MITRE TECHNICAL REPORT MTR130433

MITRE

Mapping the Cyber Terrain

Enabling Cyber Defensibility Claims and Hypotheses to Be Stated and Evaluated with Greater Rigor and Utility

Deborah Bodeau
Richard Graubart
William Heinbockel

November 2013

Project No.: 51MSR615-DA

Bedford, MA

Abstract

Evidence and analysis are needed to determine the effectiveness of cyber security, defensibility, and resiliency solutions. Claims or hypotheses about effectiveness generally are based on assumptions about the threat, and about the technical and operational settings in which solutions will be used. Evidence can be obtained in a variety of environments, ranging from conceptual models to systems supporting mission operations. This paper presents a framework for characterizing assumptions and evaluation environments – an approach to mapping the cyber terrain. The approach presented here can facilitate determination of whether a given hypothesis is meaningful to a specific real-world situation or can be evaluated in a given environment, whether different solutions can be evaluated in a common environment, and whether or how the results obtained in a given environment can be applied to real-world situations. Examples are provided of questions to ask, and sources of information to use, to characterize an environment, particularly with respect to the threat.

This page intentionally left blank.

Table of Contents

1 Introduction 1
1.1 Background 2
1.2 Overview of This Document 3
2 Evaluation Challenges and Environments 4
2.1 Challenges for Evaluation 4
2.2 Types of Evaluation Environments 5
2.2.1 Synthetic Environments 6
2.2.2 Operational Environments 8
2.2.3 Hybrid Environments 9
2.3 Red Teaming 9
2.4 Examples 10
3 Situating a Claim or Hypothesis: Three Key Aspects 12
3.1 Threat Aspects 12
3.1.1 Adversary Characteristics 13
3.1.2 Adversary Behavior 14
3.2 Technical Aspects 16
3.3 Operational Aspects 17
3.3.1 Operational Architecture 17
3.3.2 Possible Defender Decisions or Actions 18
3.4 Examples 20
3.4.1 RAMBO Demonstration 20
3.4.2 Common Criteria Evaluations 21
3.4.3 TALENT 22
4 Recommendations for Mapping the Cyber Terrain 24
4.1 Processes for Identifying Critical Assets 24
4.2 Recommended Questions 24
5 Conclusion 33
6 Bibliography 34
Appendix A Acronyms 44
Appendix B Representations of Concreteness and Comprehensiveness 46

List of Figures

Figure 1. Environments to be Aligned 4
Figure 2. General Characteristics of Types of Evaluation Environments 6
Figure 3. Notional Concreteness and Comprehensiveness of the Technical Aspects of the Environment 17
Figure 4. TALENT Assumptions 23

List of Tables

Table 1. Example of Attack Vectors and Actions in a Security Target 22
Table 2. Key Cyber Threat Features – Adversary Characteristics 26
Table 3. Key Cyber Threat Features – Adversary Behavior 28
Table 4. Key Technical Features 30
Table 5. Key Operational Features – Operational Architecture 31
Table 6. Key Operational Features – Possible Cyber Defender Actions 32
Table 7. Concreteness and Comprehensiveness of Representation: Adversary Characteristics .. 46
Table 8. Concreteness and Comprehensiveness of Representation: Adversary Behavior 46
Table 9. Completeness and Comprehensiveness of Representation: Technical Environment 48
Table 10. Concreteness and Comprehensiveness of Representation: Operational Architecture .. 49
Table 11. Concreteness and Completeness of Representation: Defender Actions 49

This page intentionally left blank.

1 Introduction

Cyber defenders, systems architects, and researchers need to evaluate claims or hypotheses about the potential effectiveness of defensive actions, decisions, and solutions.[1] Claims or hypotheses[2] about effectiveness generally are based on assumptions about the threat, and about the technical and operational settings in which solutions will be used. Support for claims and hypotheses can be obtained in a variety of environments, ranging from conceptual models to systems supporting mission operations. Those evaluation environments embody assumptions about threats, technology, and operations.

The recognition that cyberspace is a domain for military operations [1] has led to investigation of what constitutes *key cyber terrain* – "those physical and logical elements of the domain that enable mission essential warfighting functions" [2]. Which elements constitute *key* cyber terrain can best be determined by situating them in a context that includes operational and threat as well as technical aspects. A *map of the cyber terrain* is a representation of that context. More precisely, a map of the cyber terrain is a representation of knowledge and/or assumptions that determine or influence cyber decisions, i.e., decisions about cyber operations, investments, and architecture intended to improve cyber defensibility, resiliency, and/or security. This report presents a framework for mapping the cyber terrain – for characterizing knowledge and assumptions about key features of the environments in which cyber decisions are taken. A map of the cyber terrain can help determine whether

- Assumptions about features of the cyber terrain (e.g., adversary characteristics and possible adversary actions) are consistent.
- A claim or hypothesis is meaningful to a specific real-world situation or can be evaluated in a given environment.
- A set of claims or hypotheses assume the same environment and thus could be evaluated in a common integration experiment.
- Evidence or analytic results obtained in a given evaluation environment could be used to confirm or disconfirm a given claim or hypothesis.
- A claim or hypothesis supported by evidence from a given evaluation environment could be – or could fail to be – meaningful and relevant to a given real-world situation.

This report describes characteristics of three aspects of the cyber terrain in which a hypothesis or claim is intended to apply, for brevity referred to as a *claims environment*. The same characteristics can also be used to describe the cyber terrain in which evidence for or against hypotheses or claims can be sought, for brevity referred to as an *evaluation environment*. These aspects – threat, technology, and operations – can be represented with more or less

[1] For ease of exposition, the term *solution* refers to a combination of technology and practice that mitigates a risk, reduces the severity of a problem or concern, or otherwise solves (in whole or in part) a problem stated in terms of security, resiliency, or defensibility. *Security* (variously referred to as information security, computer security, or cyber security) involves meeting objectives for confidentiality, integrity, availability, and accountability. *Cyber resiliency* is the ability to anticipate, withstand, recover from, and evolve to address more effectively, cyber-domain attacks [104] [101]. *Cyber defensibility* involves causing cyber adversaries to move more slowly, spend more, and take more risks.

[2] *Claims* (e.g., "this product thwarts the following types of attacks") are typically made by product vendors, but are also made by researchers as their research matures. Many *hypotheses* (e.g., "use of this technical approach can substantially delay the effects of the following attack actions, thus increasing the likelihood that the attack will be detected before it causes harm") are stated by researchers; however, some hypotheses (e.g., "this attacker is characterized by the following IP addresses" or "this change in the system configuration will prevent the attack from succeeding") are made by cyber threat analysts or cyber defenders. Claims tend to be stable and to be validated by evidence, while hypotheses are expected to evolve as evidence confirms or disconfirms sub-hypotheses.

comprehensiveness and concreteness. Trade-offs can be identified between how concretely and comprehensively the different aspects are represented and how broadly applicable the results of an evaluation will be. In general, the more specific an evaluation environment is, the less broadly applicable the evidence obtained therein will be. The threat aspect is particularly challenging to represent, and thus is discussed in detail. Three general types of evaluation environments are described: operational, synthetic, and hybrid. The properties of the evidence that can be obtained in each type of evaluation environment are discussed, and examples are given.

1.1 Background

A question of increasing concern is whether defensibility decisions (e.g., cyber defender actions, architectural decisions, use of cyber defense technologies) have any effect on cyber adversaries' behavior or strategy. A variety of effects can be hypothesized or claimed, ranging from strategic (e.g., deterrence) to immediate (e.g., curtailing specific adversary activities). Determining the characteristics of a well-formed hypothesis is key to applying general scientific principles to cyber security, resiliency, and defensibility [3]. Similarly, evaluating claims about the effectiveness of a proposed solution is central to determining whether and how it advances from one level of technical maturity[3] to the next.

Hypotheses or claims about effects on cyber adversaries can be stated, and made more precise using a controlled vocabulary [4], attack scenarios, or requirements. For example, in Cybersecurity Developmental Test and Evaluation (DT&E), claims can be stated in terms of the correct and effective functioning of required and inherited protections, as well as in terms of the "system's resiliency and ability to detect, deny, deceive/redirect, disrupt, degrade, and recover in response to cyber-attacks"; these claims are made more precise when portrayed in DT&E events [5]. In the Common Criteria scheme, the Security Target identifies threat agents and adverse actions (i.e., attack scenarios), but does not use a controlled vocabulary for these; claims about functionality are stated using a tailorable set of requirement statements [6].

However, even when made more precise, hypotheses or claims about potential solutions frequently make hidden assumptions about threats, or about the technological or operational environment in which the solution will be used. The importance of identifying and validating key assumptions is recognized in intelligence analysis [7] and (non-cyber-specific) Red Teaming [8]. For claims or hypotheses about cyber solutions or decisions, assumptions about the adversary become more challenging to articulate, but are of central importance [9] [10]. For purposes of discussion, the environment assumed (implicitly or explicitly) by a hypothesis or claim is referred to as the *claims environment*. (The plural is used here because, as a general rule, multiple hypotheses or claims are made about a potential technology or defender action.)

Evidence to confirm or disconfirm claims or hypotheses – whether about defensibility, security, or resiliency – is obtained, and analysis performed, in an *evaluation environment*, such as a laboratory, a model or simulation, an exercise, a cyber range, a T&E environment, or an operational system. An evaluation environment expresses or includes selected aspects of the threat, technical, and operational environments in which the defensibility decision is or may be taken. Other aspects are assumed, either explicitly or implicitly. The applicability of evidence obtained in a given evaluation environment to a claim about a system, organization, or specific defensibility decision depends on how well that environment corresponds to the real-world situation in which the decision is being considered.

[3] Technology maturity or readiness for use can be measured as Technology Readiness Level (TRL) [133]. Note that a variety of readiness levels for technology have been asserted, with different uses and limitations [141].

As noted above, the recognition that cyberspace is a domain for military operations [1] has led to investigation of what constitutes key *cyber terrain* – "those physical and logical elements of the domain that enable mission essential warfighting functions" [2]. While cyberspace has many unique characteristics, the general concepts of key terrain hold [11]. In the Army Defense in Depth strategy, key cyber terrain includes "physical and logical infrastructure and mission data" [12]. The question of how to model cyber terrain is an area of active investigation. Some focus on representing the technical environment, e.g., using a directed graph with nodes and interconnections [13] [14], by analogy with physical terrain [15], or identifying relationships between physical and cyber elements [16]. Others include missions and mission dependencies as necessary to determining which terrain elements are key [17] [18]. Still others include the adversary [19].

1.2 Overview of This Document

Section 2 describes three general types of evaluation environments, provides examples of the types of evidence that can be obtained in different evaluation environments, and discusses issues related to repeatability, reproducibility, and applicability of results. Section 3 identifies characteristics of three aspects of the real-world environment in which a hypothesis or claim is intended to apply – the threat, technology, and operations environments. Section 4 presents questions that can be used to identify key features of the cyber terrain.

2 Evaluation Challenges and Environments

A variety of challenges arise for evaluation of a claim or hypothesis, particularly when the claim involves effects on an advanced cyber adversary. As illustrated in the figure below, three notional environments need to be matched up: the real world, the environment assumed (implicitly or explicitly) by claims or hypotheses, and the environment in which evidence is sought to confirm or disconfirm claims. For a claim or hypothesis to be meaningful, its assumed environment needs to match (some portion of) the real world. For a claim or hypothesis to be capable of being confirmed or refuted, construction of an evaluation environment that matches the assumed environment (the "claims environment") must be possible. For evidence obtained in an evaluation environment to be useful, the evaluation environment must represent some meaningful portion of the real world.

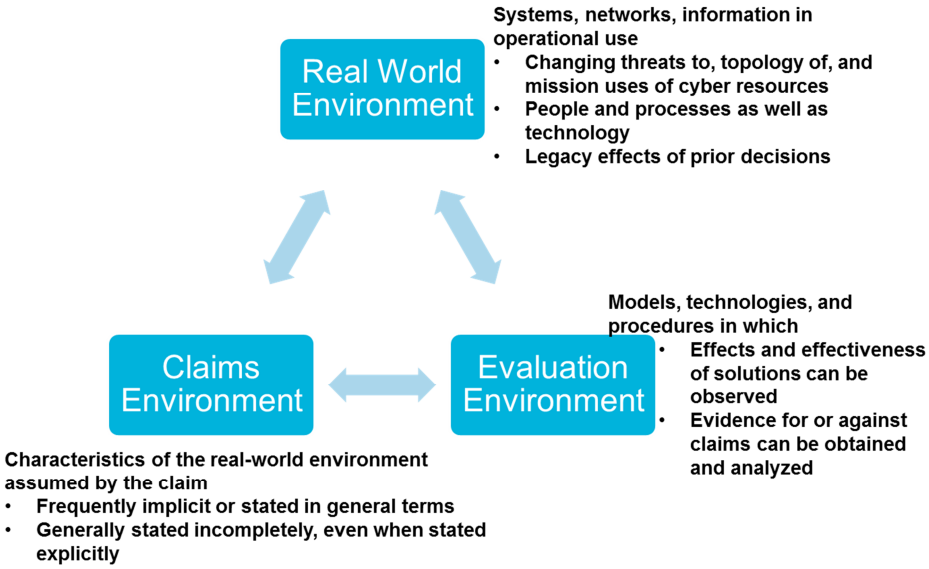

Figure 1. Environments to be Aligned

2.1 Challenges for Evaluation

Research and development in the areas of cyber security, resiliency, and defensibility is most mature for security. Even for security, numerous challenges for evaluation have been identified; several initiatives seek to provide a more scientific foundation for cyber security [20] [21]. For cyber security claims or hypotheses, relevant properties of experiments include falsifiability, controls, and reproducibility (including repeatability) [3]. A NATO workshop on determining or measuring the relative appropriateness of live vs. synthetic experimentation identified 32 indicators of relative utility; of these, those relevant to cyber include controllability, cost, validation, data collection, and observability [22]. Killourhy and Maxion argue that, while most cyber security experiments can be characterized as one-off evaluations, comparative experiments can support statistical inferences [23]; experiments can draw upon a large body of experience with conventional cyber threats, e.g., hackers or authorized users who exceed their privileges.

However, claims or hypotheses about defensibility – about having an effect on the behavior or strategy of, an advanced adversary – assume a more complex and dynamic threat model. Many alternative attack paths are possible, and cannot all be represented experimentally; representative scenarios must be defined [24]. The advanced persistent threat (APT) is characterized by adaptability. While the emerging discipline of cyber threat analysis is building a body of artifacts

(e.g., malware) and partial results (e.g., observables, indicators), such evidence of APT activity is incomplete and can become outdated. Singh's word of caution about cybersecurity becomes all the more important when applied to the APT:

> "I can't help but think that the science of security is still at its pre-Galileian stage. We should state and refine our hypotheses by all means and conduct measurements where we can, but we should remember that what we're measuring might prove as crucial to the science of security as impetus has been to modern physics." [21]

2.2 Types of Evaluation Environments

Three general types of evaluation environments can be identified: operational, synthetic, and hybrid.[4] The environment determines the properties of the evidence that can be obtained to evaluate a defensibility claim, including the granularity of evidence (and the amount of pre-analysis performed); visibility into the behavior of systems, components, and adversaries; fidelity; and the potential sophistication of the analysis of evidence. As will be discussed in Section 3, the environment expresses or includes some aspects of threats, technology, and operations, and assumes (explicitly or implicitly) other aspects; the more explicitly the assumed and actual aspects can be stated, the more easily the applicability of the evidence and analysis results from the evaluation environment to other environments can be determined.

It is possible to define a single spectrum for the completeness of an evaluation environment, i.e., for how completely the environment represents (some portion of) the real world [25]. However, particularly for considering the threat aspect, it can be useful to define two dimensions: concreteness and comprehensiveness. *Concreteness* (or specificity) refers to the extent to which details are represented vs. being abstracted or assumed away. For example, a threat model can be vague with respect to adversary characteristics, using undefined terms; alternately, adversary characteristics can be described in detail, based on threat intelligence. *Comprehensiveness* refers to the extent to which the features being represented cover all possible alternatives. Figure 1 illustrates how the three types of evaluation environments fall along these two dimensions. See Appendix B for definitions of the degrees of completeness and comprehensiveness shown on the axes.

A third dimension, *fidelity*, can also be defined. Fidelity refers to consistency with the real world, as viewed from some perspective or at some level of detail. When a feature of the cyber terrain is represented with greater completeness (i.e., with greater concreteness and comprehensiveness), its fidelity to a given real-world situation (or set of situations) is more easily determined. The degree of fidelity with which technical aspects (e.g., level and make-up of network traffic [26], whether machines are physically distinct or virtual [27]) are represented in an evaluation environment can be determined and managed.[5] However, fidelity of representation for the operational and especially the threat aspects is much harder to determine.

---

[4] For purposes of evaluating Science and Technology (S&T) cyber research, specifically including the APT in the threat model, the Cyber Measurement Campaign (CMC) identifies four approaches [25] [42]: (1) analysis, based on first principles, to develop intuition, define bounds, and identify cases to validate modeling, simulation, and emulation; (2) modeling and simulation, which is repeatable and easiest to transfer across organizations, but which faces trade-offs among fidelity, complexity, and time; (3) a cyber range, in which real applications are used in an emulated environment; and (4) prototype deployment in operational environments. However, these four categories do not include T&E, mission-oriented experiments that include a cyber aspect, or operational environments other than for purposes of evaluating prototypes.

[5] Research into cyber-physical systems, including security research, involves a strong interest in managing technical fidelity in experimentation [139] [140].

It must be noted that it is rarely feasible or desirable for an evaluation environment to be at the extreme of concreteness (fully realized) or comprehensiveness (fully specified) in all (or even most) aspects. Results of evaluations in a highly concrete environment are hard to generalize and to apply to other situations. Comprehensiveness is feasible only for selected aspects or attributes, in a model (i.e., a sub-type of synthetic) environment; even then, the question of whether all possible values have been enumerated can remain open. The extremes are identified simply to facilitate comparisons of claims and evaluation environments.

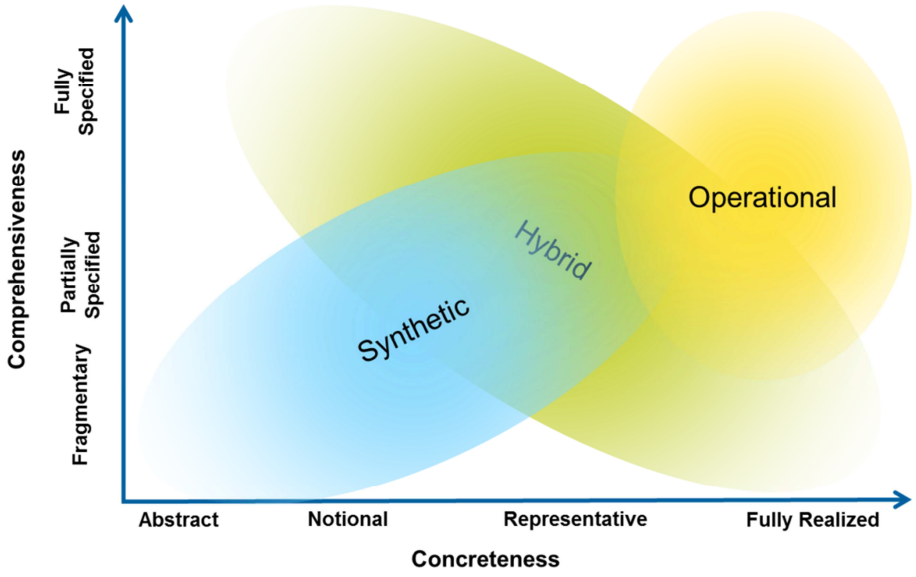

Figure 2. General Characteristics of Types of Evaluation Environments

2.2.1 Synthetic Environments

Synthetic environments abstract away many aspects of the real world and hold constant many of the factors or attributes of the aspects they represent, to focus on the effects of changing a few variables. Examples of synthetic environments include conceptual or "toy" models, executable models and simulations, laboratory environments, and experiments or exercises.[6] More specifically, synthetic environments include:

- Modeling and Simulation. Informal models are typically notional or abstract, and are expressed in human language.[7] Formal models (e.g., attack graphs, game-theoretic models) can be expressed in standard notation, and may use qualitative or quantitative values.[8] Executable models (e.g., executable game, simulations) rely on formal models; because they can be executed repeatedly with variant inputs, such models can be more comprehensive with respect to specific aspects of the situation being modeled (while relying on fragmentary representations of other aspects). See [28] [29] for a description of Raytheon's CAMEO modeling environment, specifically designed to represent cyber adversaries.

[6] Thus, the category of synthetic environments includes three of the four approaches to cyber assessment in [25]: analysis (informal and formal models), modeling and simulation (executable models), and cyber ranges (demonstration environments). The fourth approach, prototype deployment, falls into the category of operational environments.
[7] Cyber attack lifecycle models, as described in Section 2.2.3 of [4], are examples of notional informal models of adversary behavior.
[8] See Sections 2.2.1 and 2.2.2 of [4] for a discussion of how these techniques apply to cyber security, resiliency, and defensibility.

- Laboratory environments. These include research laboratories and demonstration facilities such as MITRE's Resilience Lab [30] [31], as well as product evaluation laboratories (e.g., Common Criteria Testing Laboratories) and test facilities. In research laboratories and research demonstration facilities, representative mission applications can be included, but simulation of mission environments will be limited.
- Demonstration environments. These include experimental and exercise environments such as cyber ranges, as well as simulation environments such as MITRE's Simulation Experiment (SIMEX) [32]. Potential solutions are integrated with mission applications for real-time simulation or emulation.

In addition to concreteness and comprehensiveness, laboratory and demonstration environments can be characterized in terms of focus and capability. The focus can vary from cybersecurity as ancillary component to cybersecurity-focused, while capability can vary from minimal or theoretic (e.g., tabletop exercises) to highly capable of realistic representations. Cyber ranges are cybersecurity-focused and highly capable environments for experimentation, testing, demonstration, and training. Examples of cyber ranges include:

- The Joint Cyberspace Operations Range (JCOR) [33], which provides continual training and education in realistic environments, and supports multiple cyber exercises annually. JCOR is a coalition of
    - AF Simulator Training and Exercise (SIMTEX) range
    - U.S. Navy Cyberspace Operations Range
    - U.S. Strategic Command Cyberspace Training Environment
    - Army Guard Enhanced Network Training Simulator
- The National Cyber Range (NCR), which was originally developed by DARPA. NCR transitioned to OSD/TRMC in 2012 [34]. The Army Program Executive Office for Simulation, Training and Instrumentation (PEO STRI) Project Manager for Instrumentation, Targets & Threat Simulators (PM ITTS) plans to continue Lockheed Martin's support for continuing NCR operations [35]. NCR emulates the public Internet, enables modeling of cyber attacks, and supports test and evaluation of cyber impacts.
- The DETER facility, funded by DHS and NSF and operated by USC ISI, which provides a testbed facility to advance the technology of experimental infrastructure [36] [36].
- The use of Sandia's Live, Virtual, and Constructive (LVC) approach (realized in the Umbra Simulation Framework) as a cyber testbed [37].
- The Michigan Cyber Range, a partnership of academe, industry, and government, which focuses on training, education, and exercises [38].
- Commercial offerings to provide a cyber range training facility within an enterprise [39] [40] [41].

The Cyber Measurement Campaign is exploring ways to improve the use of cyber ranges to provide a more rigorous approach to tracking progress in cybersecurity [42]. Depending on whether and how a cyber range connects to external systems, some of its characteristics might be more typical of an operational environment. Experimentation in such situations carries inherent risks, which can be managed [43].

Sonchack et al. note that major challenges for laboratory and experimental environments include reproducibility, experimental controls, difficulty (or even impossibility) of determining ground truth, and obtaining datasets large enough for experimentation at scale [44].

2.2.2 Operational Environments

In an operational environment, adversaries can be engaged directly. Experiments with real-world users can be performed, subject to compliance with organizational requirements on human subject research [24]. Operational environments are typically enterprise-internal, but can be sector-wide or even cross-sector. For enterprise-internal operational environments, operational capabilities can be characterized in terms of

- People, e.g., size and expertise of staff; extent of external relationships and information sharing / incident coordination;
- Processes, e.g., tracking, response, analysis, attribution, information sharing; and
- Technology, e.g., sensors, threat/intel knowledge base, malware analysis, forensic analysis.

For purposes of characterizing environments for evaluating hypotheses or claims about effects of defender actions / decisions on cyber adversaries, three general levels of capability can be defined:

- Basic: Incident handling / tracking. In such an operational environment, evidence can be found in monitoring and analysis sources maintained consistent with standards of good practice (e.g., audit logs, IDS read-outs, DLP reports).
- Intermediate: Incident response / incident and trend analysis. In such an environment, evidence can be derived from value-added analysis of standard sources (e.g., trend analysis).
- Sophisticated: Threat-informed proactive defense / cyber threat analysis. In such an environment, evidence can be drawn from tailored/specially developed tools (sensors, malware analysis, forensic analysis); attribution to individual threat actors is feasible. A set of best practices is emerging [45].

Hypotheses or claims can be evaluated on a supra-organizational (sector-wide or cross-sector) basis. For sector-wide operations (e.g., across the Defense Industrial Base or DIB [46], across the energy or financial sector), evidence consists of shared information. Varying levels of granularity and pre-analysis can be defined:

- Basic: incident information sharing (e.g., using the CIO Cyberthreat Report Form [47]).
- Intermediate: incident and threat information sharing, typically using semi-structured information.
- Sophisticated: threat and incident information sharing, using structured and semi-structured information (e.g., DIB information sharing [48], DSIE [49], STIX users [50]).

At the cross-sector, national, or transnational levels, evaluation of hypotheses or claims uses analysis of information presented at varying levels of granularity and pre-analysis. Such analysis is typically presented in industry threat reports [51] [52] [53] or in national CERT threat reports.

Supra-organizational data collection, analysis, and information sharing presents numerous challenges. These include policy and reputational concerns for information sharing; operational

challenges associated with analysis performed with different expertise and biases, over different timeframes; issues of cost sharing; and technical challenges associated with different tools and measurement systems, which result in data interoperability obstacles as well as differences in granularity. In addition, because supra-organizational data collection and information sharing can be costly, the desire arises naturally to use data collections for multiple purposes (e.g., policy analysis; trend analysis for different domains, including security posture, performance and usage, and threat targeting and attack methods). However, analytic communities differ in their underlying models of the problem space, including terminology and taxonomies, and expectations of data quality. Asghari and Mueller offer recommendations for large-scale data collection and analysis [54].

2.2.3 Hybrid Environments

Hybrid environments provide a combination of synthetic and operational elements, to provide as much realism as possible for experiments or tests, while allowing for a level of instrumentation and monitoring more typical of a laboratory or cyber range. Examples include

- Highly instrumented operational environments. Evaluation of claims or hypotheses in such environments can be based on observation of normal operations, or on simultaneous operations / experimentation (e.g., Red Teaming).
- Deception environments. These can range from honeypots to honeynets or mirror environments.
- Operational experimental environments. These include mission-oriented test and evaluation (T&E) environments [55], cyber test ranges [56], or mission-oriented experiments such as the Joint Cyber Operations Joint Test (JCO JT) [57], which represent a mission or operational environment. These are typically better instrumented than fully operational environments, and may interface with operational systems.

In highly instrumented operational environments (which may include deception environments), direct engagement with real-world adversaries is possible. Kanich et al. present lessons-learned from engaging with cyber criminals, and make two general observations [58]:

> "First, the adversarial conditions of engaging with attackers, in this case the ecosystem surrounding spam-advertised Web sites, requires repeated updates to experimental methodology over time. Extensible infrastructure, although often a more time-intensive investment up front, more easily accommodates unexpected yet ultimately necessary changes. Second, actively engaging with attackers and their infrastructure, such as via crawling and purchasing, often results in accidents or serendipitous insights that lead to unexpected discoveries."

That is, organizational commitment and researcher flexibility are vital to making such an environment an effective tool for learning and hypothesis evaluation.

2.3 Red Teaming

There is no direct relationship between the evaluation environment and the evaluation methodology, that is, the process by which evidence is obtained and analyzed. Red team evaluation is a specific methodology. Sandia defines it as "authorized, adversary-based assessment for defensive purposes", and observes that adversary modeling is central to effective red teaming [59]. Red teams are used primarily in hybrid and some operational environments,

but can be part of experimentation in lab environments [60]. Cyber red teams are increasingly part of operational experimentation and exercises [1].

Red team rules of engagement often explicitly map key features of the threat terrain, in particular, which types of adversary actions are out of bounds.

2.4 Examples

The table below illustrates the different types of evidence that can be obtained in different evaluation environments. For purposes of illustration, the following examples of hypotheses or claims are considered:

- A Moving Target (MT) defense such as TALENT [61] or Net Maneuver Commander [62] that relocates a mission application, running on an enterprise-internal virtual machine (VM), to another location, *degrades* or *curtails* adversary activities. This either increases the amount of time the adversary spends in the Control (or Escalate Privileges) or Execute (or Pilfer) stage of the cyber attack lifecycle (degrading adversary effectiveness), or simultaneously decreases the number of successful attacks while increasing the number of partially successful attacks (curtailing adversary activities).[9]
- End-user training and awareness *degrades* the effectiveness of phishing or spearphishing as a malware delivery mechanism, by decreasing how often users click on infected links or open infected documents.
- An attack-resistant localization scheme, which applies the concept of Substantiated Integrity (a resiliency technique) to location information in a wireless network, improves the trustworthiness of location information. [63]

[9] See [4] for a discussion of effects such as curtail or degrade. See [131] for a discussion of the metrics "Successful Attacks," "Partially Successful Attacks," and "Time Spent per Attack Phase."

Table 1. Examples of Evidence from Different Evaluation Environments

Environment		Moving Target	Anti-Phishing Training	Trustworthy Localization
Synthetic	Informal Model	Argument from general principles		
	Formal Model	Percentage of successful attacks, mean number of attack disruptions (e.g., using CAMEO M&S [28])		Error analysis [63]
	Laboratory Environment	Percentage of successful attacks, time needed for a successful attack [62]	Percentage of wrongful clicks [64]	Localization accuracy with and without simulated attacks in ORBIT Testbed [63]
Operational	Enterprise-internal	Percentage of successful attacks, time needed for a successful attack, mean number of attack disruptions based on forensic / log analysis[10]	Percentage of wrongful clicks [65] [66]	Localization accuracy with and without simulated attacks on floor of enterprise office building [63]
Hybrid	Operational Experiment	Percentage of successful attacks, time needed for a successful attack, mean number of attack disruptions in a deception environment		

[10] Note that this requires a sophisticated threat analysis capability.

3 Situating a Claim or Hypothesis: Three Key Aspects

To *situate* a claim or hypothesis is to make explicit the assumptions about the environment in which it is to hold, thereby mapping the cyber terrain in which it can be applied. No claim – about a solution's effectiveness, about changes in adversary behavior in response to defender actions, about system properties such as trustworthiness or resiliency, or about adversaries themselves – can be universally applicable. Similarly, evidence is obtained in an evaluation environment, and as discussed above, evaluation environments vary in capabilities and realism.

The assumed environment for a claim or hypothesis, and the environment in which evidence to confirm or disconfirm it may be sought, can be characterized or describe from three perspectives. A claim or hypothesis can be situated in, and an evaluation environment can be described in terms of, its

- Threat aspects. What threats are assumed to be present? What threats are explicitly excluded?
- Technical aspects. What technologies are assumed or required to be present? What architectural limitations apply? What technologies or components are assumed to be trusted or error-free?
- Operational aspects. What roles, responsibilities, and business processes are assumed to be present? What alternatives are provided for defender actions?

These aspects – or *types of features of the cyber terrain* – are described below. Examples are then presented of different evaluation environments, showing how these aspects are represented. The focus is on the threat aspect, with the technical and operational aspects discussed more briefly. Appendix B provides tables provide definitions of the degrees of concreteness and comprehensiveness used in Figures 1 and 2.

3.1 Threat Aspects

Four general types of threats can be considered for cyber systems, which include cyber-physical systems (CPS) as well as information and communications technology (ICT): adversarial, accidental, structural, and environmental threats [67]. Adversarial threats can be described in terms of adversary characteristics and behavior. This section focuses on how the adversarial threat can be represented, and in particular on the APT and on cyber attacks.[11]

General characterizations of the conventional adversarial threat (i.e., non-APT), with fragmentary representations of adversary behavior, are common in security claims for products or technologies, and in evaluation environments for such products.[12] Assumptions about the characteristics and behavior of advanced adversaries are more challenging to articulate. However, articulation of claims and hypotheses about cyber defensibility and resiliency requires that such assumptions be articulated, so that the realism and applicability of those claims can be

[11] CNSSI No. 4009 defines *cyber attack* as "An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information." [138] Cyber attack lifecycle models are consistent with this definition. Some authors construe the phrase more broadly, to include attacks on cyber resources that are not via cyberspace (e.g., physical attacks, attacks solely involving social engineering) or attacks via cyberspace on non-cyber assets (e.g., physical resources controlled by cyber-physical systems). Determining which of these definitions is used is part of defining the threat environment.

[12] For example, the Common Criteria Profiling Knowledge Base [92] and CC Security Targets provide examples of security threats to environments in which products are used.

determined, and so that evidence to confirm or disconfirm them can be sought in an environment that matches those assumptions.

Threats can be situated in an operational and/or technical setting. For example, adversary intent can be described in terms of general goals (e.g., mission impacts, financial gain) or in terms of specific cyber effects (e.g., degradation of network performance for a specific connection) which lead to specific mission effects (e.g., lack of timely targeting data). Threats in an operational and/or technical setting are more concrete.

3.1.1 Adversary Characteristics

Three general characteristics can be identified [67] [68]: capability, intent, and targeting.

Capability includes the adversary's resources, skill or expertise, knowledge, and opportunity. Resources can include attack tools and the financial or political resources to acquire new or tailored tools (e.g., 0-day exploits). Skill can include the ability to tailor existing tools or to develop new tools. Knowledge can be about the target system or component (e.g., products or technologies, functional dependencies, information flows, specific vulnerabilities), and for an operational system, mission, or organization, can also include information about key personnel.

Intent includes goals, motives, or outcomes that the adversary seeks, consequences the adversary seeks to avoid, and how strongly the adversary seeks to achieve those outcomes and/or avoid those consequences.

- *Goals* can be aligned with broad classes of threat actors; for example, the Cyber Prep levels identify cyber vandalism, cyber theft / crime, cyber incursion / surveillance, cyber sabotage / espionage, and cyber conflict / warfare [69]. NERC, citing an FBI presentation, identifies the *motives* of personal enrichment and anger for insiders, and support for a cause, personal interest, financial gain, ideology, national interest, and warfare for hacktivists, hackers, criminals, terrorists, and nation states respectively [70]. Harrison and White identify goals such as service theft, intelligence gathering, and widespread destruction, and then objectives such as information corruption and system subversion [71]; these objectives correspond closely with classes of cyber effects [72] [73], i.e., effects on cyber resources. Adversary goals can be characterized using Information Operations (IO) objectives [74]; goals can also be characterized in terms of effects on a mission or organization at different orders of distance from the immediately affected resource [75].
- *Consequences the adversary seeks to avoid* can include detection, disclosure of TTPs, and attribution; detection together with attribution could lead to legal recourse or other forms of retribution. See [10] [76] for discussions of adversary risk aversion, as well as resources and sophistication (attributes of capability) and specific targets (attribute of targeting).

Targeting describes how broadly or narrowly (i.e., with what degree of focus) and how persistently the adversary targets a specific organization, mission, program, or cyber resource (e.g., system, database or other information store, network, service). *Persistence* can be characterized in terms of how easily the adversary can be deterred, as well as in terms of timeframe.

These characteristics can be described or assessed in general terms. For example, NIST SP 800-30 Rev.1 [67] defines five levels[13]. Alternately, discriminating attributes can be identified with greater detail. Attributes can be generic or situated – when situated, intent and targeting look like actions. Note that understanding the adversary is part of Step 1 in the Cybersecurity DT&E Process [5] ("What are the cybersecurity threats?").

3.1.2 Adversary Behavior

Adversary behavior can be described in terms of actions and strategy.[14] Multiple taxonomies for adversary actions or cyber attacks have been identified; see the literature reviews as well as the taxonomies in [77] [71] [78]. For purposes of identifying assumptions about adversary behavior to make claims or hypotheses more precise, and to determine what behavior can or might be represented in an evaluation environment, it is useful to describe actions described in terms of attack vectors, type of attack action, extent, and effects of prior adversary actions. Describing adversary behavior is part of Step 3 in the Cybersecurity DT&E Process [5] ("What are the likely kill chain activities should an adversary gain access to the system?").

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. Partial sets of types of cyber attack vectors have been defined (e.g., types as identified in TARA [79], attack vectors by Sandia [80]), with the recognition that as the adversary evolves, so will cyber attack vectors. Typically, only cyber attacks (or cyber attacks in conjunction with specific forms of social engineering such as spearphishing) are considered when stating claims or hypotheses for cyber security or defensibility; evaluation environments often follow suit. However, this is recognized as a simplifying assumption, since advanced adversaries use multiple avenues of attack.

Types of cyber attack actions can be characterized[15] in terms of an attack taxonomy[16], or a cyber attack lifecycle, and can be amplified by using a list or an enumeration such as CAPEC[17] [81], or by shared information about adversary tactics, techniques, and procedures (TTPs), e.g., using STIX and TAXII [50].

- *Attack taxonomies* often conflate actions and effects; for example, Microsoft's STRIDE taxonomy [82] (adopted by the OWASP Testing Guide [83]) lists spoofing identity, tampering with data, repudiation, information disclosure, denial of service, and elevation of privilege. A variety of taxonomies have been proposed [77] [71] [78] [84] [85] [86]. Attack taxonomies often focus on specific technical environments (e.g., Web applications [87], 3G networks [88]), or are domain-specific such as for process control systems [89] [90] [91].

[13] While the Defense Science Board (DSB) [128] defines six levels, individual characteristics are not identified. The taxonomies cited in [85] (like many threat taxonomies) merge characterization of the adversary with characterization of possible behaviors.
[14] Strategy is rarely represented explicitly in threat models. Preference for specific actions, based on specific factors, is represented in some models, particularly game-theoretic and Bayesian models. However, no general taxonomy for adversarial strategies has been defined. (One possible representation is in terms of the adversary's preferences for different methods, e.g., outsource / delegate; purchase / acquire / direct; develop / execute.) Due to the lack of generally accepted representations of adversarial strategy, definitions of degrees of completeness and comprehensiveness would not be meaningful, and are not presented in this document.
[15] Verizon [51] characterizes data breaches in terms of "the four A's" – actors (whose actions affected the asset), actions (what actions affected the asset), assets (which assets were affected), and attributes (how the asset was affected). Actions are categorized as malware, hacking, social, misuse, physical, error, and environmental, with further sub-categorization.
[16] See [137] for a taxonomy of social engineering attacks.
[17] While CAPEC includes categories of attack actions as well as describing attack patterns in terms of specific of technologies (e.g., Web services), CAPEC is not intended to provide a taxonomy.

- A *cyber attack lifecycle* or *cyber kill chain* provides a useful expository and organizing structure for APT actions. See Section 2.2.3 of [4] for a discussion of cyber attack lifecycle models. NIST SP 800-30 R1 [67] and the Cybersecurity DT&E Guideline [5] identify seven stages: reconnaissance, weaponize, deliver, exploit, control, execute, and maintain.

Examples of specific actions can be obtained from multiple sources. The Common Criteria Profiling Knowledge Base [92] provides examples of actions typically associated with conventional threats, i.e., actions relevant to security rather than resiliency or defensibility.

Several sources provide information about the APT. NIST SP 800-30 R1 includes a list of attack actions in Table E-2, organized using the stages of the cyber attack lifecycle; these are described in general terms, rather than in terms of specific technologies. The attack patterns included in CAPEC tend to apply to the early stages of the cyber attack lifecycle. STIX and TAXII provide a mechanism for capturing and sharing information about real-world attacks. Publicly available reports such as Mandiant's APT1 [93] and Symantec's Hidden Lynx [94] reports identify publicly available tools used by adversaries and describe observed activities [53] [51]. Sood et al. identify typical actions in criminal attacks [95]. In addition, commercial providers are beginning to offer cyber threat intelligence services [96] [97] [98] [99] [100].[18]

The *effects of prior adversary actions* can be characterized as effects on cyber resources, which effectively increase adversary capabilities. A high-level taxonomy can be used, e.g., acquired privileges, compromised components or systems, knowledge about the technical environment (e.g., network topology, software versions, functional dependencies), and knowledge about operational environment (e.g., mission dependencies on cyber resources). Microsoft's STRIDE taxonomy can also be used [82].[19] The DIMFUI taxonomy [72] [73] identifies six effects on cyber resources: degradation, interruption (e.g., denial of service), modification, fabrication, unauthorized use (including compromise of an identity, a component, or a system), and interception (which includes gaining knowledge about the technical and/or operational environment). Note that when the effects of prior adversary actions can be situated in a technical and/or operational setting – i.e., described in terms of *which* specific cyber resources are affected, rather than in terms of the types of resources that are affected – the description becomes highly concrete, and can be tied to mission or operational effects.[20]

The *extent* of a cyber attack[21] can be characterized in terms of scale and timeframe. For ease of discussion, these two factors can be used to define four broad extents:

- Isolated (e.g., a single incident), focused on a specific target organization or mission.
- Bounded in time and scope. These include brief coordinated attacks on a specific organization or sector.
- Persistent. These are campaigns, attributable to a single actor or set of actors, focused on a specific target organization or mission. A persistent cyber attack typically seeks to exfiltrate sensitive information, provide direct benefits to the adversary (e.g., criminal

[18] See Table 20 of [142] for a list of sources of data and statistics on cyber incidents, data breaches, and cyber crime.
[19] While CAPEC provides a list of technical impacts, these are meaningful primarily in the context of CAPEC-specified attack patterns (adversary actions).
[20] Note that assessment of operational or mission effects is a key part of OT&E [135].
[21] For non-adversarial threats, extent corresponds to *range of effects* in Appendix D of NIST SP 800-30 R1; isolated corresponds to Low, while Extensive corresponds to Very High in Table D-6.

fraud), or achieve mission impacts (e.g., denial of mission-critical functionality, falsification of mission data).

- Large-scale. These include stealthy campaigns against multiple organizations (e.g., APT1 [93]), as well as more visible attacks involving worms, viruses, or botnets that extend over months or years.

One check of the realism of a claims or evaluation environment is to check the consistency of adversary characteristics and behavior, i.e., whether an adversary with the stated characteristics could or would execute the types of attack the behavior represents.

3.2 Technical Aspects

Technical aspect can be described in terms of technical architecture, management and cyber defense tools, and technical vulnerabilities. Note that describing technical aspects is part of Step 2 in the Cybersecurity DT&E Process [5], Characterize the Attack Surface.

The *technical architecture* can include specification or identification of

- The layer or layers in a notional layered architecture that are considered. For example, Table 2 in [101] identifies the following layers: hardware / firmware; networking / communications; system / network component; operating system; cloud, virtualization, and/or middleware infrastructure; mission / business function application / service; software (e.g., supporting services such as identity and access management); information stores; information streams / feeds; systems; and systems-of-systems.
- The technologies (e.g., Web, Java, cloud) that are assumed or represented. Technologies can be described in terms of technical standards or specified in terms of product suites. Alternately, technologies can be described in more general terms (e.g., “UNIX-like” rather than specifying a specific UNIX version).
- The functionality or capabilities that are assumed to be provided. Capabilities can be described in terms of standards (e.g., security capabilities described in terms of NIST SP 800-53 R4 controls) or using more general terms (e.g., names of control families).
- Technical aspects of the intended deployment environment. For example, technical aspects of the intended deployment environment that are part of the scoping conditions identified in Section 3.2 of NIST SP 800-53 R4 [102] include data connectivity, limited functionality, non-persistence, and whether the technology is inherently single-user.

The technical architecture can also include representations (frequently in the form of schematic drawings) of

- Components (e.g., servers, routers, end-user devices).
- Connectivity or interfaces between components. Representations of interfaces can range from general terms to full specifications in terms of standards, settings, and performance levels.
- Functionality or capabilities allocated to components.

Management and cyber defense *tools* can be identified in terms of types (e.g., performance monitoring, security management, intrusion detection, resilience techniques) or capabilities (e.g., activities as identified in Table 12 of [101]). Representations of tools can range from general

characterization to identification of specific tools by name and version, and can include identification of the capabilities provided by or allocated to different tools.

Technical vulnerabilities (when assumed or represented) can be identified in general terms, by reference to CVE entries, or by describing how they can be exploited. In addition, assumptions can be made about the absence of vulnerabilities, i.e., by identifying components or services that are assumed to be trusted or correctly implemented.

The following figure illustrates how different evaluation environments might be characterized in terms of the concreteness and comprehensiveness of their representations of technical aspects. (See Appendix B for definitions of the degrees of concreteness and comprehensiveness shown on the axes.)

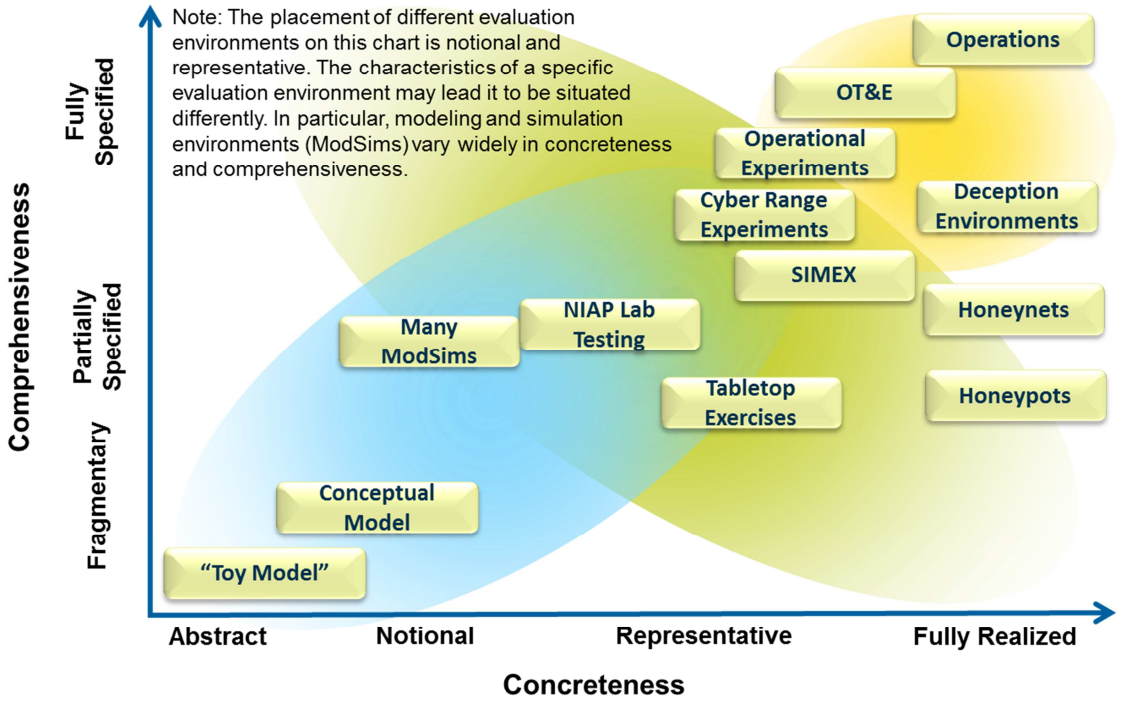

Figure 3. Notional Concreteness and Comprehensiveness of the Technical Aspects of the Environment

3.3 Operational Aspects

Operational aspects can be described in terms of the operational architecture and possible cyber defender decisions.

3.3.1 Operational Architecture

The operational architecture consists of a mission / operational architecture and a cyber management / cyber defender architecture.

The *mission / operational architecture* identifies missions or business functions, *tasks*, and their relative priorities, and can also identify mission or functional roles. In terms of the DoD Architecture Framework (DoDAF), the mission / operational architecture can be described using Operational Viewpoints (OVs) [103]. The mission / operational architecture can also include mappings to the technical architecture, identifying *task dependencies* on cyber resources (e.g.,

processes, information flows, and the systems, subsystems, components, and connectivity that provide these). Note that in an operational setting, such mappings are typically produced by a Business Impact Analysis (BIA), Mission Impact Analysis (MIA), or Crown Jewels Analysis (CJA), and can be represented dynamically as part of situational awareness (SA).

A description of the mission / operational architecture can also include identification of *weaknesses and scoping considerations*, in particular

- Potential or known errors by mission users that
    - Could affect cyber security, defensibility, or resiliency (e.g., connection of an unauthorized device).
    - Could affect mission performance by erroneous use of security mechanisms (e.g., inadvertent lockout of an account or a resource).
- Vulnerabilities in the implementation of physical, procedural, and organizational controls.
- Scoping considerations that determine whether and how security controls might apply, such as mobility. These can also be characterized as risk factors or predisposing conditions in the physical, procedural, and organizational environment, such as physical location. (See Section 3.2 of NIST SP 800-53 R4 [102] for a discussion of scoping considerations, and Appendix F of NIST SP 800-30 R1 [67] for a discussion of predisposing conditions.)

Identification of errors, vulnerabilities, and predisposing conditions is most relevant to claims about operational benefits and impacts, and to operational evaluation environments.

The *management / cyber defender architecture* identifies key roles and responsibilities for management and cyber defense[22]. Operational staff can be characterized in terms of expertise and the SOPs or cyber playbooks they use. The management / defender architecture can also include mappings to the technical architecture, to identify who's in charge of what, who coordinates with whom, and task dependencies (mapped to the technical architecture) for defensive tasks.

3.3.2 Possible Defender Decisions or Actions

Possible defender decisions can be characterized or described in terms of the venue of action / decision and of intended effects. The range of possible venues determines the overall comprehensiveness of representation, with a focus on a single venue (i.e., use of a given solution consisting of a technology or set of technologies) being typical; for any venue, actions or decisions can be described with varying degrees of concreteness. The set of intended effects can be used to determine the comprehensiveness within the chosen venue(s), and can also be used to define measures of effectiveness (MOEs) for the solution. For technical actions in an operational environment, response taxonomies or lists of possible responses can be identified.

The *venue* of action / decision characterizes how, where, and/or by whom the action or decision is taken, including

- Operational. Decisions or actions in this venue can be technical (i.e., using automated tools), procedural, or physical.

[22] See, for example, [129]; "cyber defense" includes Protect and Defend, Investigate, Operate and Collect, and Analyze, while "cyber management" includes Securely Provision and Operate and Maintain.

- Implementation / static configuration. Decisions or actions in this venue can take the form of changes to static configuration settings or to how technologies are implemented, and are typically intended to mitigate technical vulnerabilities. Many of the solutions and mitigations identified in CAPEC are of this form.
- Architectural. Decisions in this venue involve changing the technical architecture (for example, by using a cyber resiliency technique such as segmentation [104]).
- Organizational. Decisions in this venue involve changes to policies and organizational processes, which can in turn lead to architectural, implementation, or operational changes.

Intended effects can be identified in several ways: in terms of the effects on services provided by cyber resources, on the adversary's activities, or on risk and/or resilience.

- *Intended effects on services* provided by cyber resources can include[23]
  - Terminate. A service can be terminated, potentially with negative impacts on mission capabilities. For example, a process or service can be ended or forced to quit, a network connection can be terminated (e.g., by shutting off a port or protocol), a device can be shut down or disconnected, or data can be deleted.
  - Restrict. Use of a service can be restricted, potentially with usability or performance impacts. For example, the privileges required to use a resource can be made more stringent, or network throughput can be limited.
  - Alter. Some aspect of the resources providing the service can be changed, potentially with impacts on visibility or predictability. For example, a Moving Target defense can relocate a process, service, or virtual machine; previously visible traffic can be encrypted; configuration settings or encryption keys can be changed. Note that alteration can be proactive, e.g., resources can be hardened.
  - Restore. The service can be restored, e.g., by using mechanisms to reconstitute or recover resources.
  - Observe. Monitoring of the use of the service, or of the resources that provide or support it, can be increased or refocused.

  Other characterizations of effects on a system, its components, and the services it offers include rollback, rollforward, isolation, reconfiguration, and reinitialization [105] and response goals such as "catch the attack, analyze the attack, mask the attack from users, sustain service, maximize data integrity, maximize data confidentiality, or minimize cost" [106].
- *Intended effects on the adversary* can be described in terms of the vocabulary proposed in [4], which includes mapping those effects to stages in the cyber attack lifecycle.
- *Intended effects on risk and/or resilience* can be described in terms of risk factors affected (e.g., changes in vulnerability or consequence severity) and/or in terms of resilience goals or objectives better achieved. The list of activities in Table 12 of [101]

[23] These can be mapped to the functions of Intrusion Detection and Protection Systems (IDPSs) in the draft NIST SP 800-94 R.1 [130] as follows: Observe to "record information related to observed events, notify security administrators of important observed events, and produce reports", Terminate to "stopping the attack itself," Restrict, Alter, and Restore to "changing the security environment (e.g., reconfiguring a firewall)," and Alter to "changing the attack's content."

provides examples of defender actions (described in general terms), mapped to cyber resiliency techniques.

No single list or taxonomy of possible defender actions / decisions has been developed, although some partial approaches can be found in the intrusion response literature. One approach to a taxonomy of response methods is temporal: in what time frame is the response taken [107] [108]? A more common categorization is passive and active (which can be proactive or reactive) [108]. While some intrusion response research anticipates having a response taxonomy and library, lists are currently incomplete [109]. Solutions and mitigations are identified in CAPEC, and STIX includes a data structure for Courses of Action (CoAs) [50]; as CoAs are created and shared, a taxonomy or list of possible defender actions can be constructed.

3.4 Examples

This section presents two examples of evaluation environments described using the framework presented above: the RAMBO demonstration and the environment for the Common Criteria evaluation of Microsoft Active Directory Federation Services v2.0. This section also presents an example of assumptions in the claims environment (which were then represented in the synthetic evaluation environment) for TALENT.

The examples illustrate the observation that it is neither feasible or desirable for an evaluation environment to be at the extreme of concreteness (fully realized) or comprehensiveness (fully specified) in all aspects. The value of describing an evaluation environment in terms of the concreteness and comprehensiveness with which it represents threat, technical, and operational aspects arises largely from the *rationale* for the description. That is, the cyber terrain is mapped by making explicit the assumptions – particularly about the threat, but also about the technical architecture, technical vulnerabilities, the operational architecture, and possible cyber defender decisions or actions – which in turn determine whether the results of the evaluation will be meaningful or useful in a given real-world situation.

Similarly, the value of describing a claims environment is to enable determination of whether a given evaluation environment can be used to obtain evidence to confirm or disconfirm claims or hypotheses about a proposed solution. In addition, when integration of multiple solutions is considered, identification of the claims environments for those solutions can help define a common evaluation environment – or can reveal fundamental incompatibilities among the solutions.

3.4.1 RAMBO Demonstration

The RAMBO demonstration, which illustrates how cyber resiliency techniques, as implemented using commercial and prototype technologies, improve mission resilience in the face of activities by an advanced actor, provides an example of a synthetic evaluation environment which can be characterized using the framework described above. The Resiliency Lab includes real-world mission applications, a representative infrastructure (network, security services, performance monitoring and management services, cloud services), and commercial and prototype resiliency technologies.

In terms of its *technical aspects*, the *technical architecture* of MITRE's Resiliency Lab can be characterized as **Representative** and **Fully Specified**;[24] *tools* are **Representative** and **Fully Specified**; and *technical vulnerabilities* are **Fully Realized** but **Fragmentary**.

[24] See Appendix B for definitions of the levels or degrees of concreteness and comprehensiveness.

In terms of its *operational aspects*, the RAMBO demonstration identifies roles and responsibilities, and only those standard operating procedures (SOPs) relevant to the demonstration scenario, for an analyst, staff at a Cyber Operations Center, and staff at a Resiliency Operations Center. Thus, the *operational architecture* of the demonstration can be characterized as **Representative** and **Partially Specified**. Defender actions are **Partially Specified** and **Fully Realized**.

With respect to the *threat aspects* of the cyber terrain, the RAMBO demonstration provides:

- **Partially Specified** and **Representative** depiction of *characteristics*:
    - Capabilities: The adversary is able to develop tailored malware, and to make use of a command and control (C2) network (e.g., botnet).
    - Intent: The adversary's intent is disrupt mission operations, exfiltrate sensitive information, maintain stealthy presence, and hide TTPs.
    - Targeting: The adversary is specifically targeting the mission in the demonstration scenario, and the supporting cyber resources.
- **Partially Specified** and **Fully Realized** set of *attack vectors*, using the cyber attack lifecycle.
- **Partially Specified** and **Highly Concrete** set of cyber *attack actions*. The adversary performs activities in the following attack phases: control; recon, delivery, exploit in the context of control; execute; and maintain.
- Fragmentary or **Minimal** and **Highly Concrete** *extent of attack*. The attack is localized to resources in the demonstration technical environment (key databases and indexes, servers and end-user platforms, as specified in the scenario script).
- **Partially Specified** and **Highly Concrete** *effects of prior adversary actions*. The adversary is assumed to have compromised specific components and to have gained knowledge about technical and operational environment as specified in the scenario script.

3.4.2 Common Criteria Evaluations

In the Common Criteria scheme, the Security Target (ST) for a Target of Evaluation (TOE) includes a description of the security environment, including threats and assumptions about the technical and operational environment. The claims about the TOE presented in the ST are validated in a facility such as those under the U.S. National Information Assurance Program (NIAP).

In terms of *technical aspects*, the *technical architecture* as described in the ST can be characterized as **Fully Realized** and **Fully Specified**, while the technical architecture of systems in which it could be integrated is **Notional** and **Partially Specified**. *Technical vulnerabilities* are not represented, but are sought if validation includes a Vulnerability Assessment Activity.

The validation environment is implemented consistent with the characterization in the ST, and does not include integration into an operational system. Thus, the *operational architecture* of the validation environment can be characterized as **Notional** and **Fragmentary**. *Defender actions* are not considered.

With respect to the *threat aspects* of the cyber terrain, validation of a TOE against its ST provides:

- **Abstract** and **Fragmentary** depiction of *characteristics*: The threat is described in terms of a threat agent (typically characterized in terms of role, e.g., user; administrator; unauthorized user, process, or external IT entity; or malicious user), an asset, and an adverse action. Threat agents may be further described by aspects such as expertise, resource, opportunity, and motivation. Note that the threat is assumed to be conventional, rather than an APT actor.
- **Representative** but **Fragmentary** set of *attack vectors*, included in the list of Threats (i.e., attack actions).
- **Representative** and **Fragmentary** set of cyber *attack actions*. For example, the table below illustrates the threats addressed by Brocade Directors and Switches [110] [111]:

Table 2. Example of Attack Vectors and Actions in a Security Target

Identifier	Description
T.ACCOUNTABILITY	A user may not be held accountable for their actions.
T.ADMIN_ERROR	An authorized administrator may incorrectly install or configure the TOE resulting in ineffective security mechanisms.
T.MASQUERADE	An unauthorized user, process, or external IT entity may masquerade as an authorized entity to gain access to data or TOE resources.
T.TSF_COMPROMISE	A malicious user may cause configuration data to be inappropriately accessed (viewed, modified or deleted).
T.UNAUTH_ACCESS	A user may gain unauthorized access (view, modify, delete) to a storage device.

- No representation of *extent of attack*. Essentially, attacks are assumed to be restricted to the TOE.
- No representation of *effects of prior adversary actions*. However, effects may be identified in the course of executing a Vulnerability Assessment.

3.4.3 TALENT

MIT/Lincoln Lab's TALENT (Trusted dynAmic Logical hEterogeNeity sysTem) research prototype has been studied in a synthetic (laboratory) environment [61]. As illustrated in Figure 4, the description of the TALENT threat model demonstrates how assumptions about threat, technical, and operational aspects can be identified, both explicitly and implicitly.

The threat model in TALENT assumes there is **an external adversary [1] trying to exploit a vulnerability [2]** in the system (either in the OS or the binary of the application) in order **to disrupt the normal operation of a mission critical application [3]**. For simplicity and on-the-fly platform generation, we use a hypervisor (hardware-level virtualization). The threat model assumes **the hypervisor and the hardware of the system are trusted [4]**. Hardware-based cryptographic verification (e.g. using TPM) will check the authenticity of the hypervisor, but we further assume. **the implementation of the hypervisor is bug free [4] The OS-level virtualization logic must also be trusted [4]**. The remaining system (including the OS and the applications), however, is not trusted and may contain vulnerabilities or malicious logic.

It is also assumed that although an attack is feasible against a number of different platforms (OS/architecture combinations), there exist **a platform against which the attack is not applicable [5]**. …

We have chosen **UNIX-like operating systems [6]** as our platform. …

During the migration, the graphical output at the remote machine disappears for about 2 seconds **[7]**.

Adversary Characteristics

- Capability: [1] Access – external, but has established an internal presence; [2] Resources – able to craft exploits
- Intent: [3] Goal of disruption
- Targeting: [3] Targets a mission critical application

Adversary Actions

- [3] Denial of service or corruption attack on an application

Technical Aspects

- Technical Architecture: [4] Virtualization, [6] UNIX-like OS
- Technical Vulnerabilities: [4] Assume no vulnerabilities in hardware, hypervisor, OS-level virtualization; [5] one platform against which attack is not applicable

Operational Aspects

- [3] Mission critical application – [7] need to consider user-visible impacts

Figure 4. TALENT Assumptions

See the TALENT paper for more information on the synthetic evaluation environment.

4 Recommendations for Mapping the Cyber Terrain

A variety of processes have been defined to identify key cyber terrain, critical assets, or crown jewels in operational environments. These are briefly surveyed. However, those processes do not help researchers or evaluators characterize or describe assumptions that define the cyber terrain in which potential solutions could be applied. A set of questions are therefore provided.

4.1 Processes for Identifying Critical Assets

As noted in Section 3.3.1 above, assets in operational environments are typically identified and their criticality determined via a mission impact analysis or business impact analysis, performed in support of contingency planning or continuity of operations (COOP) planning [112]. A variety of processes can be applied, including

- Processes for identifying critical assets as part of emergency management planning [113]. These processes typically identify systems (e.g., within buildings or facilities) as critical assets, rather than component subsystems, services, or devices.
- Failure mode, effects, and criticality analysis (FMECA) [114], which extends failure modes and effects analysis (FMEA). FMECA processes start with an inventory of assets, and by analyzing the possible ways those assets could fail or be compromised and the effects of such failures, determines their relative criticality.
- Processes for identifying critical cyber assets in the electrical power critical infrastructure sector, based on NERC guidance [115].
- Commercial processes for identifying critical cyber assets [116], which can include integration with asset management systems [117].
- A Crown Jewels Analysis (CJA) process [118] [119] or other static analysis processes for cyber mission assurance [120].
- A dynamic process supported by a map-the-mission [121] or enterprise introspection [122] capability, or a simulation technique for mission-aware criticality assessment [123] [124].

These processes use, and sometimes can incorporate alternative, criticality rating algorithms. Research into criticality rating metrics and algorithms is ongoing [125] [126]. The TOPSIS (Technique for Order Preference by Similarity to Ideal Solution) method provides an approach to ranking or rating assets based on criticality [127] [124].

4.2 Recommended Questions

For each aspect of the cyber terrain, the tables in this section present:

- Questions a researcher might use to articulate or clarify assumptions about the environment in which the potential solution being investigated could be used.
- Questions about what is assumed or represented in an evaluation environment, and that could affect the applicability of evidence obtained in that environment.

The discussion in Section 3, and the tables defining levels of concreteness and comprehensiveness in Appendix B, provide additional information that can be used to amplify or clarify the questions. In addition, Tables 3 and 6 identify sources of information that a researcher or evaluator could use to construct a more explicit representation of assumptions about the threat environment and about possible cyber defender actions.

It must be emphasized that the following tables are not and should not be treated as questionnaires, or as outlines for a lengthy treatise on assumptions. As illustrated in the TALENT example described in Section 3.4 above, a concise but clear statement can be unpacked into answers using the framework described in Section 3. Furthermore, for any given research project, product, or evaluation environment, many of these questions will not be answered. However, the ability to state which questions are excluded from consideration – to characterize features of the cyber terrain that will not be mapped – aids in determining whether and how to compare or combine results.

Table 3. Key Cyber Threat Features – Adversary Characteristics

Feature	Research Assumptions	Evaluation Representations or Assumptions	Possible References or Sources of Information
Characteristics	What do you assume about the level of the adversary?		DSB Report [128] for general characterizations
Capabilities	What resources do you assume the adversary has? Do you assume specific tools, the expertise to develop or the financial or political resources to acquire tailored tools, knowledge about the target, or opportunity?		NIST SP 800-30 R1 for general characterizations For DT&E or OT&E, risk assessment reports
	Do you assume the adversary uses tailored attack tools?	Do you allow adversarial actors to develop or tailor attack tools?	Red Team Rules of Engagement
	What do you assume the adversary knows about the target system or component (e.g., products or technologies, functional dependencies, information flows, specific vulnerabilities)?	Do you allow adversarial actors to use system documentation? Do you assume the adversary understands mission dependencies on cyber resources?	Red Team Rules of Engagement
	Do you assume the adversary has specific opportunities? For example, do you assume an outsider, or do you include insiders? Do you assume that any components are compromised due to supply chain attacks?	Do you grant user or administrator access to adversarial actors?	Red Team Rules of Engagement
Intent	What goals do you assume the adversary has?		NIST SP 800-30 R1 for general characterizations
	Do you characterize adversary goals using any taxonomy? If so, do you identify which parts of the taxonomy (if any) are excluded from consideration?		[70] [71] for types of goals 2006 JP 3-13 [74] for IO effects DIMFUI [72] [73] for cyber effects
	Do you describe adversary goals in terms of the technology under consideration? For example, do you identify defeating specific functional capabilities as an adversary goal?	Do you link adversary goals to specific targets in the system or operational environment? For example, do you identify mission-critical resources the adversary might seek to modify or destroy?	(DT&E) Statements of functional security requirements (Operational environments) Results of Mission Impact Analysis, Business Impact Analysis, or Crown Jewels Analysis

Feature	Research Assumptions	Evaluation Representations or Assumptions	Possible References or Sources of Information
	What consequences do you assume the adversary seeks to avoid, and how strongly? For example, do you assume the adversary seeks to avoid detection, revealing TTPs, attribution, or retribution?		Threat intelligence
	Over what timeframe do you assume the adversary to be acting?	What is the maximum length of the time an adversary can act that you can represent?	
Targeting	How persistent do you assume the adversary to be? How strongly do you assume the adversary to be focused on the selected targets? Do you assume the adversary can be deterred, for example by increasing the adversary work factor?		Threat intelligence Publicly available threat reports [51] [52] [53]
	Over what timeframe do you assume the adversary to be acting?	What is the maximum length of time an adversary can act that you can represent?	
	How focused do you assume the adversary to be? Do you assume that the adversary will target specific organizations, missions, systems, or capabilities?		Threat intelligence Publicly available threat reports [51] [52] [53]
	Do you assume the adversary will target specific capabilities or components in a notional architecture?	Do you assume the adversary will target specific cyber resources? Do you assume the adversary will *not* target specific resources?	

Table 4. Key Cyber Threat Features – Adversary Behavior

Feature	Research Assumptions	Evaluation Representations or Assumptions	Possible References or Sources of Information
Attack Vectors	What attack vectors or avenues of attack do you assume? For example, do you focus solely on cyber attack, or do you consider physical / kinetic, social engineering, or supply chain attacks? Do you exclude specific vectors?		Note that assumptions about attack vectors should be consistent with those about capabilities and intent.
	Do you assume only specific types of cyber attack? Do you assume cyber attack actions at a specific layer (e.g., network, application)?	Do you allow or represent attacks that use multiple vectors (e.g., physical as well as cyber, social engineering as well as cyber)?	Types of cyber attack: CAPEC categories, representative attack types [79] [80] [51] (RT) RT Rules of Engagement
Types of Attack	Do you use an attack taxonomy or an attack model such as the cyber attack lifecycle to identify and categorize attack actions? If so, which one, and do you exclude portions of the taxonomy or model? (For example, do you focus solely on reconnaissance or execution?)		Attack taxonomies: See [77] [71] [78] [84] [85] [86] Cyber attack lifecycle: See Section 2.2.3 of [4], NIST SP 800-30 R1 [67], and the Cybersecurity DT&E Guideline [5]
Attack Actions	Where do you get information about assumed or represented attack actions?		Threat intelligence information sharing (commercial offerings include [99] [98] [97] [96]) Publicly available threat reports [51] [52] [53]
	In how much detail can or do you describe adversary actions? More specifically, do you situate the adversary's actions in the technical and operational environment?		Note that the answers to these questions should be consistent with those to questions about targeting.
	Do you assume specific actions, or simply characterize them in terms of type and/or of effects?	Do you represent adversary actions in enough detail that they could be replicated?	
	Do you identify types of resources the adversary targets?	Do you identify specific resources as targets of adversary actions?	
	Do you assume a complete or partial attack scenario (multiple steps in the cyber attack lifecycle), or do you restrict attention to a single adversary action?		

Feature	Research Assumptions	Evaluation Representations or Assumptions	Possible References or Sources of Information
Effects of Adversary Actions	Do you use a taxonomy of possible cyber effects, or do you express your assumptions about possible effects using casual terminology?		STRIDE [82] DIMFUI [72] [73]
	Do you assume or represent any effects of prior adversary action (e.g., knowledge, access)? More specifically, can you situate the adversary's assumed capabilities in the technical and operational environment? For example, using the cyber attack lifecycle, do you assume the adversary has • Mapped the network or scanned the system under attack, to know where target resources are located and what vulnerabilities exist • Developed or acquired tailored attack tools • Delivered malware or placed it in a location from which an authorized user will unwittingly download it • Exploited one or more vulnerabilities and installed malware on a system or component • Directed compromised components to map or scan internally-visible resources, and to move laterally • Achieved specific goals, e.g., exfiltrated data, degraded or denied use of a resource • Removed evidence of activities, or corrupted logs and other records to hide evidence of an ongoing presence		Cyber attack lifecycle: See Section 2.2.3 of [4] Note that the answers to these questions should be consistent with those to questions about capabilities and intent.
	Do you assume specific types of resources have been compromised by the adversary?	(OT&E, RT) Which actual effects, if any, do you allow to occur?	Red Team rules of engagement
Extent	What is the maximum extent of an attack that you consider?		Note that the answers to these questions should be consistent with those to questions about targeting.
	Do you assume the attack will affect only specific types of resources?	Do you assume that the attack will be limited to a specific component, system, or system-of-systems?	
	Do you assume that the attack will be limited in time?		

Table 5. Key Technical Features

Feature	Research Assumptions	Evaluation Environment Assumptions or Representation
Technical Architecture	What layer or layers (e.g., network, application) are considered? Are any capabilities or properties of other layers assumed?	What layers are represented? What is assumed about technologies or components at other layers?
	What supporting technologies are assumed?	What technologies are represented? Are any other technologies assumed but not represented?
	Are technologies identified in terms of specific standards (e.g., IPv4, IPv6)? Are specific products or product suites assumed?	Which specific products or product suites, if any, are provided? Are specific configurations identified?
	To what extent are components and functional relationships among them identified?	How are components and functional relationships among them identified?
Tools	What management and/or cyber defense tools or capabilities are assumed or represented?	
	Are tools or capabilities described, or are specific tools (e.g., Snort) identified?	Which tools are represented? Are specific configurations or uses identified?
Technical Vulnerabilities	What types of technical vulnerabilities are assumed or represented?	
	Are vulnerabilities described in general terms, or by reference to CVE?	Are vulnerabilities assumed or represented generically? Or are vulnerabilities instantiated in actual components?
	What elements of the technical architecture are assumed to be free of vulnerabilities? Are specific layers assumed to be trusted or error-free?	
	Are specific layers, components, or services assumed to be vulnerability-free? If so, which ones?	Are vulnerabilities in specific layers, components, or services out-of-bounds for use in testing or experimentation? If so, which ones?

Table 6. Key Operational Features – Operational Architecture

Feature	Research Assumptions	Evaluation Environment Assumptions or Representation
Mission / Operational Architecture	Is any mission or operational architecture assumed? That is, are types of missions, business functions, or mission tasks assumed in the environment in which the solution will be used?	Is any mission or operational architecture represented? If so, • What types of missions, business functions, or mission tasks are represented, and how (e.g., using OV diagrams)? • Are task dependencies on cyber resources identified, and if so, how? Is the representation dynamic (i.e., part of situational awareness)? • What mission or functional roles are identified?
	Are any operational weaknesses assumed?	Are operational weaknesses or vulnerabilities assumed? Which, if any, are represented, and how?
	What scoping considerations or predisposing conditions are assumed?	What scoping considerations or predisposing conditions are assumed? Which, if any, are represented, and how?
Management / Cyber Defense Architecture	What roles and responsibilities for management are assumed?	What roles and responsibilities for management are assumed or represented? For these, • Are management roles and responsibilities mapped to the technical architecture (i.e., components or systems managed)? • Are management staff characterized in terms of expertise or skill? • Are SOPs represented?
	What roles and responsibilities for cyber defense, if any, are assumed?	What roles and responsibilities for cyber defense are assumed or represented? For these, • How are the cyber defense roles and responsibilities described or specified? Are they described in general terms (e.g., Protect and Defend, Investigate, Operate and Collect, Analyze [129]) or in terms of specific tasks? • Are cyber defense roles and responsibilities mapped to the technical architecture (i.e., components or systems defended, tools used)? • Are cyber defense roles identified at different tiers (e.g., local, regional, enterprise-wide)? • Are roles characterized in terms of expertise or skill (e.g., using [129])? • Are SOPs, cyber CoAs, or cyber playbooks represented?

Table 7. Key Operational Features – Possible Cyber Defender Actions

Feature	Research Assumptions	Evaluation Environment Assumptions or Representation	Possible References or Sources of Information
Venue	In what venues are cyber defender actions assumed to occur? Are defender actions described solely in terms of the solution being considered, or are other venues (e.g., physical) considered?	What venues for cyber defender actions are represented or assumed?	
Intended Effects	How (if at all) are the intended effects of cyber defender actions characterized? For example, are intended effects characterized in terms of effects on the adversary (defensibility), ability to achieve resiliency goals or objectives, ability to achieve security objectives or meet security requirements, or using another taxonomy of response options?		Effects on adversary [4] Support to resilience objectives: Table 12 of [101] Other taxonomies of response options: [130] [105] [106]
	Are metrics for, or forms of evidence of, the intended effects identified? How is success of cyber defender actions described?		Effects on adversary [4] [131] Resilience [132] [131]
Defender Actions	Are specific defender actions (e.g., ways to use the solution being considered) described?	What defender actions are represented or allowed?	Allowed: RT rules of engagement
	Are defender actions drawn from any pre-established list, or from a cyber playbook?		Lists: Table 12 of [101], CoAs in STIX, solutions and mitigations in CAPEC
	Are defender actions situated in the technical and/or operational architectures? For example, are defender actions described in terms of specific technologies, components, or tools?		
	Are defender actions mapped to general responsibilities?		General responsibilities: Protect and Defend, Investigate, Operate and Collect, Analyze [129]

5 Conclusion

Technologies and practices for cyber security, resiliency, and defensibility vary widely in maturity and applicability. Evidence is needed to determine the effectiveness of proposed solutions. In order to obtain that evidence, and subsequently to determine whether the results of analyzing the evidence can be applied to a specific real-world situation, a map of the cyber terrain in which the solution is assumed or intended to be situated is needed. This report presents a framework for characterizing assumptions and evaluation environments – an approach to mapping the cyber terrain.

The framework presented in this report can help determine whether

- Assumptions about features of the cyber terrain (e.g., adversary characteristics and possible adversary actions) are consistent.
- A claim or hypothesis is meaningful to a specific real-world situation or can be evaluated in a given environment.
- A set of claims or hypotheses assume the same environment and thus could be evaluated in a common integration experiment.
- Evidence or analytic results obtained in a given evaluation environment could be used to confirm or disconfirm a given claim or hypothesis.
- A claim or hypothesis supported by evidence from a given evaluation environment could be – or could fail to be – meaningful and relevant to a given real-world situation.

The framework, including the questions and information sources identified in Section 4, can also help clarify the assumptions for DT&E (characterizing the attack surface, identifying likely kill chain activities), as well as red teams in cyber exercises and in operational experiments.

This framework is part of a larger approach to analyzing claims or hypotheses, together with evidence obtained in different evaluation environments, about the effects of defensibility decisions on cyber adversaries' behavior or strategy. However, the framework can also be used to compare claims, and to situate evidence, about security and resiliency.

6 Bibliography

[1] DoD, "Department of Defense Strategy for Operating in Cyberspace," July 2011. [Online]. Available: http://www.defense.gov/news/d20110714cyber.pdf.

[2] B. G. J. Franz III, "Effective Synchronization and Integration of Effects Through Cyberspace for the Joint Warfighter," 14 August 2012. [Online]. Available: http://www.afcea.org/events/tnlf/east12/documents/4V3EffSynchIntEffthruCybrspcforJtWarfighter_forpublicrelease.pdf.

[3] S. Peisert and M. Bishop, "How to Design Computer Security Experiments," in *Proceedings of 2007 World Conference on Information Security Education, IFIP — International Federation for Information Processing, Volume 237*, West Point, NY.

[4] D. Bodeau and R. Graubart, "Characterizing Effects on the Cyber Adversary: A Vocabulary for Analysis and Assessment," The MITRE Corporation, Bedford, MA, 2013.

[5] Office of the DASD (DT&E), "Guidelines for Cybersecurity DT&E, version 1.0," 19 April 2013. [Online]. Available: https://acc.dau.mil/adl/en-US/649632/file/71914/Guidelines%20for%20Cybersecurity%20DTE%20v1.0%2020130419.pdf.

[6] Common Criteria Recognition Arrangement (CCRA) Management Committee, "Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, Version 3.1," September 2012. [Online]. Available: http://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R4.pdf.

[7] U.S. Government, "A Tradecraft Primer: Structured Analysis Techniques for Improving Intelligence Analysis," March 2009. [Online]. Available: https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/Tradecraft%20Primer-apr09.pdf.

[8] University of Foreign Military and Cultural Studies, "Red Team Handbook," April 2012. [Online]. Available: http://usacac.army.mil/cac2/UFMCS/repository/RT_Handbook_v6.pdf.

[9] T. Parker, M. Sachs, T. Miller and M. Devost, "Cyber Adversary Characterization," 2003. [Online]. Available: http://www.blackhat.com/presentations/bh-usa-03/bh-us-03-parker.pdf.

[10] B. J. Wood and R. A. Duggan, "Red Teaming of Advanced Information Assurance Concepts," 2000. [Online]. Available: http://cs.uccs.edu/~gsc/pub/master/sjelinek/doc/research/00821513.pdf.

[11] J. R. Mills, "The Key Terrain of Cyber," *Georgetown Journal of International Affairs,* 2012.

[12] R. Hernandez (LGen), "Concerning Digital Warrior: Improving Military Capabilities in the Cyber Domain," 25 July 2012. [Online]. Available: http://armedservices.house.gov/index.cfm/files/serve?File_id=210e8c59-142f-400a-ad8e-9582207686bc.

[13] D. Fava, J. Holsopple, S. J. Yang and B. Argauer, "Terrain and behavior modeling for projecting multistage cyber attacks," in *Proceedings of the 10th International Conference on Information Fusion*, Quebec, 2007.

[14] G. Jakobson, "Extending Situation Modeling with Inference of Plausible Future Cyber

Situations," in *2011 IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support (CogSIMA)*, Miami Beach, FL, 2011.

[15] P. W. Phister, Jr., "Cyberspace: The Ultimate Complex Adaptive System," *The International C2 Journal, Vol. 4, No. 2*, 2010-2011.

[16] K. Quinn, "Cyber-Location Nexus: Closing the Gap Between the Physical and Cyber Realms and What That Means for GEOINT," 2013. [Online]. Available: http://trajectorymagazine.com/2013-issue-2/item/1458-cyber-location-nexus.html.

[17] USTRANSCOM, "Joint Cyber Center: command and control in the USTRANSCOM cyber domain," 18 March 2013. [Online]. Available: http://www.transcom.mil/news/read.cfm?id=8933.

[18] G. Jakobson, "Mission Cyber Security Situation Assessment Using Impact Dependency Graphs," in *Proceedings of the 14th International Conference on Information Fusion*, Chicago, IL, 2011.

[19] M. Stern, "Cyber Intelligence: Identifying the Threat and Understanding the Terrain in Cyberspace," 10 October 2012. [Online]. Available: http://www.securityweek.com/cyber-intelligence-identifying-threat-and-understanding-terrain-cyberspace.

[20] NSA, "Building a National Program for Cybersecurity Science," The Next Wave, Vol. 19, No.4, 2012. [Online]. Available: http://cps-vo.org/file/6555/download/18505.

[21] M. P. Singh, "Toward a Science of Cybersecurity: Guest Editor's Introduction," *IEEE Computing Now*, January 2013.

[22] P. Hubbard, "Measuring the Appropriateness of Simulation and Live Experiments, RTO-MP-MSG-087," 9 November 2011. [Online]. Available: ftp.rta.nato.int/public//PubFullText/RTO/...///MP-MSG-087-02.docx.

[23] K. S. Killourhy and R. A. Maxion, "Should Security Researchers Experiment More and Draw More Inferences?," in *Proceedings of the 4th Workshop on Cyber Security Experimentation and Test (CSET'11)*, 2011.

[24] M. Ben Salem and S. Stolfo, "On the Design and Execution of Cyber-Security User Studies: Methodology, Challenges, and Lessons Learned," in *Workshop on Cyber Security Experimentation and Test (CSET'11)*, 2011.

[25] S. King, "National and Defense S&T Strategies & Initiatives," 25-26 July 2012. [Online]. Available: http://www.cyber.st.dhs.gov/wp-content/uploads/2012/08/Dr_Steven_King-_ASD_RE.pdf. [Accessed 4 March 2013].

[26] C. V. Wright, C. Connelly, T. Braje, J. C. Rabek, L. M. Rossey and R. K. Cunningham, "Generating Client Workloads and High-Fidelity Network Traffic for Controllable, Repeatable Experiments in Computer Security," in *RAID 2010*, Ottawa, Ontario, 2010.

[27] T. Benzel, "The Science of Cyber Security Experimentation," 19 May 2013. [Online]. Available: http://www.ieee-security.org/grepsec/talks/Testbeds-deter.pdf.

[28] S. Hassell, P. Beraud, A. Cruz, G. Ganga, S. Martin, J. Toennies, P. Vazquez, G. Wright, D. Gomez, F. Pietryka, N. Srivastava, T. Hester, D. Hyde and B. Mastropietro, "Evaluating Network Cyber Resiliency Methods using Cyber Threat, Vulnerability, and Defense Modeling and Simulation," in *Proceedings of MILCOM 2012*, 2012.

[29] S. Martin and S. Hassell, "Cyber Analysis Evaluation Modeling for Operations - Countering the Cyberthreat," 2013. [Online]. Available: Cyber Analysis Modeling Evaluation for Operations (CAMEO) — Countering the Cyberthreat - See more at:

http://www.raytheon.com/newsroom/technology_today/2013_i1/cameo.html#sthash.gYtx3MKS.dpuf.

[30] MITRE, "Cybersecurity Research: Resilient Architectures for Mission and Business Objectives (RAMBO)," 2013. [Online]. Available: http://www.mitre.org/work/cybersecurity/research_program.html.

[31] MITRE, "RAMBO: Resilient Architectures for Mission and Business Objectives," 2012. [Online]. Available: http://www.mitre.org/work/cybersecurity/pdf/rambo.pdf.

[32] MITRE, "The MITRE Corporation Annual Report 2012," 2013. [Online]. Available: http://www.mitre.org/about/annual_reports/mitre_2012_annual.pdf.

[33] G. I. Seffers, "Joint Range Tailors Cyber Training to Warfighter Needs," 1 February 2013. [Online]. Available: http://www.afcea.org/content/?q=node/10644.

[34] DARPA, "National Cyber Range Rapidly Emulates Complex Networks," 13 November 2012. [Online]. Available: http://www.darpa.mil/NewsEvents/Releases/2012/11/13.aspx.

[35] W. Welsh, "National Cyber Range follow-on work goes to Lockheed," 13 November 2012. [Online]. Available: http://defensesystems.com/articles/2012/11/13/lockheed-national-cyber-range-contract.aspx.

[36] T. Benzel, "The DETER Project: Leading-edge Experimental Facilities and Methodologies for the Cyber-Security Research Community," October 2012. [Online]. Available: http://www.cyber.st.dhs.gov/wp-content/uploads/2012/10/Day-1.11-DETER-USC-Benzel.pdf.

[37] B. Van Leeuwen, V. Urias, J. Eldridge, C. Villamarin and R. Olsberg, "Performing Cyber Security Analysis Using a Live, Virtual, and Constructive (LVC) Testbed," in *MILCOM*, 2010.

[38] Merit Network, Inc., "Michigan Cyber Range," 2013. [Online]. Available: http://www.merit.edu/cyberrange/.

[39] iSIGHT Partners, "ThreatSPACE Cyber Range: Practiced Intelligence," 2013. [Online]. Available: http://www.isightpartners.com/products/threatspace/.

[40] Northrop Grumman, "Cyber Test Range," 2013. [Online]. Available: http://www.northropgrumman.com/Capabilities/CyberTestRange/Pages/default.aspx.

[41] Ixia, "Boeing: Cyber Range in a Box," 13 March 2013. [Online]. Available: http://www.youtube.com/watch?v=Eyw0LS473UE.

[42] C. Wright and L. Rossey, "Cyber Measurement Campaign (presentation at the ITEA Technology Review)," 25-27 July 2012. [Online]. Available: http://www.itea.org/~iteaorg/images/pdf/Events/2012_Proceedings/2012_Technology_Review/track1_2_cybermeasurementcampaign_wright.pdf.

[43] J. Wroclawski, J. Mirkovic, T. Faber and S. Schwab, "A Two-Constraint Approach to Risky Cybersecurity Experiment Management," in *Sarnoff Symposium*, Princeton, NJ, 2008.

[44] J. Sonchack, A. J. Aviv and J. M. Smith, "Bridging the Data Gap: Data Related Challenges in Evaluating Large Scale Collaborative Security Systems," in *6th Workshop on Cyber Security Experimentation and Test (CSET'13)*, 2013.

[45] T. Townsend, M. Ludwick, J. McAllister, A. O. Mellinger and K. A. Sereno, "SEI Emerging Technology Center: Cyber Intelligence Tradecraft Project - Summary of Key Findings," January 2013. [Online]. Available:

http://www.sei.cmu.edu/library/assets/whitepapers/citp-summary-key-findings.pdf.

[46] Deputy Secretary of Defense, "Defense Industrial Base Cyber Security," 31 October 2012. [Online]. Available: http://www.acq.osd.mil/dpap/policy/policyvault/OSD012537-12-RES.pdf.

[47] National Council of ISACs, "CIO Cyberthreat Response and Reporting Guidelines," August 2010. [Online]. Available: http://www.isaccouncil.org/images/CIO-Cyberthreat-rptg-guide.pdf.

[48] Defense Cyber Crime Center, "Defense Industrial Base Collaborative Information Sharing Environment," 14 June 2013. [Online]. Available: http://www.dc3.mil/dib-cybersecurity/about-dcise.

[49] W. Ennis, "Defense Security Information Exchange (DSIE): A partnership for the Defense Industrial Base," 29 April 2009. [Online]. Available: http://www.whitehouse.gov/files/documents/cyber/Defense%20Security%20Information%20Exchange%20-%20DSIE%20summary%20-%20William%20Ennis.pdf.

[50] S. Barnum, "Standardizing Cyber Threat Intelligence Information with the STructured Information eXpression (STIX(TM))," 30 May 2013. [Online]. Available: http://stix.mitre.org/about/documents/STIX_Whitepaper_v1.0.pdf.

[51] Verizon, "2013 Data Breach Investigations Report," 22 April 2013. [Online]. Available: http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2013_en_xg.pdf.

[52] Symantec, "2013 Internet Security Threat Report, Volume 18," April 2013. [Online]. Available: http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v18_2012_21291018.en-us.pdf.

[53] Sophos, "Security Threat Report 2013," December 2012. [Online]. Available: http://www.sophos.com/en-us/medialibrary/PDFs/other/sophossecuritythreatreport2013.pdf?id=ee65b697-1d30-4971-b240-ce96b5e529aa&dl=true.

[54] H. Asghari and M. J. Mueller, "Internet Measurements and Public Policy: Mind the Gap," in *6th Workshop on Cyber Security Experimentation and Test*, 2013.

[55] JMETC, "JMETC Brings Readily Available Persistent Connectivity for Joint Distributed Test Events," 9 July 2013. [Online]. Available: https://www.tena-sda.org/download/attachments/6750/JMETC-Connectivity-2013-07-09.pdf?version=1&modificationDate=1373471525000.

[56] Northrop Grumman, "Federate Cyber Range," June 2012. [Online]. Available: http://www.northropgrummaninternational.com/wp-content/uploads/2013/02/Federated-Cyber-Range.pdf.

[57] M. J. Gonzalez, "Joint Experimentation Enables Regional Cyber Protection," 1 February 2013. [Online]. Available: http://www.afcea.org/content/?q=node/10638.

[58] C. Kanich, N. Chachra, D. McCoy, C. Grier, D. Y. Wang, M. Motoyama, K. Levchenko, S. Savage and G. M. Voelker, "No Plan Survives Contact: Experience with Cybercrime Measurement," in *4th Workshop on Cyber Security Experimentation and Test (CSET'11)*, 2011.

[59] Sandia, "Red Team Methodology," 2009. [Online]. Available: http://www.idart.sandia.gov/methodology/index.html.

[60] D. Levin, "Lessons Learned in Using Live Red Teams in IA Experiments," Proceedings of

the DARPA Information Survivability Conference and Exposition (DISCEX'03), April 2003. [Online]. Available: http://www.bbn.com/resources/pdf/RedTeamExptsPaper-Levin10-02.pdf.

[61] H. Okhravi, E. I. Robinson, A. Cornella, S. Yannalfo, P. W. Michaleas and J. Haines, "TALENT: Dynamic Platform Heterogeneity for Cyber Survivability of Mission Critical Applications," 29 October 2010. [Online]. Available: http://web.mit.edu/ha22286/www/papers/conference/TALENT_Dynamic_Platform_Heterogeneity_for_Cyber_Survivability_of_Mission_Critical_Applications.pdf.

[62] P. Beraud, A. Cruz, S. Hassell and S. Meadows, "Using Cyber Maneuver to Improve Network Resiliency," in *MILCOM*, Baltimore, MD, 2011.

[63] J. Yang and Y. Chen, "Toward attack-resistant localization under infrastructure attacks," *Security and Communications Networks*, vol. 5, pp. 384-403, 2012.

[64] Wombat Security Technologies, "An Empirical Evaluation of PhishGuru Embedded Training," April 2009. [Online]. Available: http://www.wombatsecurity.com/assets/files/pg-whitepaperC.pdf.

[65] P. Kumaraguru, J. Cranshaw, A. Acquisti, L. Cranor, J. Hong, M. A. Blair and T. Pham, "School of phish: a real-world evaluation of anti-phishing training," in *Proceedings of the 5th Symposium on Usable Privacy and Security (SOUPS'09)*, 2009.

[66] D. D. Caputo, S. L. Pfleeger, J. D. Freeman and M. E. Johnson, "Going Spear Phishing: Exploring Embedded Training and Awareness," *IEEE Security and Privacy*, p. DOI 10.1109/MSP.2013.106, (to appear).

[67] NIST, "Guide for Conducting Risk Assessments, NIST SP 800-30 Rev.1," September 2012. [Online]. Available: http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf.

[68] D. Bodeau, J. Fabius-Greene and R. Graubart, "How Do You Assess Your Organization's Cyber Threat Level?," August 2010. [Online]. Available: http://www.mitre.org/work/tech_papers/2010/10_2914/10_2914.pdf.

[69] D. Bodeau, R. Graubart and J. Fabius-Greene, "Improving Cyber Security and Mission Assurance via Cyber Preparedness (Cyber Prep) Levels," in *IEEE International Conference on Privacy, Security, Risk and Trust*, 2010.

[70] NERC, "Cyber Attack Task Force Final Report," 26 March 2012. [Online]. Available: http://www.nerc.com/docs/cip/catf/12-CATF_Final_Report_BOT_clean_Mar_26_2012-Board%20Accepted%200521.pdf.

[71] K. Harrison and G. White, "A Taxonomy of Cyber Events Affecting Communities," in *Proceedings of the 44th Hawaii International Conference on System Sciences*, 2011.

[72] S. Musman, A. Temin, M. Tanner, D. Fox and B. Pridemore, "Evaluating the Impact of Cyber Attacks on Missions (PR Case No. 09-4577)," 2009. [Online]. Available: http://198.49.146.10/work/tech_papers/2010/09_4577/09_4577.pdf.

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

[74] Joint Chiefs of Staff, "Joint Publication (JP) 3-13, Information Operations," 13 February 2006. [Online]. Available: http://www.carlisle.army.mil/DIME/documents/jp3_13.pdf.

[75] P. Phister, "Mission Effectiveness: Proposed Nth Order Taxonomy," in *17th International Command and Control Research and Technology Symposium*, 2012.

[76] G. Schudel and B. Wood, "Modeling Behavior of the Cyber-Terrorist," in *Research on Mitigating the Insider Threat to Information Systems #2*, Santa Monica, CA.

[77] C. Simmons, C. Ellis, S. Shiva, D. Dasgupta and Q. Wu, "AVOIDIT: A Cyber Attack Taxonomy, University of Memphis, Technical Report CS-09-003," 2009. [Online]. Available: http://issrl.cs.memphis.edu/files/papers/CyberAttackTaxonomy_IEEE_Mag.pdf.

[78] M. Uma and G. Padmavathi, "A Survey on Various Cyber Attacks and their Classification," *International Journal of Network Security, Vol.15, No.6*, pp. 391-397, November 2013.

[79] J. Wynn, J. Whitmore, G. Upton, L. Spriggs, D. McKinnon, R. McInnes, R. Graubart and L. Clausen, "Threat Assessment and Remediation Analysis (TARA) Methodology Description, V. 1.0 (MTR 110176, PR 11-4982)," October 2011. [Online]. Available: http://www.mitre.org/work/tech_papers/2012/11_4982/11_4982.pdf. [Accessed 2 January 2013].

[80] M. Mateski, C. M. Trevino, C. Veitch, J. Michalski, J. M. Harris, S. Maruoka and J. Frye, "Cyber Threat Metrics, SAND2012-2427," Sandia National Laboratories, Albuquerque, NM, 2012.

[81] MITRE, "CAPEC: Common Attack Pattern Enumeration and Classification," 2013. [Online]. Available: http://capec.mitre.org/.

[82] Microsoft, "Designing for securability," 2013. [Online]. Available: http://msdn.microsoft.com/en-us/library/aa291875(v=vs.71).aspx.

[83] OWASP Foundation, "OWASP Testing Guide," 2008. [Online]. Available: https://www.owasp.org/images/5/56/OWASP_Testing_Guide_v3.pdf.

[84] C. Meyers, S. Powers and D. Faissol, "Taxonomies of Cyber Adversaries and Attacks: a Survey of Incidents and Approaches (LLNL-TR-419041)," April 2009. [Online]. Available: https://www-eng.llnl.gov/pdfs/taxonomies.pdf.

[85] B. Gourley, "Enhancing Collective Defense with Taxonomies for Operational Cyber Defense," CTO Vission, 15 August 2011. [Online]. Available: http://ctovision.com/2011/08/enhancing-collective-defense-with-taxonomies-for-operational-cyber-defense/.

[86] Z. Wu, Y. Ou and Y. Liu, "A Taxonomy of Network and Computer Attacks Based on Responses," in *2011 International Conference of Information Technology, Computer Engineering and Management Sciences*, 2011.

[87] Web Application Security Consortium, "WASC Threat Classification, Version 2.0," 1 January 2010. [Online]. Available: http://projects.webappsec.org/f/WASC-TC-v2_0.pdf.

[88] K. Kotapati, P. Liu, Y. Sun and T. F. LaPorta, "A Taxonomy of Cyber Attacks on 3G Networks," in *Proceedings of the 2005 IEEE international conference on Intelligence and Security Informatics* , 631-633, 2005.

[89] B. Zhu, A. Joseph and S. Sastry, "A Taxonomy of Cyber Attacks on SCADA Systems," in *Proceedings of the 2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing*, 2011.

[90] T. Fleury, H. Khurana and V. Welch, "Toward a Taxonomy of Attacks Against Energy Control Systems," in *Proceedings of the IFIP International Conference on Critical Infrastructure Protection*, 2008.

[91] M. Yampolskiy, P. Horvath, X. D. Koutsoukos, Y. Xue and J. Sztipanovits, "Systematic

Analysis of Cyber-Attacks on CPS - Evaluating Applicability of DFD-based Approach," in *5th International Symposium on Resilient Control Systems (ISRCS)*, 2012.

[92] NIATEC, "Common Criteria Tools," [Online]. Available: http://134.50.70.12/cctools.htm.

[93] Mandiant, "APT1: Exposing One of China's Cyber Espionage Units," 18 February 2013. [Online]. Available: http://www.mcafee.com/us/resources/reports/rp-threat-predictions-2013.pdf. [Accessed 12 March 2013].

[94] S. Doherty, J. Gegeny, B. Spasojevic and J. Baltazar, "Hidden Lynx - Professional Hackers for Hire, Version 1.0," 17 September 2013. [Online]. Available: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/hidden_lynx.pdf.

[95] A. K. Sood, R. Bansal and R. J. Enbody, "Cybercrime: Dissecting the State of Underground Enterprise," *IEEE Internet Computing, Vol. 17, No. 1*, pp. 60-68, January-February 2013.

[96] CrowdStrike, "Falcon Intelligence: Actionable & Comprehensive Security Intelligence," 2013. [Online]. Available: http://www.crowdstrike.com/falcon-intelligence/index.html.

[97] iSIGHT Partners, "ThreatScape: Comprehensive Cyber Threat Intelligence," 2013. [Online]. Available: http://www.isightpartners.com/products/threatscape/.

[98] Cyber Squared, "Threat Connect," 2013. [Online]. Available: http://www.threatconnect.com/.

[99] AlienVault, "Open Threat Exchange," 2013. [Online]. Available: http://www.alienvault.com/open-threat-exchange.

[100] C. Blake, "Announcing HP Threat Central security intelligence platform," 17 September 2013. [Online]. Available: http://h30499.www3.hp.com/t5/HP-Security-Products-Blog/Announcing-HP-Threat-Central-security-intelligence-platform/ba-p/6186875.

[101] D. Bodeau and R. Graubart, "Cyber Resiliency Assessment: Enabling Architectural Improvement (MTR 120407, PR 12-3795)," May 2013. [Online]. Available: http://www.mitre.org/work/tech_papers/2013/12_3795/12_3795.pdf.

[102] NIST, "Security and Privacy Controls for Federal Information Systems and Organizations (NIST SP 800-53 R4)," April 2013. [Online]. Available: http://dx.doi.org/10.6028/NIST.SP.800-53r4.

[103] DoD CIO, "DoD Architecture Framework Version 2.02," 3 March 2011. [Online]. Available: http://dodcio.defense.gov/Portals/0/Documents/DODAF/DoDAF_v2-02_web.pdf.

[104] D. Bodeau and R. Graubart, "Cyber Resiliency Engineering Framework," September 2011. [Online]. Available: http://www.mitre.org/work/tech_papers/2012/11_4436/11_4436.pdf.

[105] S. A. Zonouz, H. Khurana, W. H. Sanders and T. M. Yardley, "RRE: A Game-Theoretic Intrusion Response and Recovery Engine," in *IEEE/IFIP International Conference on Dependable Systems & Networks (DSN '09)*, 2009.

[106] C. A. Carver, J. M. Hill, J. R. Surdu and U. W. Pooch, "A Methodology for using Intelligent Agents to provide Automated Intrusion Response," in *Proceedings of the IEEE Systems, Man, and Cybernetics Information Assurance and Security Workshop*, 2000.

[107] W. Kanoun, L. Samarji, N. Cuppens-Boulahia, S. Dubus and F. Cuppens, "Towards a Temporal Response Taxonomy," in *Data Privacy Management and Autonomous*

Spontaneous Security, Lecture Notes in Computer Science Vol. 7731, Springer, 2013, pp. 318-331.

[108] N. B. Anuar, M. Papadaki, S. Furnell and N. Clarke, "An investigation and survey of response options for Intrusion Response Systems (IRSs)," in *Information Security for South Africa (ISSA)*, 2010.

[109] A. Shameli-Sendi, N. Ezzati-jivan, M. Jabbarifar and M. Dagenais, "Intrusion Response Systems: Survey and Taxonomy," *International Journal of Computer Science and Network Security*, vol. 12, no. 1, 2012.

[110] Brocade, "Brocade Directors and Switches Security Target," 30 August 2012. [Online]. Available: http://www.commoncriteriaportal.org/files/epfiles/st_vid10376-st.pdf.

[111] NIAP, "Common Criteria Evaluation and Validation Scheme Validation Report: Brocade Directors and Switches (CCEVS-VR-10376-2012)," September 2012. [Online]. Available: http://www.commoncriteriaportal.org/files/epfiles/st_vid10376-vr.pdf.

[112] NIST, "NIST SP 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems," 11 November 2010. [Online]. Available: http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf. [Accessed 19 May 2011].

[113] FEMA, "FEMA 426, Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings," December 2003. [Online]. Available: http://www.fema.gov/pdf/plan/prevent/rms/426/fema426.pdf.

[114] Department of the Army, "Technical Manual No. 5-698-4, Failure Modes, Effects, and Criticality Analyses (FMECA) for Command, Control, Communications, Computer, Intelligence, Surveillance, and Reconnaissance (C4ISR) Facilities," 29 September 2006. [Online]. Available: http://armypubs.army.mil/eng/DR_pubs/dr_a/pdf/tm5_698_4.pdf.

[115] NERC, "Security Guideline for the Electrical Sector: Identifying Critical Cyber Assets," 17 July 2010. [Online]. Available: http://www.nerc.com/fileUploads/File/Standards/Critcal%20Cyber%20Asset_approved%20by%20CIPCl%20and%20SC%20for%20Posting%20with%20CIP-002-1,%20CIP-002-2,%20CIP-002-3.pdf.

[116] Verizon, "A New Level of Security for Your Business: Taking a Business Process Approach to Assets and Risk," 2011. [Online]. Available: http://www.verizonenterprise.com/resources/whitepaper/wp_a-new-level-of-security-for-your-business_en_xg.pdf.

[117] RSA, "RSA Asset Criticality Intelligence: Adding business context to security alerts," 2012. [Online]. Available: https://community.emc.com/docs/DOC-26497 or http://webobjects.cdw.com/webobjects/media/pdf/rsa/7044_RSA_Asset_Criticality_Intelligence_ACI_Datasheet.pdf.

[118] The MITRE Corporation, "Systems Engineering Guide: Crown Jewels Analysis," 2011. [Online]. Available: http://www.mitre.org/publications/systems-engineering-guide/enterprise-engineering/systems-engineering-for-mission-assurance/crown-jewels-analysis.

[119] J. Watters, S. Morrissey, D. Bodeau and S. C. Powers, "The Risk-to-Mission Assessment Process (RiskMAP): A Sensitivity Analysis and an Extension to Treat Confidentiality Issues," July 2009. [Online]. Available: http://www.mitre.org/sites/default/files/pdf/09_2994.pdf.

[120] M. D. Pritchett, "Cyber Mission Assurance: A Guide to Reducing the Uncertainties of Operating in a Contested Cyber Environment," 14 June 2012. [Online]. Available: http://www.dtic.mil/get-tr-doc/pdf?AD=ADA563712.

[121] Wright-Patterson Air Force Base, "User Needs Drive Air Space Cyber-User Defined Operational Picture," 2 April 2012. [Online]. Available: http://www.wpafb.af.mil/news/story.asp?id=123296337.

[122] T. E. Carroll, "Kritikos: Identifying Cyber Assets and Inferring Criticality in Terms of Business Processes," July 2013. [Online]. Available: http://cybersecurity.pnnl.gov/documents/projects/Carroll.pdf.

[123] H. Cam and P. Mouallem, "Mission-Aware Time-Dependent Cyber Asset Criticality and Resilience," in *Proceedings of the 8th CSIIRW Cyber Security and Information Intelligence Research Workshop*, Oak Ridge National Lab, Oak Ridge, TN, 2013.

[124] H. Cam, "PeerShield: Determining Control and Resilience Criticality of Collaborative Cyber Assets inNetworks," in *Cyber Sensing 2012, SPIE Defense, Security, and Sensing*, Baltimore, MD, 2012.

[125] R. Sawilla and X. Ou, "Identifying critical attack assets in dependency attack graphs, DRDC Ottawa TM 2008-180," September 2008. [Online]. Available: http://people.cis.ksu.edu/~xou/publications/drdc08.pdf.

[126] Y. Park, C. Gates and S. C. Gates, "Estimating Asset Sensitivity by Profiling Users," in *ESORICS 2013*, 2013.

[127] A. Kim and M. H. Kang, "NRL/MR/5540--11-9350: Determining Asset Criticality for Cyber Defense," 23 September 2011. [Online]. Available: http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA550373.

[128] DoD Defense Science Board, "Task Force Report: Resilient Military Systems and the Advanced Cyber Threat," January 2013. [Online]. Available: http://www.acq.osd.mil/dsb/reports/ResilientMilitarySystems.CyberThreat.pdf.

[129] NICE, "National Initiative for Cybersecurity Education Cybersecurity Workforce Framework," 6 February 2013. [Online]. Available: http://csrc.nist.gov/nice/framework/national_cybersecurity_workforce_framework_03_2013_version1_0_for_printing.pdf.

[130] NIST, "DRAFT NIST SP 800-94 R.1, Guide to Intrusion Detection and Prevention Systems (IDPS)," 25 July 2012. [Online]. Available: http://csrc.nist.gov/publications/drafts/800-94-rev1/draft_sp800-94-rev1.pdf.

[131] S. Marra, S. Hassell, C. Eck, J. (. Moody, S. R. Martin, G. Ganga, K. Harward, E. Rickard, J. Sandoval and J. Brown, "Cyber Resiliency Metrics for Discussion," 14 June 2013. [Online]. Available: http://bbn.com/resources/pdf/whitepaper_CyberResiliencyMetricsMASTERv4.pdf.

[132] D. Bodeau, R. Graubart, L. LaPadula, P. Kertzner, A. Rosenthal and J. Brennan, "Cyber Resiliency Metrics," April 2012. [Online]. Available: https://registerdev1.mitre.org/sr/12_2226.pdf.

[133] Assistant Secretary of Defense for Research and Engineering (ASD(R&E)), "Technology Readiness Assessment (TRA) Guidance," 13 May 2011. [Online]. Available: http://www.acq.osd.mil/ddre/publications/docs/TRA2011.pdf.

[134] S. Hansman and R. Hunt, "A taxonomy of network and computer attacks," *Computers and Security*, pp. 31-43, February 2005.

[135] DOT&E, "Test and Evaluation of Information Assurance in Acquisition Programs," 1 February 2013. [Online]. Available: http://www.dote.osd.mil/pub/policies/2013/2013-02-01_TE_of_IA_in_Acq_Programs(6079).pdf.

[136] T. Benzel, "The Science of Cyber Security Experimentation: The DETER Project," in *Annual Computer Security Applications Conference (ACSAC)*, 2011.

[137] B. Oosterloo, "Managing Social Engineering Risk," 6 October 2008. [Online]. Available: http://essay.utwente.nl/59233/1/scriptie_B_Oosterloo.pdf.

[138] CNSS, "National Information Assurance (IA) Glossary (CNSS Instruction No. 4009)," 26 April 2010. [Online]. Available: https://www.cnss.gov/Assets/pdf/cnssi_4009.pdf.

[139] M. J. McDonald, G. N. Conrad, T. C. Service and R. H. Cassidy, "Cyber Effects Analysis Using VCSE: Promoting Control System Reliability, Sandia Report SAND2008-5954," September 2008. [Online]. Available: http://energy.sandia.gov/wp/wp-content/gallery/uploads/Cyber_Effects_Analysis_Using_VCSE_09.pdf.

[140] T. Edgar, T. Carroll and D. Manz, "Challenges of Cybersecurity Research in a Multi-user Cyber-Physical Testbed," 23 April 2012. [Online]. Available: http://csrc.nist.gov/news_events/cps-workshop/cps-workshop_abstract-5_pnnl.pdf.

[141] J. Malas, B. Nolte and J. Jackson, "Limitations of Readiness Levels," 26 October 2011. [Online]. Available: http://www.dtic.mil/ndia/2011system/13131_MalasTuesday.pdf.

[142] R. Tehan, "Cybersecurity: Authoritative Reports and Resources, Congressional Research Service Report R42507," 25 October 2013. [Online]. Available: http://www.fas.org/sgp/crs/misc/R42507.pdf.

Appendix A Acronyms

AF	Air Force
APT	Advanced Persistent Threat
CAPEC	Common Attack Pattern Enumeration and Classification
CCRA	Common Criteria Recognition Arrangement
CERT	Computer Emergency Response Team
CIO	Chief Information Officer
CNSS	Committee on National Security Systems
CoA	Course of Action
CPS	Cyber-Physical Systems
CRS	Congressional Research Service
CSET	(Workshop on) Cyber Security Experimentation and Test
CVE	Common Vulnerabilities and Exposures
CWE	Common Weaknesses Enumeration
DARPA	Defense Advanced Research Projects Agency
DHS	Department of Homeland Security
DIB	Defense Industrial Base
DIMFUI	Degradation, Interruption, Modification, Fabrication, Unauthorized Use, Interception
DLP	Data Loss Prevention
DoD	Department of Defense
DoDAF	DoD Architecture Framework
DOT&E	Director, Operational Test & Evaluation
DSB	Defense Science Board
DSIE	Defense Security Information Exchange
DT&E	Developmental Test and Evaluation
FBI	Federal Bureau of Investigation
FMEA	Failure Modes and Effects Analysis
FMECA	Failure Modes, Effects, and Criticality Analysis
ICT	Information and Communications Technology
IDS	Intrusion Detection System
ISAC	Information Sharing and Analysis Center
IT	Information Technology

JCO JT	Joint Cyber Operations Joint Test
JCOR	Joint Cyberspace Operations Range
MOE	Measure of Effectiveness
MT	Moving Target
NCR	National Cyber Range
NERC	North American Electrical Reliability Corporation
NIATEC	National Information Assurance Training and Education Center
NICE	National Initiative for Cybersecurity Education
NIST	National Institute of Standards and Technology
NSF	National Science Foundation
OSD/TRMC	Office of the Secretary of Defense
OT&E	Operational Test & Evaluation
RAID	Recent Advances in Intrusion Detection
RAMBO	Resilient Architectures for Mission and Business Objectives
SIMEX	Simulation Experiment
SIMTEX	Simulator Training and Exercise
SOP	Standard Operating Procedure
SP	Special Publication
STIX	Structured Threat Information eXpression
STRIDE	Spoofing identity, Tampering with data, Repudiability, Information disclosure, Denial of service, Elevation of privilege
T&E	Test and Evaluation
TARA	Threat Assessment and Remediation Analysis
TAXII	Trusted Automated eXchange of Indicator Information
TRA	Technology Readiness Assessment
TRL	Technology Readiness Level
TTPs	Tactics, Techniques, and Procedures
USC ISI	University of Southern California Information Sciences Institute
VM	Virtual Machine

Appendix B Representations of Concreteness and Comprehensiveness

The following tables provide definitions of the degrees of concreteness and comprehensiveness used in Figures 1 and 2.

Table 8. Concreteness and Comprehensiveness of Representation: Adversary Characteristics[25]

Attributes	Degree of Concreteness	Degree of Comprehensiveness
• **Capabilities** • **Intent** • **Targeting** (Note: The adversary characterization can be more fully fleshed out for specific attributes, such as adversary resources, expertise, knowledge, opportunity; goals, avoided consequences; focus, persistence.)	• **Abstract**: Vague or unspecified, using ill-defined terms or levels, if any • **Notional**: General, e.g., using the levels defined in NIST SP 800-30R1 • **Representative**, e.g., using the levels defined in NIST SP 800-30R1, annotated with examples • **Fully Realized**: Highly concrete (e.g., using specific and validated examples, for example from threat intelligence)	• **Fragmentary** or Minimal: some characteristics are not specified; attributes are not identified; a single example is provided • **Partially Specified**: all characteristics are specified; some relevant attributes may be identified and specified; a few examples are provided • **Fully Specified or Extensive**: for each characteristic, relevant attributes are identified and specified, using a taxonomy (of capabilities, intended effects and concerns, and target types, respectively)

Table 9. Concreteness and Comprehensiveness of Representation: Adversary Behavior

Attribute	Alternatives for Concreteness	Alternatives for Comprehensiveness
Attack Vectors	• **Abstract**: General / high-level (e.g., "cyber") • **Notional**: general types of cyber attack vectors identified, e.g., distributed denial of service (DDoS), intrusion • **Representative**: well-defined set of attack vector types identified (note that definitions often include examples) • **Fully realized**: well-defined set of attack vector types identified and situated in the technical / operational environment	• **Fragmentary** or Minimal: subset of cyber, at least one example provided • **Partially Specified**: cyber, no restriction on types of attack actions, a few examples provided • **Fully Specified or Extensive**: cyber, other IO, supply chain, physical / kinetic; multiple examples for each type

[25] Because characteristics and behavior of adversaries cannot be always be known, "Extensive" is offered as an alternative to "Fully Specified" for comprehensiveness.

Attribute	Alternatives for Concreteness	Alternatives for Comprehensiveness
Types of Cyber Attack Actions (using a taxonomy or attack lifecycle framework)	• **Abstract**: General / high-level (e.g., phase in cyber attack lifecycle) • **Notional**: identified using a taxonomy or attack lifecycle framework (e.g., threat events in NIST SP 800-30R1; CAPEC categories, situated using attack prerequisites) • **Representative**: identified using a taxonomy or lifecycle framework, situated in a fragmentary or partial technical / operational environment (e.g., detailed CAPEC attack patterns or attack steps) • **Fully Realized or Highly Concrete**: able to be executed by following a script; situated in representative technical / operational environment (e.g., described in terms of specific observables and indicators)	• **Fragmentary** or Minimal: no more than one example for each type included • **Partially Specified**: at least one example for most types; for types not represented, effects are assumed or represented; at least one complete attack lifecycle or scenario • **Fully Specified or Extensive**: multiple examples for each type; at least two complete attack lifecycles or scenarios
Extent of attack (using a range that includes isolated incidents, uncoordinated attacks, coordinated attacks, and persistent / stealthy campaigns)	• Abstract: Vague/Unspecified • Notional: General (targets characterized) • Representative (targets described) • Highly concrete (specific targets identified)	• **Fragmentary** or Minimal: covering one point in the range, e.g., isolated or localized incidents • **Partially Specified** :covering part of the range, e.g., isolated incidents and uncoordinated attacks • **Fully Specified or Extensive**: covering the full range
Effects of prior adversary actions (For Representative, Highly Concrete, Partial, and Extensive, a taxonomy or vocabulary of possible effects must be identified and used)	• Vague/Unspecified • General (e.g., using undefined but intuitive terms) • Representative (described using the vocabulary) • Highly concrete (described using the vocabulary; situated in terms of the technical and/or operational environment)	• **Fragmentary:** addressing only one type of effect, e.g., access • **Partially Specified**: described in terms of multiple types of effects • **Fully Specified or Extensive**: described in terms of all possible types of effects

Table 10. Completeness and Comprehensiveness of Representation: Technical Environment

Attribute	Degree of Concreteness	Degree of Comprehensiveness
Technical Architecture	• **Abstract:** system described in terms of notional architecture (e.g., boxes and lines) with allocated capabilities • **Notional:** system described in terms of a technical architecture (e.g., specifying technologies, products, standards), with allocated functional capabilities • **Representative:** system described in terms of technical components and connectivity, but lacking real-world / real-time external interfaces and data flows, the full complement of components, and/or the legacy of prior operational configuration decisions • **Fully realized:** system described as it operates in its real-world environment, interfacing with other real-world systems, including the legacy of prior operational configuration decisions	• **Fragmentary:** only the technical attributes relevant to the technology under consideration are specified, and the specification only covers those aspects relevant to the claim • **Partially specified:** technical attributes relevant to the technology and to a range of possible technical environments are specified; e.g., components specified in terms of technical features, standards, and relevant functionality; interfaces specified in terms of standards • **Fully specified:** all identified technical attributes are specified; e.g., components specified in terms of product versions and configuration settings; interfaces specified in terms of standards, settings, and performance
Tools	• **Abstract:** management and defense tools are described in general terms (e.g., security management) • **Notional**: defense tools are described in terms of defensive capabilities (e.g., reconfiguration, isolation) • **Representative**: defense tools are identified by name or described in terms of capabilities provided by commercial products or prototypes • **Fully realized**: defense tools are implemented and configured in the evaluation environment	• **Fragmentary:** only those tool capabilities relevant to evaluating claims or hypotheses are described • **Partially specified**: a set of tools providing a range of defensive capabilities is identified • **Fully specified or Extensive**: a full set of tools, providing defensive capabilities across the range of intended effects, is identified
Technical Vulnerabilities	• **Abstract:** vulnerabilities are described in general terms (e.g., headings in Appendix 2 of [5]) • **Notional:** vulnerabilities are described in terms of bad practices (e.g., entries in Appendix 2 of [5]) • **Representative:** vulnerabilities are described using CVE and CWE • **Fully realized:** vulnerabilities are described in terms of the system as it operates in its real-world environment	• **Fragmentary:** only vulnerabilities addressed by the solution under consideration are identified • **Partially specified:** vulnerabilities relevant to the technologies used in the solution, and in those system components or elements on which the solution depends, are identified • **Fully specified:** all known (or knowable, using existing tools) vulnerabilities in the system in which the solution is intended to be used are identified

Table 11. Concreteness and Comprehensiveness of Representation: Operational Architecture

Attribute	Degree of Concreteness	Degree of Comprehensiveness
Operational Architecture	• **Abstract:**[26] missions and tasks are identified in general or vague terms (e.g., office automation) • **Notional:** mission flows are described in terms of tasks and performers • **Representative:** mission flows are described in terms of tasks, performers, and cyber resources (e.g., technical components and connectivity) on which they depend • **Fully realized:** missions and tasks are performed in a real-world environment; vulnerabilities, predisposing conditions, and errors are described in practical terms (e.g., in SOPs)	• **Fragmentary:** only missions and tasks relevant to the claim (if any) are identified • **Partially specified:** high-priority or critical missions and tasks are described; predisposing conditions are identified • **Fully specified:** all missions and tasks are identified, whether critical, essential, supporting, or ancillary; predisposing conditions and vulnerabilities are identified
Management / Cyber Defender Architecture	• **Abstract:** roles, responsibilities, and expertise are identified in general or vague terms (e.g., system administrator) if at all • **Notional:** key roles and responsibilities for management and defense are identified • **Representative:** key roles and responsibilities for management and cyber defense are identified and (if possible) expressed in terms of components of the technical architecture or in terms of scope and hierarchy (e.g., local, regional, enterprise-wide), and expertise is described in general terms • **Fully realized:** roles, responsibilities, and expertise for management and cyber defense are described and expressed in terms of components of the technical architecture, with supporting information provided in SOPs, cyber playbooks	• **Fragmentary:** only roles needed by the solution under consideration are identified • **Partially specified:** roles and responsibilities for cyber defense are identified • **Fully specified:** roles, responsibilities, and required expertise for management and cyber defense are identified

Table 12. Concreteness and Completeness of Representation: Defender Actions

Degree of Concreteness	Degree of Comprehensiveness
• **Abstract:** defender actions are identified in terms of venue • **Notional:** defender actions are identified in terms of venue and intended effects, described in general terms • **Representative:** defender actions are described in terms of venue and intended effects, using representative examples • **Fully realized:** defender actions are described in practical terms (e.g., in SOPs or in a cyber playbook)	• **Fragmentary:** at least one possible defender action is identified • **Partially specified:** all venues relevant to the solution are identified; several possible defender actions are identified • **Fully specified:** all venues relevant to the solution are identified; a list of possible defender actions is provided, and intended effects are specified in a way that enables MOEs to be defined

[26] The degrees of concreteness correspond roughly to levels of Operational Viewpoint: Abstract to OV-1, Notional to OV-2 or OV-5, and Representative to OV-6c. A Fully Realized operational architecture is manifest in an operational system or system-of-systems.