2012.pdf

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

32. 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, April 2014.

33. FIRST. 2015. "Common Vulnerability Scoring System v3.0: Specification Document," December 15, 2015. https://www.first.org/cvss/specification-document

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

35. Fox-IT. 2016. "Financial Sector and the Evolving Threat Landscape: Live Cyber Exercise, RSA Conference Learning Labs," March 22, 2016. https://www.rsaconference.com/writable/presentations/file_upload/lab1-w13_financial_sector_and_the_evolving_threat_landscape_live_cyber-exercise_-_follow_up.pdf

36. Franz, M. D. 2005. "ThreatMind," November 2005. http://threatmind.sourceforge.net/

37. Freund, J. and Jones, J. 2015. *Measuring and Managing Information Risk*, Elsevier, 2015.

38. FSSCC and ABA. 2016. "2016 Cyber Insurance Buying Guide," April 18, 2016. https://www.aba.com/Tools/Function/Documents/2016Cyber-Insurance-Buying-Guide_FINAL.pdf or https://www.fsscc.org/files/galleries/FSSCC_Cyber_Insurance_Purchasers_Guide_FINAL-TLP_White.pdf

39. Giakouminakis, T. 2013. "Understanding and Building Threat Models," RSA Conference, Asia Pacific 2013. http://www.rsaconference.com/writable/presentations/file_upload/sec-t03_final3.pdf

40. Greitzer, F.L, Kangas, L.J., Noonan, C.F., Brown, C.R., and Ferryman, T. 2013. "Psychosocial Modeling of Insider Threat Risk Based on Behavioral and Word Use Analysis," e-Service Journal, Vol. 9, No. 1, Fall 2013.

41. Hahn, A., Thomas, R., Lozano, I., and Cardenas, A. 2015. "A multi-layered and kill-chain based security analysis framework for cyber-physical systems," International Journal of Critical Infrastructure Protection 11 (2015), pp. 39-50.

42. Hardy, G.M. 2012. "Beyond Continuous Monitoring: Threat Modeling for Real-time Response," SANS Institute Reading Room, October 2012. https://uk.sans.org/reading-room/whitepapers/analyst

43. Heartfield, R., and Loukas, G. 2015. "A Taxonomy of Attacks and a Survey of Defence Mechanisms for Semantic Social Engineering Attacks," ACM Computing Surveys, Vol. 48, No. 3, Article 37, December 2015.

44. Howard, M., and LeBlanc, D. 2003. *Writing Secure Code*, Microsoft Press, 2003.

45. Hutchins, E.M., Cloppert, M.J., and Amin, R.M. 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 2011), 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

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

47. International Organization for Standardization (ISO). 2103. "ISO/IEC 27001 - Information security management," Second Edition, 2013.

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

49. Intel. 2009. IT@Intel White Paper, Intel Information Technology Security "Prioritizing Information Security Risks with Threat Agent Risk Assessment," December 2009. http://media10.connectedsocialmedia.com/intel/10/5725/Intel_IT_Business_Value_Prioritizing_Info_Security_Risks_with_TARA.pdf

50. 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

51. Invincea. 2015. "Know Your Adversary: An Adversary Model for Mastering Cyber-Defense Strategies," November 30, 2015. http://www.ten-inc.com/presentations/invincea1.pdf

52. ISACA. 2009. "The Risk IT Framework," 2009.

53. ISACA. 2014. "Risk Scenarios: Using COBIT 5 for Risk," September 2014.

54. Kadivar, M. 2014. "Cyber-Attack Attributes," Technology Innovation Management Review, Vol. 4, No. 11, November 2014, pp. 22-27.

55. Kazim, M., and Evans, D. 2016. "Threat Modeling for Services in the Cloud," Proceedings of the 2016 IEEE Symposium on Service-Oriented System Engineering.

56. 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

57. 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

58. Kohnfelder, L. and Garg, P. 1999. "The threats to our products," Microsoft Interface, April 1, 1999. https://blogs.microsoft.com/cybertrust/2009/08/27/the-threats-to-our-products/.

59. 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, pages 1-38. November, 2014.

60. Kosten, S. 2017. "Moving Toward Better Security Testing of Software for Financial Services: A SANS Whitepaper," January 2017. https://www.sans.org/reading-room/whitepapers/analyst

61. Leblanc, D. 2007. "DREADful," August 14, 2007. https://blogs.msdn.microsoft.com/david_leblanc/2007/08/14/dreadful/

62. Lewis, E. 2012. "From the Physical to the Virtual – Threat Modeling the Landscape of Virtualization." August 29, 2012.

http://i.dell.com/sites/doccontent/business/smb/sb360/en/Documents/wp-desk-virt-threat-models.pdf

63. Magar, A. 2016. “State-of-the-Art in Cyber Threat Modeling Models and Methodologies,” March 2016. http://cradpdf.drdc-rddc.gc.ca/PDFS/unc225/p803699_A1b.pdf

64. Management Solutions. 2014. “Model Risk Management: Quantitative and Qualitative Aspects.” July 22, 2014. http://www.managementsolutions.com/PDF/ENG/Model-Risk.pdf

65. Mandiant. 2013. “APT1: Exposing One of China's Cyber Espionage Units.” February 18, 2013. https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf

66. Maybury, M., Chase, M., Cheikes, B., Brackney, D., Matzner, S., Hetherington, T., Wood, B., Sibley, C., Marin, J., Longstaff, T., Spitzner, L., Haile, H., Copeland, J., and Lewandowski, S. 2005. “Analysis and Detection of Malicious Insiders.” 2005. http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA456356

67. McCall, B. 2014. “An Overview of Threat Models for Virtualization and Cloud Computing (MTR 140312, PR 15-1743),” The MITRE Corporation, Bedford, MA. August 25, 2014.

68. 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

69. Miller, J. 2013. “Supply Chain Attack Framework and Attack Patterns,” MTR 140021, PR Case No. 14-0228, The MITRE Corporation. December 2013. https://www.mitre.org/sites/default/files/publications/supply-chain-attack-framework-14-0228.pdf

70. 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

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

72. The MITRE Corporation. 2013. “Threat Assessment and Remediation Analysis (TARA) Overview,” October 2013. https://www.mitre.org/sites/default/files/publications/pr-2359-threat-assessment-and-remediation-analysis.pdf

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

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

75. The MITRE Corporation. 2016b. “PRE-ATT&CK – Model to Improve Cyber Threat Detection Before Adversaries Compromise Your Network (PR 16-3852)” and “PRE-ATT&CK Briefing (PR 16-4128),” The MITRE Corporation, McLean, VA, November 30, 2016. https://attack.mitre.org/pre-attack/index.php/Main_Page

76. The MITRE Corporation. 2017. “ATT&CK Mobile Profile,” 2017. https://attack.mitre.org/mobile/index.php/Main_Page

77. Moore, A.P., Kennedy, K.A., and Dover, T.J. 2016. "Special Issue on Insider Threat Modeling and Simulation," Computational and Mathematical Organization Theory, Volume 22, Issue 3. September 2016.

78. Muckin, M. and Fitch, S.C. 2015. "A Threat-Driven Approach to Cyber Security; Methodologies, Practices, and Tools to Enable a Functionally Integrated Cyber Security Organization," Lockheed Martin Corporation, April 24, 2015. https://pdfs.semanticscholar.org/be09/f7a16eb4a379e698d8f42100fd8a91943a0c.pdf

79. Naegele, T. 2018. "CDM Program Starts to Tackle Complexities of Cloud," January 31, 2018. https://www.govtechworks.com/cdm-program/#gs.JnhqfhA

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

81. National Cyber Security Centre (NCSC). 2016. "Common Cyber Attacks: Reducing the Impact," January 2016. https://www.ncsc.gov.uk/file/1477/download?token=3n7aC5e_

82. National Institute of Standards and Technology (NIST). 2010. "Guide for Applying the Risk Management Framework to Federal Information Systems, NIST SP 800-37 Rev. 1." February 2010. http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf

83. NIST. 2011. "Managing Information Security Risk: Organization, Mission, and Information System View," NIST Special Publication 800-39, April 2011. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf

84. NIST. 2012. "Guide for Conducting Risk Assessments," NIST Special Publication 800-30, Revision 1, September 2012. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

85. NIST. 2012b. "Computer Security Incident Handling Guide," NIST Special Publication 800-61, Revision 2, August 2012. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

86. NIST. 2013. "Security and Privacy Controls for Federal Information Systems and Organizations," NIST Special Publication 800-53, Revision 4, April 2013. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

87. NIST. 2014. "Framework for Improving Critical Infrastructure Cybersecurity," Revision 1, February, 2014.

88. NIST. 2014b. "Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans," NIST SP 800-53A, Revision 4, December 2014. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf

89. NIST. 2016. "Guide to Data-Centric System Threat Modeling," Draft NIST Special Publication 800-154, March 2016. https://csrc.nist.gov/CSRC/media/Publications/sp/800-154/draft/documents/sp800_154_draft.pdf

90. NIST. 2016b. "Assessing Threats to Mobile Devices & Infrastructure: The Mobile Threat Catalogue," Draft NIST Interagency Report (NISTIR) 8144, September 2016. https://nccoe.nist.gov/sites/default/files/library/mtc-nistir-8144-draft.pdf

91. NIST. 2016c. "Guide to Cyber Threat Information Sharing," NIST SP 800-150, October 2016. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf

92. NIST. 2017. "The Cybersecurity Framework: Implementation Guidance for Federal Agencies," Draft NISTIR 8170, May 2017. http://csrc.nist.gov/publications/drafts/nistir-8170/nistir8170-draft.pdf

93. NIST. 2018. "Systems Security Engineering: Cyber Resiliency Considerations for the Engineering of Trustworthy Secure Systems," NIST Special Publication 800-160 Volume 2 (Draft), March 2018. https://csrc.nist.gov/CSRC/media/Publications/sp/800-160/vol-2/draft/documents/sp800-160-vol2-draft.pdf

94. NIST. 2018b. "Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1," April 16, 2018. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

95. National Security Agency (NSA). 2018. "NSA/CSS Technical Cyber Threat Framework v1," March 6, 2018, https://www.iad.gov/iad/library/reports/assets/public/upload/NSA-CSS-Technical-Cyber-Threat-Framework-v1.pdf

96. National Science and Technology Council (NSTC). 2016. "Federal Cybersecurity Research and Development Strategic Plan," February 2016. https://www.nitrd.gov/cybersecurity/publications/2016_Federal_Cybersecurity_Research_and_Development_Strategic_Plan.pdf

97. OASIS Cyber Threat Intelligence (CTI) Technical Committee. 2017. "STIX 2.0 Specification: Objects and Vocabularies, Version 2.0, Committee Specification Draft 01 / Public Review Draft 01," March 6, 2017. http://docs.oasis-open.org/cti/stix/v2.0/csprd01/stix-v2.0-csprd01.zip

98. OCC. 2011. "Supervisory Guidance on Model Risk Management," OCC 2011-12 Attachment. April 4, 2011. http://www.occ.treas.gov/news-issuances/bulletins/2011/bulletin-2011-12a.pdf

99. ODNI. 2017. "The Cyber Threat Framework." March 13, 2017. https://www.dni.gov/index.php/cyber-threat-framework, Overview: https://www.dni.gov/files/ODNI/documents/features/A_Common_Cyber_Threat_Framework_Overview.pdf, How to Use: https://www.dni.gov/files/ODNI/documents/features/A_Common_Cyber_Threat_Framework.pdf, Lexicon: https://www.dni.gov/files/ODNI/documents/features/Cyber_Threat_Framework_Lexicon.pdf, and Detailed Description: https://www.dni.gov/files/ODNI/documents/features/Threat_Framework_A_Foundation_for_Communication.pdf

100. OFR. 2017. "OFR Viewpoint: Cybersecurity and Financial Stability: Risks and Resilience. 17-01." February 15, 2017. https://www.financialresearch.gov/viewpoint-papers/files/OFRvp_17-01_Cybersecurity.pdf

101. OMG. 2014. "UML Operational Threat & Risk Model Request for Proposal," SysA/2014-06-17. June 18, 2014. http://www.omg.org/cgi-bin/doc?sysa/14-06-17.pdf

102. OWASP. 2016. "OWASP Automated Threat Handbook: Web Applications, Version 1.1," November 3, 2016. https://www.owasp.org/images/3/33/Automated-threat-handbook.pdf

103. OWASP. 2017. "OWASP Top 10 Application Security Risks – 2017," April 10, 2017. https://www.owasp.org/index.php/Top_10-2017_Top_10

104. Payments UK. 2014. "Cyber Threat Intelligence: An analysis of an intelligence led, threat centric, approach to Cyber Security strategy within the UK Banking and Payment Services

sector," May 12, 2014 (modified January 29, 2016). http://www.foo.be/docs/informations-sharing/Payments%20UK%20Cyber%20Threat%20Intelligence%20Research%20Paper.pdf

105. Perla, P., et al. 2004. "Wargame-Creation Skills and the Wargame Construction Kit." December, 2004. https://www.cna.org/cna_files/pdf/D0007042.A3.pdf

106. Potteiger, B. Martins, G., and Koutsoukos, X. 2016. "Software and Attack Centric Integrated Threat Modeling for Quantitative Risk Assessment," Hot Topics in Science of Security Symposium (HotSoS '16), April 19-21, 2016.

107. PwC. 2015. "The Modeling Continuum," June 2015. https://www.pwc.com/us/en/insurance/publications/assets/pwc-modeling-continuum.pdf

108. Reidy, P. 2013. "Combatting the Insider Threat at the FBI: Real World Lessons Learned." July 28, 2013. https://media.blackhat.com/us-13/US-13-Reidy-Combating-the-Insider-Threat-At-The-FBI-Slides.pdf

109. Reed, M., Miller, J.F., and Popick, P. "Supply Chain Attack Patterns: Framework and Catalog, Office of the Deputy Assistant Secretary of Defense for Systems Engineering," August 6, 2014. https://www.acq.osd.mil/se/docs/supply-chain-wp.pdf

110. 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

111. Sgandurra, D. and Lupu, E. 2016. "Evolution of attacks, threat models, and solutions for virtualized systems." February 2016. ACM Computing Surveys 48, 3, Article 46.

112. Shackleford, D. 2015. "Combatting Cyber Risks in the Supply Chain," September 2015. https://www.sans.org/reading-room/whitepapers/analyst

113. Sheingold, P., Bodeau, D., and Graubart, R. 2017. "Cyber Prep 2.0 Instruments for Review, PR 17-2174." The MITRE Corporation, McLean, VA, June 2017.

114. Shostack, A. 2014. *Threat Modeling, Designing for Security*, John Wiley & Sons, 2014.

115. Shull, F., Mead, N. 2016. "Cyber Threat Modeling: An Evaluation of Three Methods." November 11, 2016. https://insights.sei.cmu.edu/sei_blog/2016/11/cyber-threat-modeling-an-evaluation-of-three-methods.html

116. Simmons, C.B., Shiva, S.G., Bedi, H., and Dasgupta, D. 2014. "AVOIDIT: A Cyber Attack Taxonomy," Proceedings of the 9th Annual Symposium on Information Assurance (ASIA'14), June 2014. http://www.albany.edu/iasymposium/proceedings/2014/ASIA14Proceedings.pdf

117. Steiger, S. 2016. "Maelstrom: Are you playing with a full deck? Using an Attack Lifecycle Game to Educate, Demonstrate and Evangelize." 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

118. Tarala, J., and Tarala, K.K. 2015. "Open Threat Taxonomy (Version 1.1)," October 12, 2015. http://www.auditscripts.com/resources/open_threat_taxonomy_v1.1a.pdf

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

120. TripWire. 2015. "The Insider Threat: Detecting Indicators of Human Compromise." November 18, 2015. https://www.tripwire.com/misc/the-insider-threat-detecting-indicators-of-human-compromise-register/

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

122. WASC. 2010. "WASC Threat Classification, Version 2.00." January 1, 2010. http://projects.webappsec.org/f/WASC-TC-v2_0.pdf

123. Wynn, J., et al. 2011. "Threat Assessment and Remediation Analysis (TARA) Methodology Description, Version 1.0," MTR 110176, PR 11-4982, The MITRE Corporation, Bedford, MA, October 2011. https://www.mitre.org/sites/default/files/pdf/11_4982.pdf

124. Wynn, J. 2014. "Threat Assessment and Remediation Analysis (TARA)," PR 14-2359, The MITRE Corporation, Bedford, MA, 2014. https://www.mitre.org/sites/default/files/publications/pr-2359-threat-assessment-and-remediation-analysis.pdf

125. Wynn, J. 2017. "MITRE ICS/SCADA Cyber Repository (Presentation to International Atomic Energy Agency (IAEA) Research Coordination Meeting (RCM), PR 17-0876," The MITRE Corporation, Bedford, MA, March 2017.

126. Xin, T., and Xiaofang, B. 2014. "Online Banking Security Analysis based on STRIDE Threat Model," International Journal of Security and Its Applications, Vol. 8, No. 2 (2014), pp. 271-282.

127. ZoneFox. 2015. "Introducing the Insider Threat Kill Chain." April 3, 2015. http://www.infosecurityeurope.com/__novadocuments/86466?v=635671049778130000