MITRE TECHNICAL REPORT MTR130432

MITRE

Characterizing Effects on the Cyber Adversary

A Vocabulary for Analysis and Assessment

Project No.: 51MSR615-DA

Deborah Bodeau
Richard Graubart

November 2013

Bedford, MA

Abstract

This paper presents a vocabulary for stating claims or hypotheses about the effects of cyber mission assurance decisions on cyber adversary behavior. Cyber mission assurance decisions include choices of cyber defender actions, architectural decisions, and selections and uses of technologies to improve cyber security, resiliency, and defensibility (i.e., the ability to address ongoing adversary activities). The vocabulary enables claims and hypotheses to be stated clearly, comparably across different assumed or real-world environments, and in a way that suggests evidence that might be sought but is independent of how the claims or hypotheses might be evaluated. The vocabulary can be used with multiple modeling and analysis techniques, including Red Team analysis, game-theoretic modeling, attack tree and attack graph modeling, and analysis based on the cyber attack lifecycle (also referred to as cyber kill chain analysis or cyber campaign analysis).

This page intentionally left blank.

Executive Summary

This paper presents a vocabulary for stating claims or hypotheses about the effects of cyber mission assurance decisions on cyber adversary behavior. Cyber mission assurance decisions include choices of cyber defender actions, architectural decisions, and selections and uses of technologies to improve cyber security, resiliency, and defensibility (i.e., the ability to address ongoing adversary activities). The vocabulary enables claims and hypotheses to be stated clearly, comparably across different assumed or real-world environments, and in a way that suggests evidence that might be sought but is independent of how the claims or hypotheses might be evaluated.

Multiple vocabularies have been used to describe effects on adversary behavior, for example by researchers, product or solution vendors, and cyber threat analysts. However, these have been incomplete (e.g., adversary work factor) or tied to specific modeling or analysis techniques (e.g., game-theoretic models), making comparisons difficult or limiting how claims can be evaluated. The vocabulary presented in this paper can be used with multiple modeling and analysis techniques, including Red Team analysis, game-theoretic modeling, attack tree and attack graph modeling, and analysis based on the structure of the cyber attack lifecycle (also known as cyber kill chain analysis or cyber campaign analysis).

The vocabulary enables hypotheses and claims about effects of decisions on cyber adversary behavior to be stated clearly. Each term suggests types of evidence that analysts could use to support or refute hypotheses or claims. As with any vocabulary intended for human (rather than machine) use, some overlap among terms exists; a rough taxonomy is illustrated in the figure below. The vocabulary is expected to evolve based on use, particularly by including examples of use and of evidence relevant to each term.

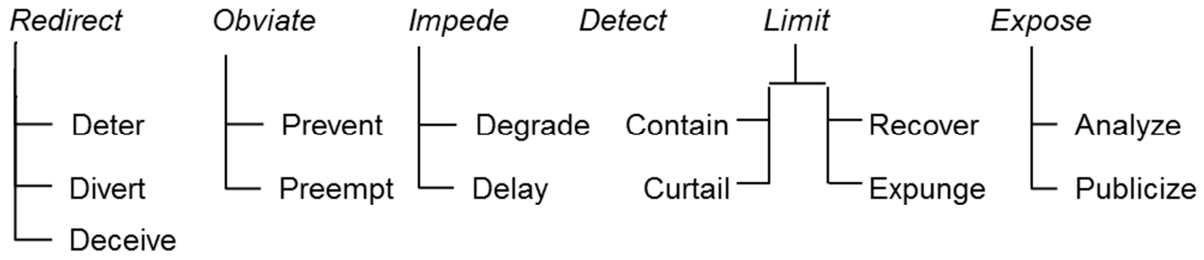

Figure ES-1. Proposed Vocabulary for Describing Effects of Defensive Actions / Decisions on Adversary Behavior

Table of Contents

List of Figures

List of Tables

1 Introduction

The increasing visibility of campaigns and activities by the advanced persistent threat (APT) has raised the importance of the question: How defensible are the cyber resources on which organizations, missions or business processes, and individuals depend? How secure are cyber systems? How resilient are missions, systems-of-systems, or individual systems? It is possible to measure or assess many security-, resiliency-, and defensibility-related properties of systems, systems-of-systems, or components. Similarly, the effects of different architectural approaches, technologies, or defensive actions on those measurements can also be evaluated.

However, the real challenge is knowing how our actions affect our adversaries. Have we made their job harder – do they need to spend more resources or take longer to achieve the same effects? Have we made their behavior riskier – do they reveal their intent, targeting, or tactics, techniques, and procedures (TTPs), or is attribution easier? Claims or hypotheses about how different cyber mission assurance decisions[1] affect adversary behavior are made by researchers, product or solution vendors, and cyber threat analysts. However, the lack of a common vocabulary makes claims or hypotheses difficult to compare.

This paper presents a vocabulary for stating claims or hypotheses about the effects of cyber mission assurance decisions on cyber adversary behavior. The vocabulary enables claims and hypotheses to be stated clearly, comparably across different assumed or real-world environments, and in a way that suggests evidence that might be sought but is independent of how the claims or hypotheses might be evaluated.

1.1 Background

Questions about effects on cyber adversaries arise in multiple contexts, including research, product evaluation, architectural or design decision-making, and defensive cyber operations (DCO) or Computer Network Defense (CND). As described in Section 2 below, a variety of metrics and analysis techniques have been explored and applied in experimental or operational environments. However, the absence of a consistent approach to describing effects on cyber adversaries impedes comparison or aggregation of the results of experiments and operational observations.

For ease of exposition, the phrase “the cyber adversary” is used in two ways: First, the phrase refers to the collection of advanced actors – whether state-sponsored, criminal, terrorist, or other – that persistently and covertly seek to exploit mission or organizational dependence on cyberspace to accomplish their goals. Those goals can include destroying resources, undermining current or future mission effectiveness, or obtaining an information advantage by exfiltrating large amounts of sensitive information. “Advanced” refers to the level of technical and operational sophistication. (The phrase “advanced persistent threat” is often used synonymously; however, some sources use “APT” to refer solely to advanced actors that seek to exfiltrate sensitive information.) Second, the phrase may refer to a specific threat actor, as determined by cyber threat intelligence. This narrow use of the phrase assumes a threat analysis capability.

[1] Cyber mission assurance decisions include choices of cyber defender actions, architectural decisions, and selections and uses of technologies to improve cyber security, resiliency, and defensibility (i.e., the ability to address ongoing adversary activities).

1.2 Overview of This Document

This white paper presents a vocabulary for characterizing the tactical effects of architectural approaches, technologies, and defender actions on the cyber adversary, whether broadly or narrowly construed. The decisions are assumed to be defensive in nature and to be focused on the design, acquisition, and use of information and communications technology (ICT). The vocabulary is intended to enable hypotheses or claims about effects on the adversary to be stated in a clear and consistent manner. Thus, it is intended to serve solution providers and researchers as well as cyber defenders. Once claims or hypotheses are clearly stated, evidence (whether anecdotal, analytic, or derived from measurements or sets of observations) can be sought and evaluated.

While statements of claims and hypotheses – and hence the vocabulary – are intended to drive identification of possible evidence, the evidence that can actually be developed depends on the environment in which the hypotheses are to be evaluated. A framework for characterizing evaluation environments is presented in a companion document [1].

Section 2 provides background on prior and related work. Section 3 presents the proposed vocabulary, relates it to that work, and illustrates how the proposed vocabulary can be used to describe how cyber resiliency techniques can affect adversary activities across the cyber attack lifecycle. Section 4 identifies future directions. An appendix presents the analysis of the potential effects of cyber resiliency techniques.

2 Prior and Related Work

This section describes prior work on approaches to considering effects on the adversary, adversary modeling, and vocabularies for talking about affecting the adversary.

2.1 Approaches to Considering Effects on the Cyber Adversary

Researchers and product vendors make hypotheses or claims about their technologies; those claims can be evaluated in experimental environments or via red teaming, subject to numerous caveats on the evaluation. Security architects and engineers make claims about how different architectural approaches make the adversary's job harder; those claims are typically evaluated via analysis.

2.1.1 Experimental Approaches

Laboratory and operational experimentation using Red Team evaluation of technologies and hypotheses produced a notional measurement: Red Team Work Factor (RTWF). RTWF, however, was too vague to provide good comparisons [2]. Sandia's Information Design Assurance Red Team (IDART) Methodology [3] identified several factors that could be measured or assessed, including attack mean time to recover (MTTR), cost to develop, time to develop and implement, skills to develop and implement, and resources to develop and implement. Sandia's experience [4] indicates that Red Teams are most effective when informed by adversary modeling, in terms of adversary characteristics and of behavior represented by attack graphs (see Section 2.2.2 below).

DARPA-sponsored research defined a composite measurement and used it in selected experiments: Adversary Work Factor (AWF) [5] [6]. While conceptually appealing, AWF has been used relatively little, even when coupled with attack potential (based on an adversary's initial access, initial knowledge, and capabilities) [7]. Recently, work factor ratio (WFR), i.e., the ratio of adversary to defender work factor, has been identified as an "overarching cyber metric" [8] and is being explored experimentally [9].

Experiments must be carefully formulated and executed, to address such issues as internal validity, external validity (or realism), repeatability, reproducibility, and the quality of analysis and reporting [10]. To facilitate reproducibility, the WOMBAT (Worldwide Observatory of Malicious Behaviors and Attack Threats) project has defined the goal of collecting and studying real-world, large-scale datasets [11]. The BADGERS (Building Analysis Datasets and Gathering Experience Returns for Security) workshop characterizes this goal as the experimental (as contrasted with the operational) use of Big Data for security [12].

The results of experiments are difficult to compare or aggregate, primarily due to different environmental assumptions. However, differences in how hypotheses or claims are stated also make comparison and aggregation challenging. This provides one motivation for a common vocabulary.

2.1.2 Architectural Analysis Approaches

Security architectures are based on assumptions about the threat, although those assumptions frequently are very high-level. Architectural analysis can specifically consider how architectural alternatives address threats, for example by using coverage analysis [13], attack graphs,

simulation, or survivability analysis [14]. Threat analysis, particularly using Microsoft's DREAD methodology [15], is recognized as an important component of architectural analysis [16]. However, most techniques for analyzing or comparing security architectures do not define terminology beyond such general terms as detect, prevent, and recover for comparing effects on the adversary. MITRE's Cyber Prep [17] and Threat Assessment and Remediation Analysis (TARA) methodologies [18] provide terminology for characterizing how countermeasures address adversary TTPs.

2.2 Adversary Modeling

Adversary modeling – abstract representations of adversary behavior and characteristics – is central to developing and analyzing hypotheses or claims about the effects of technologies, architectural decisions, and/or defender actions on the cyber adversary. Hypotheses or claims assume (with varying degrees of explicitness and specificity) some elements of an adversary model, so that the effects on other elements can be stated. Three broad classes of adversary models are discussed in more detail in Appendix B: game-theoretic modeling, attack graph (or attack tree) models, and cyber attack lifecycle models.

2.3 Existing Vocabularies

This section summarizes how different stakeholders talk about the cyber adversary, and in particular about effects on the adversary, changes in adversary behavior, and changes in adversary characteristics. Groups of stakeholders include those engaged in information operations, threat trend reporting, cyber security research, and cyber defense.

2.3.1 Information Operations Terminology

Information Operations (IO) is defined as "the integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own." [19] The 2006 version of Joint Publication (JP) 3-13, Information Operations [20], defined objectives for information operations as shown below.[2] A subset of these (i.e., "disrupt, deny, degrade, destroy, or deceive an adversary's ability to use the cyberspace domain to his advantage") have been identified as Cyberspace Warfare Attack capabilities [21]. An alternative set of IO objectives and effects (e.g., limit, mislead, confuse, disrupt, delay, divert, destroy, isolate; deny, preserve, exploit) have been identified to provide greater precision [22]. (Note that JP 3-13 defines the objectives of the defender in the face of an adversary that relies on information and cyberspace. However, adversaries can also adopt these as their own goals.)

[2] The 2012 version of JP 3-13 does not include this enumeration.

Table 1. Goals Defined in 2006 version of JP 3-13 (Desired Effects on the Adversary)

Objective	Definition in 2006 version of JP 3-13
Destroy	To damage a system or entity so badly that it cannot perform any function or be restored to a usable condition without being entirely rebuilt.[3]
Disrupt	To break or interrupt the flow of information.
Degrade	To reduce the effectiveness or efficiency of adversary C2 [command and control] or communications systems, and information collection efforts or means.
Deny	To prevent the adversary from accessing and using critical information, systems, and services.
Deceive	To cause a person to believe what is not true. MILDEC [military deception] seeks to mislead adversary decision makers by manipulating their perception of reality.
Exploit	To gain access to adversary C2 systems to collect information or to plant false or misleading information.
Influence	To cause others to behave in a manner favorable to US forces.
Protect	To take action to guard against espionage or capture of sensitive equipment and information.
Detect	To discover or discern the existence, presence, or fact of an intrusion into information systems.
Restore	To bring information and information systems back to their original state.
Respond	To react quickly to an adversary's or others' IO attack or intrusion.

2.3.2 Terminology in Threat Trend Reporting

A number of different organizations publish reports on trends in cyber threats [23] [24] [25] [26]. For the most part, the discussion of threat trends focuses on descriptions of adversary behavior and characteristics, as well as on trends in organizational uses of technology and security improvements. However, some terminology does describe possible or intended effects on the adversary. For example, Sophos [23] mentions "deter" and "prevent." Threat trend reporting discusses classes of adversaries, e.g., cyber criminals and nation states, with limited analysis of specific campaigns.

2.3.3 Terminology in Research Agenda and Technology Claims

Some cyber security research roadmaps and agendas tend to focus on security technology improvements and new technologies, rather than on the adversary [27] [28] [29]. Others include some discussion of intended effects on adversaries, for example, increasing cost and complexity [30] or increasing the work factor ratio [8]. However, research roadmaps typically address a range of adversaries, and do not explicitly define an adversary model.

Claims about the effectiveness and usefulness of technologies can be stated in terms of an adversary model. Such is the case in several IETF drafts[4]. However, the main effect on the adversary is "prevent." In the cyber security research literature, adversary models (and hence claims about the effects of the technology or approach that is the subject of the research) are described most often for analysis of cryptographic protocols, using variants of the Dolev-Yao model.

[3] For further discussion of Destroy and Exploit, see [94]. Note that these effects are related to OCO/CNA, and thus are outside the scope of this paper.

[4] See, for example, http://tools.ietf.org/html/draft-kent-bgpsec-threats-01, http://www.ietf.org/id/draft-pouwelse-censorfree-scenarios-02.txt, and http://tools.ietf.org/html/draft-ietf-ecrit-trustworthy-location-04.

2.3.4 Cyber Threat Analyst Terminology

Any vocabulary for effects on cyber adversaries must be meaningful for defensive cyber operations (DCO). Since DCO needs to be informed by cyber threat analysis/intelligence, the vocabulary must also be meaningful to cyber threat analysts. Therefore, it is important to have a vocabulary that works with cyber attack lifecycle models.

However, the value of a vocabulary is to point to possible evidence. Hence, it is also important to look at how analysts do their jobs and what they look at. The STIX™ (Structured Threat Information eXpression) schema is intended to enable cyber threat analysts to exchange threat information [31]. Key elements in the STIX schema include observables, indicators, TTPs, threat actors, and campaigns. These elements are defined, but the definitions are deliberately broad enough to support a range of use cases, depending on the capabilities and goals of stakeholders in cyber threat information sharing.

Table 2. Key Elements of Cyber Threat Information

Term	Definition/Discussion
Observable	"Observables are stateful properties or measurable events pertinent to the operation of computers and networks. Information about a file (name, hash, size, etc.), a registry key value, a service being started, or an HTTP request being sent are all simple examples of observables." [31] See [32] for taxonomy of cyber observables, mapped to a version of the cyber attack lifecycle.
Indicator	"A set of cyber observables combined with contextual information intended to represent artifacts and/or behaviors of interest within a cyber security context." [31] "An indicator can be defined as human-readable cyber data used to identify some form of malicious cyber activity and are data related to IP addresses, domains, email headers, files, and strings." [33]
TTP	"TTPs are representations of the behavior or *modus operandi* of cyber adversaries. It is a term taken from the traditional military sphere and is used to characterize what an adversary does and how they do it in increasing levels of detail." [31] "TTPs consist of the targeting, tools, techniques, infrastructure, and kill-chain activities that the adversary uses to conduct a series of related intrusion attempts." [34] Examples of high-level TTPs are given in Appendix E of NIST SP 800-30 Rev. 1. [35]
Threat Actor	"Threat Actors are characterizations of malicious actors (or adversaries) representing a cyber attack threat including presumed intent and historically observed behavior." [31] Note that such characterizations need not include attribution. As discussed in [36], attribution is problematic, although increasingly feasible [37] [38]. However, for purposes of cyber threat analysis and cyber defense, differentiating between threat actors based on historically observed behavior generally suffices.
Incident	"Incidents are discrete instances of Indicators affecting an organization along with information discovered or decided during an incident response investigation. They [are described using] data such as time-related information, location of effect, related Indicators, leveraged TTP, suspected intent, impact assessment, response Course of Action requested, response Course of Action taken, source of the Incident information, log of actions taken, etc." [31]
Attack Lifecycle	The stages that an adversary goes through to achieve the objectives of establishing, using, and maintaining (or removing) a presence in an enterprise's information infrastructure (derived from [39] [40] [41] [42] [23] [38])
Campaign	"Campaigns are instances of Threat Actors pursuing an intent, as observed through sets of Incidents and/or TTP, potentially across organizations." [31] "At the highest level, a campaign represents an unclassified construct that packages together all of the intelligence-based information about a particular kill-chain-based intrusion in a related set of activities. Campaigns consist of Intrusion attempts combined with Tactics, Techniques and Procedures (TTPs)." [34]

3 Proposed Vocabulary

The proposed vocabulary presented in this section is intended to describe effects that defender actions or decisions could have on the cyber adversary, whether narrowly or broadly construed. The focus is on tactical effects, i.e., effects on current adversary activities and on activities that could reasonably be expected to follow in the near term from current activities.

3.1 Assumptions

The proposed vocabulary of possible effects on adversary activities is meaningful when cyber defenders 1) have a threat intelligence analysis capability that can associate activities with a given campaign, and thus attribute activities to a distinct[5] adversary or set of actors; and 2) apply mitigations or execute cyber courses of action (CCoAs) in response to anticipated, suspected, or observed adversary activities. Without those cyber defender capabilities, the extent to which any assertion about effects on the adversary holds cannot be determined.

The proposed vocabulary describes effects on a distinct adversary or set of actors, with the following general characteristics:

- The adversary's efforts consist of a coordinated set of activities, in which each activity has intended effects on the resources cyber defenders seek to protect. Adversary activities can be characterized broadly as stages in the cyber attack lifecycle or more specifically as tactics, techniques, and procedures (TTPs).
- The adversary's efforts are intended to achieve one or more overall objectives, e.g., interfering with a mission that relies on the defended cyber resources, obtaining sensitive information, or using the defended cyber resources as a launch point for attacks on cyber resources beyond the purview of cyber defenders.
- The adversary has a strategy or decision criteria for performing specific activities, selecting TTPs, and selecting targets. Decision criteria include perceived risks or anticipated costs as well as success criteria.
- The adversary has defined success criteria (intended effects, which in some cases could be expressed as measures of performance) for their activities. Some success criteria are related to the adversary's overall objectives; others may be more specific to an activity or phase in the campaign.

3.2 Definitions

The terminology proposed to describe effects on the cyber adversary is represented in Figure 1. Terms for six high-level effects are defined: Redirect, Obviate, Impede, Detect, Limit, and Expose. These terms could suffice for a general description, but (except for Detect) are too general to suggest measures of effectiveness for cyber defenders. Thus, more specific terms are also provided (e.g., Prevent and Pre-empt for Obviate; Constrain, Curtail, Recover, and Expunge for Limit). In Table 3, terms are defined and described in terms of their expected effects on the

[5] Attack attribution ranges from characterization (attributing an attack or incident to classes of adversaries) to differentiation (attributing an attack, incident, or campaign to a distinct threat actor or set of actors) to identification (attributing an attack, incident, or campaign to an identified individual, group, or location).

adversary. Examples of evidence that could be found on or derived from defender systems are also provided. If an example of evidence would be related to a specific actor, the example is italicized.

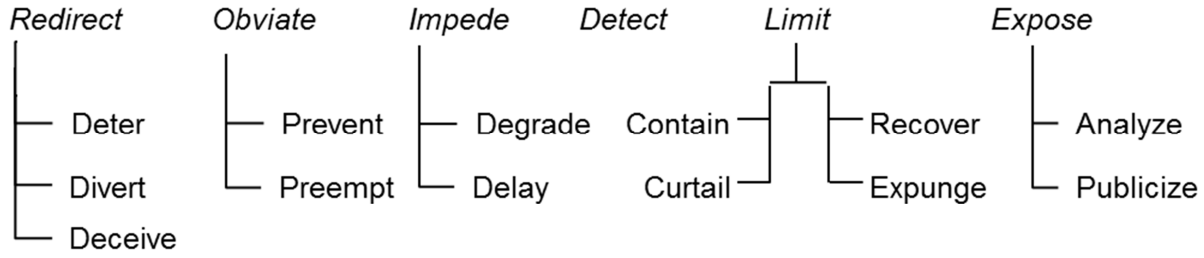

Figure 1. Proposed Vocabulary for Characterizing Effects on a Cyber Adversary

Figure 1 and the vocabulary in Table 3 describe tactical effects, i.e., those that an adversary could experience in the course of conducting a set of activities across the cyber attack lifecycle or a cyber campaign: the expected value of that set of activities (or of a specific activity or TTP) to the adversary would be decreased. It must be noted that the experience of tactical effects, particularly on a repeated basis, could also result in strategic effects.[6]

One further tactical effect could be identified: inflame. That is, cyber defender actions could anger the adversary, inciting harmful action. However, this effect is unpredictable, as it depends on the character or group culture of the adversary, as well as the adversary's strategy. In addition, it is not an intended effect as claimed by a solution provider or hypothesized by a researcher; evidence can be found only in operational environments. Thus, inflammatory effects are outside the scope of this document.

[6] It should also be noted that, while the vocabulary is designed for use by defenders, it could also be applied (with refinement, particularly with respect to the "Exploit" IO objective identified in Table 1) to Offensive Cyber Operations (OCO).

Table 3. Possible Effects of Cyber Defender Activities and/or Investments on Adversary Activities

Defender Goal	Definition	Effect	Evidence
Redirect (includes Deter, Divert, and Deceive)	*Direct adversary activities away from defender-chosen targets.*	*The adversary's efforts cease, or become mistargeted or misinformed.*	*See evidence for Deter, Divert, and Deceive.*
Deter	Discourage the adversary from undertaking further activities, by instilling fear (e.g., of attribution or retribution) or doubt that those activities would achieve intended effects (e.g., that targets exist).[7]	The adversary ceases or suspends activities.	Activities attributable to the adversary are no longer observed by the organization. Activities attributable to the adversary are no longer observed by other organizations and this fact is made known via threat intelligence information sharing.
Divert	Lead the adversary to direct activities away from defender-chosen targets.	The adversary refocuses activities on different targets (e.g., other organizations, defender-chosen alternate targets). The adversary's efforts are wasted.	Adversary activities are directed towards defender-chosen alternate targets (e.g., to a special enclave). Activities attributable to the adversary are observed by other organizations and made known via threat intelligence information sharing.
Deceive	Lead the adversary to believe false information about defended systems, missions, or organizations, or about defender capabilities or TTPs.	The adversary's perception of defenders or defended systems is false. The adversary's efforts are wasted.	Adversary activities reveal that the adversary is relying on false information (e.g., a dummy account is spearphished, delivered malware is tailored to a simulated environment).
Obviate (includes Prevent and Preempt)	*Render the adversary's efforts or intentions ineffective by ensuring that adversary efforts or resources cannot be used or will have no effects.*	*The adversary's efforts or resources cannot be applied or are wasted.*	*See evidence for Prevent and Preempt.*
Prevent	Make the adversary's activity ineffective.	The adversary's efforts are wasted, as no intended effects can be achieved.	Logs or other captured data provide evidence that the activity occurred but had no effects.
Preempt[8]	Ensure that the adversary cannot apply resources or perform activities.	The adversary's resources cannot be applied and/or the adversary cannot perform activities (e.g., because resources are destroyed or made inaccessible).	The adversary's resources are observed to be denied (e.g., destroyed, made inaccessible or unusable).

[7] Instilling fear can also be characterized as "deterrence-by-punishment," while instilling doubt can be characterized as "deterrence-by-denial" [92]. Deterrence-by-punishment raises a number of policy issues, as well as practical issues of acquiring adequate evidence for attribution [95].

[8] A preemptive action forestalls or prevents something from happening; that is, it is taken in anticipation of the undesired event or action. Here, preemption is aimed at the effects of potential adversary activities, and is used in the sense of a preemptive strike against the cyber adversary. (Others use "preemption" more broadly, in the sense of proactive rather

Defender Goal	Definition	Effect	Evidence
Impede (includes Degrade and Delay)	*Make the adversary work harder or longer to achieve intended effects.*	*The adversary achieves the intended effects, but only by investing more resources or undertaking additional activities.*	*See evidence for Degrade and Delay.*
Degrade	Decrease the effectiveness of an adversary activity, i.e., the level of impact achieved.	The adversary achieves some but not all of the intended effects, or achieves all intended effects but only after taking additional actions.	The number of resources affected by the adversary is lower than for prior instances of the activity. The severity of the impacts caused by the adversary activity is less than for prior instances of the activity. Malware or other attack vectors attributable to the adversary are crafted or tailored, based on failures of prior activities attributable to the same adversary to achieve effects. Repeated activities (e.g., to establish information channels, to start processes) are attributable to the same adversary.
Delay	Increase the amount of time needed for an adversary activity to achieve its intended effects.	The adversary achieves the intended effects, but may not achieve them within the intended time period. (The adversary's activities may therefore be exposed to greater risk of detection and analysis.)	The length of time between an initial event and its effects, as determined by forensic or other analysis, is increased.

than reactive behavior [43].) In cyberspace, some forms of preemptive actions are referred to as active cyber defense. Preemption may not be a valid intended effect, depending on policy, legal, regulatory, or other organizational considerations related to active cyber defense [91]. Therefore, while preemption in the sense of active cyber defense is included for completeness, it will not be discussed in detail in this paper.

Defender Goal	Definition	Effect	Evidence
Detect	*Identify adversary activities or their effects by discovering or discerning the fact that an adversary activity is occurring, has occurred, or (based on indicators, warnings, and precursor activities) is about to occur.*	*The adversary's activities become susceptible to defensive responses.*	*Adversary activities are detected, or indicators, warnings, and/or precursor activities are observed.*
Limit (includes Contain, Curtail, Recover, & Expunge)	*Restrict the consequences of adversary efforts by limiting the damage or effects of adversary activities in terms of time, cyber resources, and/or mission impacts.*	*The adversary's effectiveness is limited.*	*See evidence for Contain, Curtail, Recover, & Expunge.*
Contain	Restrict the effects of the adversary activity to a limited set of resources.	The value of the activity to the adversary, in terms of achieving the adversary's goals, is reduced.	Damage assessment, in terms of • (Scope) The number of affected resources • (Impact) A function of o The number of affected resources and their value (e.g., criticality) Duration and the mission or operational cost per unit time
Curtail	Limit the duration of an adversary activity.	The time period during which the adversary's activities have their intended effects is limited.	Damage assessment, in terms of (Time) The duration of an outage or of degraded functionality
Recover	Roll back adversary gains, particularly with respect to mission impairment.	The adversary fails to retain mission impairment due to recovery of the capability to perform key mission operations.	Recovery metrics, including • (Functionality) Level of performance (typically expressed in terms of Measures of Effectiveness (MOEs), Measures of Performance (MOPs), or Key Performance Parameters (KPPs)). (Assurance) Degree of trustworthiness or confidence in restored resources.
Expunge	Remove adversary-directed malware, repair corrupted data, or damage an adversary-controlled resource so badly that it cannot perform any function or be restored to a usable condition without being entirely rebuilt.	The adversary loses a capability for some period of time.	Removal of malware or of privileges from adversary-controlled resources.

Defender Goal	Definition	Effect	Evidence
Expose (includes Analyze and Publicize)	*Remove the advantages of stealth from the adversary by developing and sharing threat intelligence.*	*The adversary loses advantages, as defenders are better prepared.*	*Size and quality of a growing body of threat intelligence information.*
Analyze	Understand the adversary better, based on analysis of adversary activities, including the artifacts (e.g., malware) and effects associated with those activities and correlation of activity-specific observations with observations from other activities (as feasible).	The adversary loses the advantages of uncertainty, confusion, and doubt; the defender can recognize adversary TTPs.	Number and quality (e.g., correctness, usefulness) of malware signatures and characteristics. Number and quality (e.g., degree of confirmation) of observables and indicators. Distinct threat actors and/or campaigns being observed.
Publicize	Increase awareness of adversary characteristics and behavior across the stakeholder community (e.g., across all CSIRTs that support a given sector, which might be expected to be attacked by the same actor(s)).	The adversary loses the advantage of surprise and possible deniability; the adversary's ability to compromise one organization's systems to attack another organization is impeded.	Distinct threat actors, campaigns, and/or TTPs observed by multiple organizations. Degree of confidence in attribution of events to threat actors or campaigns.

3.3 Mapping the Proposed Vocabulary to Other Terminologies

As discussed in Section 2, other ways of describing effects on the adversary have been identified, particularly in the context of red team and experimental evaluations. In Table 4, these are mapped to the set of goals defined in Table 3.

Table 4. Mapping Other Terminology to Proposed Vocabulary

Described Effect	Where Described	Defender Goal(s)
Hinder adversary intelligence gathering	AWF [5]	Impede
Shorten time for adversary reconnaissance Limit time window for exploitation	WFR [8]	Impede, Curtail
Limit the time-value (life span) of adversary knowledge	AWF [5]	Impede, Curtail
Increase adversary resource expenditures • Time • Effort	 AWF [5], Raytheon [43] AWF [6], Raytheon [43]	 Degrade Impede, Disrupt
Limit effectiveness of malware	WFR [8]	Impede
Limit propagation of malware	WFR [8]	Contain
Increase adversary's perceived risk	AWF [5]	Deter, Alter strategy
Force adversary to move larger files through the network	AWF [5]	Degrade
Prevent unauthorized access	AWF [6]	Prevent
Deter unauthorized access	AWF [6]	Deter
Change the relative amount of time the adversary spends on different phases of an attack	Red Team Lessons-Learned [2], Raytheon [43]	Alter strategy
Prevent	Microsoft [44], Cyber Prep [17]	Prevent
Detect	Microsoft [44], TARA [18] [45], Raytheon [43]	Detect
Contain	Microsoft [44]	Contain
Recover (reconstitute, restore to a "known good state")	Microsoft [44], TARA [18] [45], Raytheon [43]	Recover
Neutralize	TARA [18] [45]	Prevent, Impede, Degrade, Delay, Divert
Limit	TARA [18] [45]	Contain, Curtail
Detect the actions or presence of a TTP	Cyber Prep [17]	Detect
Disrupt ("Disruptions are any effect a cyber defense produces that impedes the progress of an attack through its process.")	Raytheon [43]	Divert, Prevent, Impede, Degrade, Delay, Contain, Curtail
Reduce dwell time	Raytheon [43]	Curtail, Expunge
Identify conditions that a TTP might exploit	Cyber Prep [17]	-[9]
Deter or prevent the execution of a TTP	Cyber Prep [17]	Deter, Prevent
Materially reduce the effectiveness of a TTP	Cyber Prep [17]	Degrade
Contain the effectiveness of a TTP to a specific physical or logical (e.g., platform, sub-network) location	Cyber Prep [17]	Contain
Facilitate recovery from the successful execution of a TTP	Cyber Prep [17]	Recover

[9] This does not affect the adversary; it improves the defender's knowledge of resources to be defended.

Described Effect	Where Described	Defender Goal(s)
Validate security relevant conditions (e.g., identity claims, configurations) that are intended to counter TTPs	Cyber Prep [17]	- (See note on "Identify conditions that a TTP might exploit)
Characterize the TTP(s) in use during an attack	Cyber Prep [17]	Analyze
Train users, administrators, and developers to raise awareness of one or more TTPs	Cyber Prep [17]	Publicize
Reduce the likelihood of successfully completing an attack	MORDA [46]	Prevent, Impede, Degrade, Delay, Contain, Curtail, Expunge
Increase the likelihood of detection	MORDA [46], Raytheon [43]	Divert, Deceive, Detect
Increase the resources required to execute the attack	MORDA [46]	Divert, Deceive, Prevent, Impede, Degrade, Delay, Detect
Reduce the impact of the attack	MORDA [46]	Contain, Recover, Expunge
Change the set of possible adversary actions	Game-theoretic and attack graph models [47]	Preempt, Alter strategy
Place constraints on possible adversary actions	Game-theoretic and attack graph models [47]	Prevent, Impede, Degrade, Delay
Change the costs of possible adversary actions	Game-theoretic and attack graph models [47], Raytheon [43]	Divert, Deceive, Prevent, Impede, Degrade, Delay, Detect
Change the adversary's payoff or utility function	Game-theoretic and attack graph models [47]	Detect, Expose, Contain, Recover, Expunge
Change the adversary's beliefs Increase the adversary's uncertainty about success	Bayesian attack graph models, Raytheon [43]	Deter, Deceive
Destroy	2006 JP3-13 [20]	Preempt[10]
Disrupt	2006 JP 3-13 [20]	Impede[11]
Degrade	2006 JP 3-13 [20]	Impede (efficiency), Degrade (effectiveness)
Deny	2006 JP 3-13 [20]	Prevent
Deceive	2006 JP 3-13 [20]	Deceive, Divert
Exploit	2006 JP 3-13 [20]	Pre-empt, Deceive (insofar as the exploitation of adversary malware or C2 channels within the defended environment misleads the adversary)
Influence	2006 JP 3-13 [20]	Deter, Alter strategy
Protect	2006 JP 3-13 [20]	Prevent
Detect	2006 JP 3-13 [20]	Detect
Restore	2006 JP 3-13 [20]	Recover
Respond	2006 JP 3-13 [20]	Impede, Degrade, Delay, Contain, Curtail
Prevent	CNSS 048-07 [48]	Prevent
Prepare	CNSS 048-07 [48]	Expose
Detect	CNSS 048-07 [48]	Detect

[10] For further discussion of Destroy and Exploit, see [94].

[11] "Disrupt" in the 2006 JP 3-13 involves impeding the adversary by disrupting communications. "Impede" as defined in Table 4 can involve a variety of methods, including some that would fall under the definition of "Disrupt." For example, cyber defenders could break or interrupt adversary-initiated information flows, or could terminate adversary-initiated processes.

Described Effect	Where Described	Defender Goal(s)
Contain	CNSS 048-07 [48]	Contain
Eradicate	CNSS 048-07 [48]	Expunge
Recover	CNSS 048-07 [48]	Recover
Degrade	CIE [49] [50]	Degrade
Interrupt	CIE [49] [50]	Impede (see footnote 11)
Modify	CIE [49] [50]	Preempt, Deceive
Fabricate	CIE [49] [50]	Deceive, Divert
Unauthorized use	CIE [49] [50]	Deceive (insofar as defender use of adversary malware or C2 channels within the defended environment misleads the adversary)
Intercept	CIE [49] [50]	Detect

3.4 Mapping to the Cyber Attack Lifecycle

The terms in the proposed vocabulary are not equally relevant to all phases of the cyber attack lifecycle. Table 5 indicates how the different effects might apply, using a few representative examples of cyber defender actions or countermeasures, drawn from cyber security as well as resiliency.

Table 5. Relevance of Effects to Phases of the Cyber Attack Lifecycle

Intended Effect	Relevance: Intended Effect Applies to …
Redirect	*See Deter, Divert, and Deceive*
Deter	• A cyber campaign as a whole (e.g., adversary intelligence about a potentially targeted organization's policies and capabilities indicates that attribution and response are likely) • The set of phases of the cyber attack lifecycle after Recon (e.g., adversary reconnaissance indicates that the expected value of carrying out a cyber attack does not justify the expected costs or risks)
Divert	• Recon (e.g., redirection into a honeynet lead the adversary to expend resources with no benefits) • Deliver (e.g., suspicious emails are diverted to a detonation chamber) • Exploit (e.g., the adversary's malware installs itself in a defender-chosen enclave) • Control (e.g., the defender directs adversary C2 traffic to a black hole) • Execute (e.g., a DoS attack is focused on a defender-chosen target)
Deceive	• Recon (e.g., recon within a honeynet deceive the adversary about the topology and contents of the organization's network) • Weaponize (e.g., the components or configuration of a honeynet lead the adversary to develop attack tools that will not work on the organization's network) • Deliver (e.g., the adversary sends phishing emails to bogus email addresses) • Exploit (e.g., the adversary's malware installs itself in a honeynet) • Control (e.g., honeypots on the organization's internal network provide the adversary with false information about the organization and its missions, or about the internal network configuration) • Execute (e.g., the adversary exfiltrates bogus data) • Maintain (e.g., honeypots on the organization's internal network provide the adversary with false information about the status of resources the adversary believes compromised or owned)

Intended Effect	Relevance: Intended Effect Applies to …
Obviate	*See Prevent and Preempt*
Prevent	• Recon (e.g., OPSEC prevents an adversary from learning critical information) • Weaponize (e.g., the adversary cannot develop exploits against critical customized components) • Deliver (e.g., email filtering can prevent delivery of malware-loaded attachments) • Exploit (e.g., vulnerabilities can be removed, or configurations changed so that vulnerabilities are not exposed) • Control (e.g., honeypots on the organization's internal network can provide the adversary with false information about the organization and its missions) • Execute (e.g., Data Loss Prevention technologies can prevent certain forms of exfiltration) • Maintain (e.g., honeypots on the organization's internal network can provide the adversary with false information about the status of resources the adversary believes compromised or owned)
Preempt	All phases
Impede	*See Degrade and Delay. In some cases, a cyber defender action or countermeasure simultaneously degrades and delays:* • Weaponize (e.g., use of randomizing compilers impedes development of tailored malware)
Degrade	• Recon (e.g., cryptographic protections against adversary sniffing a common carrier network to gain insight into defender patterns of usage can make the adversary need to acquire decryption resources) • Deliver (e.g., use of URL whitelisting means adversary must compromise a strongly protected Web site in order to place malware where it will be downloaded by target) • Exploit (e.g., patching and configuration controls can reduce the number of vulnerable devices) • Control (e.g., controlled information flows between enclaves can make lateral movement across a network more difficult) • Execute (e.g., data rights management mechanisms can make exfiltration harder; however, steganography and covert channels can still be used) • Maintain (e.g., periodic refreshing of virtual machines from a gold copy can make it harder to keep copies of malware on the target network)
Delay	• Recon (e.g., cryptographic protections against adversary sniffing a common carrier network to gain insight into defender patterns of usage can make the adversary's analysis take longer) • Exploit (e.g., unpredictable responses can force the adversary to make repeated attempts before one succeeds) • Control (e.g., non-persistent communications channels can make lateral movement take longer) • Execute (e.g., data rights management mechanisms can make exfiltration require slower mechanisms such as steganography and covert channels)
Detect	*All phases*[12]

[12] Note that detection of Weaponization activities involves gathering and analyzing intelligence from systems other than those being defended.

Intended Effect	Relevance: Intended Effect Applies to …
Limit	*See Contain, Curtail, Recover, & Expunge*
Contain	• Recon (e.g., adversary network mapping can be restricted to an Extranet) • Deliver (e.g., automated quarantine of incoming messages can restrict delivery to a detonation chamber) • Exploit (e.g., automated quarantine and remediation can sever the connection between an exploited resource and other resources) • Control (e.g., a set of suspected internal network addresses can be quarantined; a sub-network can be isolated) • Maintain (e.g., a sub-network can be isolated; network connections can be restricted based on mission criticality)
Curtail	• Recon (e.g., traffic from a suspected prober can be cut off) • Deliver (e.g., Web traffic from a suspected watering hole can be automatically blocked) • Exploit (e.g., the adversary's attempt to exploit a vulnerability is curtailed when the attacked service is terminated) • Control (e.g., adversary-acquired privileges can be revoked) • Execute (e.g., detected exfiltration can be blocked) • Maintain (e.g., compromised resources can be removed from enterprise systems / networks)
Recover	• Exploit (e.g., automated quarantine and remediation can return the exploited resource to a known good state) • Control (e.g., re-instantiation of a compromised service that the adversary is using from a known good version restores that service) • Execute (e.g., failover to a backup system can return service to its required level, in spite of adversary denial-of-service activities) • Maintain (e.g., re-instantiation of a compromised component from a known good version restores that service to a trustworthy state)
Expunge	• Deliver (e.g., email from a blacklisted source is deleted rather than delivered) • Exploit (e.g., automated quarantine and remediation can remove malware before it can take any further action) • Control (e.g., deletion of dropped files can remove the malware they contain before it is installed) • Maintain (e.g., removal of a compromised component – whether or not it is subsequently re-instantiated or replaced – can remove the adversary's point of presence)

Intended Effect	Relevance: Intended Effect Applies to …
Expose	*See Analyze and Publicize*
Analyze	• Recon (e.g., analysis of usage patterns can provide indications and warning (I&W) of adversary recon) • Weaponize (e.g., analysis of the speed with which the adversary acquires or develops 0-day exploits can reveal adversary resources and strategy) • Deliver (e.g., analysis of previous attacks can reveal delivery of malicious payloads) • Exploit (e.g., analysis of anomalous behavior can reveal an exploit) • Control (e.g., malware analysis can help identify compromised components) • Execute (e.g., analysis of which documents the adversary exfiltrated can reveal adversary intent) • Maintain (e.g., malware analysis that indicates how to locate dormant / hidden malware)
Publicize[13]	• Recon (e.g., sharing of information about indicators can enable I&W of adversary recon) • Deliver (e.g., sharing of observables, indicators, or signatures can reveal delivery of malicious payloads) • Exploit (e.g., sharing of observables, indicators, or signatures can reveal exploits) • Control (e.g., sharing of observables or indicators can reveal lateral movement) • Maintain (e.g., sharing of observables, indicators, or signatures can reveal compromised components)

Table 6 describes the intended or potential effects on adversary activities of different instances or applications of cyber resiliency techniques. The overarching claim is that each resiliency technique interrupts the lifecycle of a cyber attack ("breaks" the cyber kill chain) in one or more phases, either by preventing an activity in that phase, or by increasing the cost, decreasing the benefit, or increasing the risk of one or more activities in that phase. Therefore, each instance of a resiliency technique is mapped to one or more phases of the cyber attack lifecycle. Amplification (including definitions of the techniques as well as explanations of the effects) is provided in Appendix C. Because Table 5 considers a wider range of countermeasures than resilience techniques (e.g., conventional cyber security measures), some entries in Table 5 are not reflected in Table 6.

[13] Note that Publicize affects adversary activities on systems and networks belonging to partner organizations, or other recipients of information sharing and publication, while Analyze affects adversary activities on systems and networks belonging to the organization that performs the analysis.

Table 6. Use of Proposed Vocabulary to Describe Effects of Cyber Resiliency Techniques at Different Attack Phases

Cyber Resiliency Technique	Recon	Weaponize	Deliver	Exploit	Control	Execute	Maintain
Adaptive Response	Contain Curtail	Impede	Curtail	Prevent Recover	Contain Curtail	Curtail Degrade Recover	Contain Curtail
Analytic Monitoring	Detect Analyze		Prevent	Detect Analyze	Detect Analyze	Detect	Detect Analyze
Coordinated Defense		Impede		Impede	Detect Impede		Detect Impede
Deception	Prevent Impede Divert Deceive Detect Analyze	Deter Deceive Analyze	Deter Divert Deceive Analyze	Deter Divert Deceive Analyze	Deter Divert Deceive Detect Analyze	Deter Divert Deceive Degrade Detect Analyze	Deter Deceive Detect Analyze
Diversity		Impede			Degrade Contain Recover	Recover	Degrade Contain Recover
Dynamic Positioning	Divert Detect Curtail				Divert Detect Impede Curtail Expunge	Divert Detect Impede Curtail Expunge	Divert Detect Impede Curtail Expunge
Dynamic Representation	Obviate				Obviate Expunge	Recover	Obviate Expunge
Non-Persistence				Curtail Expunge	Curtail Expunge	Curtail	Curtail Expunge
Privilege Restriction				Prevent Degrade Delay Contain	Prevent Degrade Delay Contain	Prevent Degrade Delay Contain	Prevent Degrade Delay Contain
Realignment	Impede	Prevent Impede	Impede	Prevent Impede	Prevent Impede	Prevent Impede	Prevent Impede
Redundancy						Degrade Curtail Recover	
Segmentation	Contain		Degrade	Impede Contain	Impede Delay Contain Detect	Impede Delay Contain Detect	Impede Delay Contain
Substantiated Integrity			Prevent Detect		Detect Curtail Expunge	Curtail Recover Expunge	Detect Curtail Expunge
Unpredictability	Deter Delay	Impede		Delay	Deter Delay		

4 Future Directions

This paper presents an initial vocabulary for stating claims or hypotheses about the effects of cyber mission assurance decisions on cyber adversary behavior. That is, it provides a way to describe the tactical effects of architectural decisions, technologies and approaches being researched, and cyber defender actions on the adversary. The vocabulary is intended to enable claims and hypotheses to be stated clearly and consistently, so that evidence can be identified and metrics can be defined to evaluate their validity. This paper illustrates how the vocabulary is consistent with existing terminology and can be used with multiple modeling and analysis techniques, including Red Team analysis, game-theoretic modeling, attack tree and attack graph modeling, and analysis based on the cyber attack lifecycle.

Claims and hypotheses must be grounded in assumptions about or observations of the threat, technical and operational aspects of the environments in which they are expected to hold. A companion document [1] provides an approach to identifying those assumptions. Future work will apply the vocabulary in the identification and analysis of evidence to confirm or disconfirm claims or hypotheses in multiple environments.

The vocabulary presented in this paper focuses on tactical effects. Future work will also include defining a framework for discussing strategic effects on cyber adversaries.

5 References/Bibliography

[1] D. Bodeau, R. Graubart and W. Heinbockel, "Mapping the Cyber Terrain: Enabling Cyber Defensibility Claims and Hypotheses to Be Stated and Evaluated with Greater Rigor and Utility (MTR130433)," The MITRE Corporation, Bedford, MA, 2013.

[2] 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.

[3] 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.

[4] B. Hutchinson and M. Skroch, "Lessons Learned Through Sandia's Cyber Assessment Program," 12 December 2001. [Online]. Available: http://www.naseo.org/committees/energysecurity/archive/meetings/2001-12-12/hutchinson.pdf.

[5] G. Schudel and B. Wood, "Adversary Work Factor as a Metric for Information Assurance," New Security Paradims Workshop, 2000. [Online]. Available: http://www.nspw.org/papers/2000/nspw2000-schudel.pdf.

[6] D. L. Kewley and J. Lowry, "Observations on the effects of defense in depth on adversary behavior in cyber warfare," Proceedings of the IEEE SMC Information, June 2001. [Online]. Available: http://www.bbn.com/resources/pdf/USMA_IEEE02.pdf.

[7] J. McDermott, "Attack-Potential-Based Survivability Modeling for High-Consequence Systems, NRL 04-1226-3437," 24 March 2004. [Online]. Available: http://www.nrl.navy.mil/chacs/pubs/04-1226-3437.pdf.

[8] 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.

[9] C. Wright and L. Rossey, "Cyber Measurement Campaign," 25-27 July 2012. [Online]. Available: http://www.itea.org/~iteaorg/images/pdf/Events/2012_Proceedings/2012_Technology_Review/track1_2_cybermeasurementcampaign_wright.pdf.

[10] T. Frazier, "Lessons from 8 Years of Government Experiments in Cyber Warfare Research and Development," 2-5 July 2009. [Online]. Available: http://webhost.laas.fr/TSF/IFIPWG/Workshops&Meetings/56/workshop/04.frazier.pdf.

[11] BADGERS, "Proceedings of the First Workshop on Building Analysis Datasets and Gathering Experience Returns for Security (BADGERS 2011)," 10 July 2011. [Online]. Available: http://iseclab.org/badgers2011/badgers2011-proceedings.pdf.

[12] BADGERS, "2012 Workshop on Building Analysis Datasets and Gathering Experience Returns for Security (BADGERS'12)," 15 October 2012. [Online]. Available: http://www.badgersconf.com/.

[13] S. A. Butler, "Security Attribute Evaluation Method, CMU-CS-03-132," May 2003.

[Online]. Available: http://reports-archive.adm.cs.cmu.edu/anon/anon/home/ftp/usr/ftp/2003/CMU-CS-03-132.pdf.

[14] B. Lawlor and L. Vu, "A Survey of Techniques for Security Architecture Analysis, DSTO-TR-1438," May 2003. [Online]. Available: http://www.dsto.defence.gov.au/publications/2547/DSTO-TR-1438.pdf.

[15] Microsoft, "Threat Modeling," June 2003. [Online]. Available: http://msdn.microsoft.com/en-us/library/ff648644.aspx.

[16] OWASP, "Application Threat Modeling," 6 March 2013. [Online]. Available: https://www.owasp.org/index.php/Application_Threat_Modeling.

[17] D. Bodeau, S. Boyle, J. Fabius and R. Graubart, "Using Cyber Prep: The Concept of Operations for MITRE's Cyber Prep Methodology, MTR 100313, PR 10-3915," The MITRE Corporation, Bedford, MA, 2010.

[18] 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/sites/default/files/pdf/11_4982.pdf.

[19] Joint Chiefs of Staff, "Joint Publication (JP) 3-13, Information Operations," 27 November 2012. [Online]. Available: http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf.

[20] 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.

[21] AFLCMC/HNJG, "Broad Agency Announcement (BAA ESC 12-0011): Cyberspace Warfare Operations Capabilities (CWOC) Technology Concept Demonstrations," 22 August 2012. [Online]. Available: https://www.fbo.gov/utils/view?id=48a4eeb344432c3c87df0594068dc0ce.

[22] M. Romanych and R. Cordray III, "Objectives in the Information Environment," *IOSphere*, no. Winter, pp. 26-29, 2006.

[23] 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.

[24] Cisco, "2013 Cisco Annual Threat Report," 2013. [Online]. Available: https://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2013_ASR.pdf.

[25] Georgia Institute of Technology, "Emerging Cyber Threats 2013," December 2012. [Online]. Available: http://www.gtcybersecuritysummit.com/pdf/2013ThreatsReport.pdf.

[26] McAfee, "2013 Threats Predictions," December 2012. [Online]. Available: http://www.mcafee.com/us/resources/reports/rp-threat-predictions-2013.pdf.

[27] DHS, "A Roadmap for Cybersecurity Research," November 2009. [Online]. Available: http://www.cyber.st.dhs.gov/docs/DHS-Cybersecurity-Roadmap.pdf.

[28] Centre for Secure Information Technologies (CSIT), "Report of the World Cybersecurity Research Summit," 2012. [Online]. Available: http://www.csit.qub.ac.uk/InnovationatCSIT/Reports/Filetoupload,295595,en.pdf.

[29] A. Sarma, D. Velthausz and A. Leitjens, "Trust in Digital Life Strategic Research Agenda," 26 March 2012. [Online]. Available:

http://www.trustindigitallife.eu/uploads/TDL-SRA-version-2.pdf.

[30] National Science and Technology Council, "Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program," December 2011. [Online]. Available: http://www.cyber.st.dhs.gov/wp-content/uploads/2011/12/Fed_Cybersecurity_RD_Strategic_Plan_2011.pdf.

[31] S. Barnum, "Standardizing Cyber Threat Intelligence Information with the STructured Information eXpression (STIX(TM))," 2012. [Online]. Available: http://stix.mitre.org/about/documents/STIX_Whitepaper_v1.0_(Draft).pdf. [Accessed 14 February 2013].

[32] M. Maybury, "Detecting Malicious Insiders in Military Networks," 2006. [Online]. Available: http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA456254.

[33] DHS/NPPD, "Privacy Impact Assessment for the Enhanced Cybersecurity Services (ECS), DHS/NPPD/PIA-028," 13 January 2013. [Online]. Available: http://www.dhs.gov/sites/default/files/publications/privacy/privacy_pia_nppd_ecs_jan2013.pdf.

[34] The MITRE Corporation, "Threat-Based Defense: A New Cyber Defense Playbook," July 2012. [Online]. Available: http://www.mitre.org/work/cybersecurity/pdf/cyber_defense_playbook.pdf.

[35] 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.

[36] S. Charney, "Rethinking the Cyber Threat: A Framework and a Path Forward," 2009. [Online]. Available: download.microsoft.com/download/.../rethinking-cyber-threat.pdf.

[37] Invincea, "Defending Against the Advanced Persistent Threat: A Case Study in Deriving Adversarial Attribution from a Thwarted Targeted Attack," 24 January 2013. [Online]. Available: http://www.invincea.com/wp-content/uploads/INVINCEA-ATTRIBUTIONAL-WHITE-PAPER.pdf.

[38] 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.

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

[40] E. M. Hutchins, M. J. Cloppert and R. M. Amin, "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains," Proceedings of the 6th International Conference on Information-Warfare & Security (ICIW 2011), March 2011. [Online]. Available: http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf.

[41] J. Espenschied and A. Gunn, "Threat Genomics: An evolution and recombination of best-available models and techniques for characterizing and understanding computer network threats," 2012. [Online]. Available: http://www.securitymetrics.org/content/attach/Metricon7.0/Metricon_7_paper_Threat_Genomics-EspenschiedGunn2012.pdf.

[42] Dell Secureworks, "Lifecycle of an Advanced Persistent Threat," 2013. [Online]. Available: http://www.secureworks.com/cyber-threat-intelligence/advanced-persistent-threats/understand-threat/.

[43] 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.

[44] Microsoft, "Determined Adversaries and Targetted Attacks: Microsoft Security Intelligence Report, Volume 12," December 2011. [Online]. Available: http://www.microsoft.com/en-us/download/details.aspx?id=29569.

[45] The MITRE Corporation, "Cyber Risk Remediation Analysis," Systems Engineering Guide, 2 May 2012. [Online]. Available: http://www.mitre.org/work/systems_engineering/guide/enterprise_engineering/se_for_mission_assurance/cyberrisk_remediation.html.

[46] D. L. Buckshaw, G. S. Parnell, W. L. Unkenholz, D. L. Parks, J. M. Wallner and O. S. Saydjari, "Mission Oriented Risk and Design Analysis of Critical Information Systems," *Millitary Operations Research, V.10, No.2,* pp. 19-38, 2005.

[47] T. Heberlein, M. Bishop, E. Ceesay, M. Danforth, C. G. Senthilkumar and T. Stallard, "A Taxonomy for Comparing Attack-Graph Approaches," 5 April 2005. [Online]. Available: http://www.netsq.com/Documents/AttackGraphPaper.pdf.

[48] CNSS, "National Information Assurance (IA) Approach to Incident Management (IM), CNSS 048-07," May 2007. [Online]. Available: http://www.cnss.gov/Assets/pdf/CNSS-048-07.pdf.

[49] S. Musman, A. Temin, M. Tanner, D. Fox and B. Pridemore, "Evaluating the Impact of Cyber Attacks on Missions, PR 09-4577," 2009. [Online]. Available: http://www.mitre.org/work/tech_papers/2010/09_4577/09_4577.pdf.

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

[51] S. Roy, C. Ellis, S. Shiva, D. Dasgupta,, V. Shandilya, and Q. Wu, "A Survey of Game Theory as Applied to Network Security," in *Proceedings of the 43rd Hawaii International Conference on System Sciences - 2010*, Honolulu, 2010.

[52] S. Shen, G. Yue and Q. Cao, "A Survey of Game Theory in Wireless Sensor Network Security," *Journal of Networks*, pp. 521-532, March 2011.

[53] M. H. Manshaei, Q. Zhu, T. Alpcan, T. Basar and J.-P. Hubaux, "Game Theory Meets Network Security and Privacy," *ACM Transactions on Computational Logic*, September 2010.

[54] B. Paramasivan and K. M. Pitchai, "Comprehensive Survey on Game Theory based Intrusion Detection System for Mobile Adhoc Networks," 2011. [Online]. Available: http://research.ijcaonline.org/nsc/number5/SPE055T.pdf.

[55] T. Alpcan and T. Baser, Network Security: A Decision and Game-Theoretic Approach, Cambridge University Press, 2011.

[56] S. Jajodia, A. K. Ghosh, V. S. Subrahmanian, V. Swarup, C. Wang, X. S. Wang and (editors), Moving Target Defense II: Application of Game Theory and Adversarial Modeling (Advances in Information Security), New York: Springer, 2012.

[57] R. Pibil, V. Lisy, C. Kiekintveld, B. Bosansky and M. Pechoucek, "Game Theoretic Model of Strategic Honeypot Selection in Computer Networks," *Proceedings of the 3rd Annual Conference on Decision and Game Theory for Security (GameSec 2012), LNCS 7638,* pp. 201-220, November 2012.

[58] P. Sweeney and G. Cybenko, "An Analytic Approach to Cyber Adversarial Dynamics," in *Sensors, and Command, Control, Communications, and Intelligence (C3I) Technologies for Homeland Security and Homeland Defense XI, Proceedings of SPIE vol.8359,* 2012.

[59] P. Liu, W. Zang and M. Yu, "Incentive-Based Modeling and Inference of Attacker Intent, Objectives, and Strategies," *ACM Transactions on Information and Systems Security (TISSEC),* 7 February 2005.

[60] J. Lin, P. Liu and J. Jing, "Using Signaling Games to Model the Multi-Step Attack-Defense Scenarios on Confidentiality," *GameSec 2012: Conference on Decision and Game Theory for Security*, November 2012.

[61] C. A. Kamhoua, N. Pissinou and K. Makki, "Game-Theoretic Modeling and Evolution of Trust in Autonomous Multi-Hop Networks," June 2011. [Online]. Available: http://202.194.20.8/proc/ICC2011/DATA/01-022-02.PDF.

[62] M. van Dijk, A. Juels, A. Oprea and R. L. Rivest, "FLIPIT: The Game of “Stealthy Takeover”," 26 February 2012. [Online]. Available: http://www.rsa.com/rsalabs/presentations/Flipit.pdf.

[63] K. D. Bowers, M. van Dijk, R. Griffin, A. Juels, A. Oprea, R. L. Rivest and N. Triandopoulos, "Defending Against the Unknown Enemy: Applying FLIPIT to System Security," 2012. [Online]. Available: http://eprint.iacr.org/2012/579.pdf.

[64] L. Dritsoula, P. Loiseau and J. Musacchio, "Computing the Nash Equilibria of Intruder Classification Games," *GAMESEC 2012, 3rd Conference on Decision and Game Theory for Security*, November 2012.

[65] B. Z. Moayedi and A. M. Azgomi, "A game theoretic framework for evaluation of the impacts of hackers diversity on security measures," *Reliability Engineering and System Safety, Vol. 99,* pp. 45-54, March 2012.

[66] A. Nochenson and C. L. Heimann, "Simulation and Game-Theoretic Analysis of an Attacker-Defender Game," *Proceedings of the 3rd International Conference on Decision and Game Theory for Security (GameSec 2012), LNCS 7638,* pp. 138-151, November 2012.

[67] J. Blocki, N. Christin, A. Datta and A. Sinha, "Audit Mechanisms for Provable Risk Management and Accountable Data Governance," *Decision and Game Theory for Security (GameSec 2012), Lecture Notes in Computer Science 7638,* pp. 38-59, November 2012.

[68] M. J. Kearns, M. L. Littman and S. P. Singh, "Graphical Models for Game Theory," *UAI '01 Proceedings of the 17th Conference in Uncertainty in Artificial Intelligence,* 2001.

[69] B. Schneier, "Attack trees: modeling security threats," *Dr. Dobbs Journal,* December 1999.

[70] S. Mauw and M. Oostdijk, "Foundations of Attack Trees," *International Conference on Information Security and Cryptology – ICISC 2005,* 2005.

[71] A. Singhal and X. Ou, "Security Risk Analysis of Enterprise Networks Using Probabilistic Attack Graphs, NISTIR 7788," August 2011. [Online]. Available:

http://csrc.nist.gov/publications/nistir/ir7788/NISTIR-7788.pdf.

[72] S. Jajodia and S. Noel, "Advanced Cyber Attack Modeling, Analysis, and Visualization (AFRL-RI-RS-TR-2010-078)," March 2010. [Online]. Available: http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA516716.

[73] J. H. Espedalen, "Attack Trees Describing Security in Distributed Internet-Enabled Metrology," 2007. [Online]. Available: http://www.justervesenet.no/getfile.aspx/document/epcx_id/564/epdd_id/1113.

[74] S. Khaitan and S. Raheja, "Finding Optimal Attack Path Using Attack Graphs: A Survey," *International Journal of Soft Computing and Engineering (IJSCE),* pp. 33-36, July 2011.

[75] O. Sheyner and J. Wing, "Tools for Generating and Analyzing Attack Graphs," *Proceedings of Workshop on Formal Methods for Components and Objects,* 2004.

[76] X. Ou, W. F. Boyer and M. A. McQueen, "A Scalable Approach to Attack Graph Generation," *Proceedings of the 13th ACM conference on Computer and communications security (CCS'06),* 2006.

[77] F. Chen, R. Tu, Y. Zhang and J. Su, "Two Scalable Analyses of Compact Attack Graphs for Defending Network Security," *2009 International Conference on Networks Security, Wireless Communications and Trusted Computing,* 2009.

[78] D. M. Johnson and L. Notargiacomo, "Decision Analysis to Counter Cyber Attacks (DACCA)," 2009. [Online]. Available: http://www.mitre.org/news/events/exchange09/03X97563.pdf.

[79] W. Li, R. B. Vaughn and Y. S. Dandass, "An Approach to Model Network Exploitations Using Exploitation Graphs," *Simulation,* pp. 523-541, August 2006.

[80] N. Idika and B. Bhargava, "Extending Attack Graph-Based Security Metrics and Aggregating Their Application," *IEEE Transactions on Dependable and Secure Computing,* pp. 75-85, January 2012.

[81] E. LeMay, M. D. Ford, K. Keefe, W. H. Sanders and C. Muercke, "Model-based Security Metrics using ADversary VIew Security Evaluation (ADVISE)," *8th International Conference on Quantitative Evaluation of Systems (QEST),* 2011.

[82] E. A. LeMay, "Adversary-Driven State-Based System Security Evaluation," 2011. [Online]. Available: https://www.perform.csl.illinois.edu/Papers/USAN_papers/11LEM02.pdf.

[83] N. Poolsappasit, R. Dewri and I. Ray, "Dynamic Security Risk Management Using Bayesian Attack Graphs," *IEEE Transactions on Dependable and Secure Computing, Vol. 9, No. 1,* pp. 61-74, January/February 2012.

[84] 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.

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

[86] HP, "Business White Paper: Collaborative Defense," September 2013. [Online]. Available: http://h20195.www2.hp.com/V2/GetPDF.aspx%2F4AA4-6187ENW.pdf.

[87] 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.

[88] 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.

[89] S. Bhattacharya and S. K. Ghosh, "A Decision Model based Security Risk Management Approach," *Proceedings of the International MultiConference of Engineers and Computer Scientists 2008 Vol II*, March 2008.

[90] M. Frigault, L. Wang, A. Singhal and S. Jajodia, "Measuring Network Security Using Dynamic Bayesian Network," *Proceedings of the 2008 Quality of Protection Workshop (QoP '08)*, October 2008.

[91] I. Lachow, "Active Cyber Defense: A Framework for Policymakers," February 2013. [Online]. Available: http://www.cnas.org/files/documents/publications/CNAS_ActiveCyberDefense_Lachow_0.pdf.

[92] C. L. Glaser, "Deterrence of Cyber Attacks and U.S. National Security, Report GW-CSPRI-2011-5," 1 June 2011. [Online]. Available: http://www.cspri.seas.gwu.edu/Seminar%20Abstracts%20and%20Papers/2011-5%20Cyber%20Deterrence%20and%20Security%20Glaser.pdf.

[93] O. M. Sheyner, "Scenario Graphs and Attack Graphs," 12 April 2004. [Online]. Available: http://www.cs.cmu.edu/~scenariograph/sheynerthesis.pdf.

[94] H. S. Lin, "Offensive Cyber Operations and the Use of Force," Journal of National Security Law & Policy, Vol. 4:63, 2010. [Online]. Available: http://jnslp.com/wp-content/uploads/2010/08/06_Lin.pdf.

[95] DoD, "Department of Defense Cyberspace Policy Report," November 2011. [Online]. Available: http://s3.documentcloud.org/documents/266862/department-of-defense-cyberspace-policy-report.pdf.

Appendix A Acronyms

ADVISE	ADversary VIew Security Evaluation
APT	Advanced Persistent Threat
AS&W	Attack Sensing and Warning
AWF	Adversary Work Factor
BADGERS	Building Analysis Datasets and Gathering Experience Returns for Security
C2	Command and Control
C3	Command, Control, and Communications
CIE	Cyber Impact Effects
CNA	Computer Network Attack
CND	Computer Network Defense
CNSS	Committee on National Security Systems
CCoA	Cyber Course of Action
CoA	Course of Action
DACCA	Decision Analysis to Counter Cyber Attacks
DARPA	Defense Advanced Research Projects Agency
DCO	Defensive Cyber Operations
DoD	Department of Defense
DREAD	Damage, Reproducibility, Exploitability, Affected users, Discoverability
DT&E	Developmental Test and Evaluation
FBI	Federal Bureau of Investigation
I&W	Indications and Warning
ICT	Information and Communications Technology
IDART	Information Design Assurance Red Team
IETF	Internet Engineering Task Force
IO	Information Operations
JP	Joint Publication
KPP	Key Performance Parameter
MODA	Multiple Objective Decision Analysis
MOE	Measure of Effectiveness

MOP	Measure of Performance
MORDA	Mission Oriented Risk and Design Analysis
MTTR	Mean Time to Recover
NIST	National Institute of Standards and Technology
NSF	National Science Foundation
OCO	Offensive Cyber Operations
RAdAC	Risk-Adaptive Access Control
RTWF	Red Team Work Factor
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
TTP	Tactic, Technique, Procedure
WFR	Work Factor Ratio
WOMBAT	Worldwide Observatory of Malicious Behaviors and Attack Threats

Appendix B Approaches to Adversary Modeling

This appendix examines different approaches to adversary modeling, with the goal of identifying elements that can be used to make hypotheses and claims about effects on the adversary meaningful, useful, and capable of being supported or refuted via analysis and evidence[14].

B.1.1 Game-Theoretic Modeling

Game-theoretic approaches have long been applied to computer and network security (see [51] [52] [53] [54] [55] for surveys), and are increasingly viewed as useful for more novel cyber defense techniques (e.g., moving target [56], deception [57]). Roy et al. identify several key weaknesses in conventional approaches to applying game theory to cyber security: many approaches assume perfect information, complete information, or static (rather than dynamic) games [51]. Meta-game analysis [58], in which aspects of the underlying game can change in the course of the game, is an attempt to address these weaknesses. In addition, dynamic [59] (or multi-step [60]) and evolutionary [61] game-theoretic approaches, which partially address these weaknesses, are increasingly applied to the security domain. FLIPIT [62] provides a game framework for understanding stealthy compromise, and enables strategic principles to be stated clearly and succinctly [63].

In game-theoretic modeling, key aspects of an adversary to be modeled include intent, objectives, and strategies [59]; these (together with resources) can be summarized as the adversary type. To the extent that defender strategies are predicated on knowledge of or beliefs about the adversary, determining the adversary type (or more specific aspects) can provide defender advantages [64] [65]. Aspects of the game environment that can be viewed as part of the adversary model include the set of possible actions, constraints, costs, and payoffs (or utilities) applicable to adversaries. Effects on the adversary can be represented as changes to these aspects of the game environment. In meta-game analysis, changes to the game environment can also represent effects on the adversary (e.g., changes to the set of possible adversary actions).

The formalization of game-theoretic modeling enables hypotheses or claims about the effects of a defender action on the adversary to be stated in terms of modeling constructs. Theorems can be proven, to provide (sometimes counter-intuitive) insights about cost-effective defense. Attacker and defender strategies can be examined, and Nash equilibrium strategies can be derived [66]. Metrics for effects on the adversary can be derived, e.g., as changes in expected values of utility functions. Empirical studies to validate predicted effects can be suggested [67].

B.1.2 Attack Graph Models

While graphical models of games are used in game theory [68][15], attack trees [69] (and more generally, attack graphs), these models are historically more related to fault trees [70]. Attack trees and attack graphs are used in risk analysis [71], vulnerability analysis [72], and penetration testing [73]. A variety of automated tools for attack graph generation and analysis

[14] Metrics, based on measurements and observations, are a highly desired form of evidence. The body of data needed to evaluate metrics may be too sparse for metric values to be meaningful. However, analysis of such data as exists may still provide evidence to support or refute hypotheses or claims.

[15] See [93] for a discussion of attack graphs and game theory.

have been developed and applied [74] [75] [47], supplemented with approaches to problems of scalability [76] [77].

MORDA (Mission Oriented Risk and Design Analysis) incorporates attack trees, together with models of the adversary, the user, and service providers [46]. An adversary has a set of possible attacks and an attack preference function, which reflects the adversary's value model. For the value model in [46], four adversary objectives are identified: maximize the likelihood of successfully completing an attack, minimize the likelihood of detection, minimize the resources required to execute the attack, and maximize the impact of the attack; qualitative value scales are included for minimizing the likelihood of detection and for mission impact of a denial-of-service attack. An effect on the adversary would be represented as a change in the adversary's ability to achieve one or more of these objectives.

MORDA applies MODA (multiple objective decision analysis) primarily to possible defender activities, but MODA can also be applied to the adversary [46]. DACCA (Decision Analysis to Counter Cyber Attacks [78] [18]) defines attack attractiveness as a combination of attacker objectives, resources, and risk. An effect on the adversary would be represented as a change in one or more elements of attack attractiveness.

Attack graphs, while represented in different ways, can be mapped to a representation consisting of nodes and arcs, where an arc represents an attack that changes the state of the system and a node represents a state of the system (including attacker capabilities) [47].[16] Depending on the specific attack tree or attack graph model, an attack (a traversal of the graph or tree) can have an associated likelihood of success, payoff or utility to the attacker, or combination (i.e., expected payoff). Exploitation graphs enable AWF to be evaluated in several ways, including as the number of branches; minimum, maximum, and average path length; and minimum, maximum, and average cost for each path [79]. An approach to aggregating the results of attack graph analysis and metrics addresses weaknesses in the use of these metrics to compare the relative security of different attack graphs [80]. The ADVISE (ADversary VIew Security Evaluation) method [81] [82] provides a rich attack graph representation, in which effects on the adversary can involve changes to the attractiveness, cost, probability of detection, and expected payoff of an attack step to the adversary (within a specified time horizon).

Bayesian attack graphs enable adversary beliefs and attack evidence to be considered in assessing likelihoods [83].[17] In this context, effects on the adversary include changes in the adversary's knowledge and beliefs.

B.1.3 Cyber Attack Lifecycle Modeling

The recognition that attacks or intrusions by advanced cyber adversaries against organizations or missions are multistage, and occur over periods of months or years, has led to the development of models of the cyber attack lifecycle[18]. A model of the cyber attack lifecycle is frequently referred to as a "cyber kill chain." An initial cyber kill chain model was developed by Lockheed

[16] Other representations use different types of nodes to represent, for example, system state and attacker actions, with arcs representing pre- and post-conditions of attacker actions [71].
[17] Bayesian networks derived from attack graphs have more commonly considered the defender's beliefs and evidence [89] [90].
[18] NIST SP 800-30 uses the phrase "cyber campaign" to describe the cyber attack lifecycle [35]. However, some prefer to reserve the phrase "cyber campaign" to apply to multiple intrusion attempts, sometimes involving multiple organizational targets and/or non-cyber attack vectors.

Martin [39]. In a subsequent paper [40], six types of effects on the adversary, consistent with the 2006 version of JP 3-13, are considered: detect, deny, disrupt, degrade, deceive, and destroy.

MITRE uses a slightly different version [34], consistent with NIST SP 800-30 Rev.1 [35] and the Guidelines for Cybersecurity DT&E [84]. As illustrated in Figure 1, the cyber attack lifecycle includes seven phases:

- Phase 1, Recon (or Perform Reconnaissance): The adversary identifies a target and develops intelligence to inform attack activities. The adversary develops a plan to achieve desired objectives.
- Phase 2, Weaponize: The adversary develops or acquires a harmful mechanism (e.g., tailored malware, 0-day exploits) and places it in a form that can be delivered to and executed on the target device, computer, or network. For example, malware is tailored to a target system and inserted into a document; a compromised component that includes a backdoor is developed for insertion into the supply chain for network components.
- Phase 3, Deliver: The mechanism is delivered to the target system. For example, tailored malware is included in an attachment to a spearphishing email; compromised components inserted in the supply chain are integrated into a target network.
- Phase 4, Exploit: The initial attack on the target is executed. A vulnerability is exploited, and malware is installed and activated on an initial target system.
- Phase 5, Control: The adversary employs mechanisms to manage the initial targets, perform internal reconnaissance, and compromise additional targets via lateral movement and privilege escalation. The structure of the cyber attack lifecycle is recursive – within the control phase, the entire attack lifecycle can be carried out.
- Phase 6, Execute: Leveraging numerous techniques, the adversary executes the plan and achieves desired objectives.
- Phase 7, Maintain: The adversary maintains a long-term presence on target devices, systems, or networks. To do so, the adversary may erase indications of prior presence or activities.

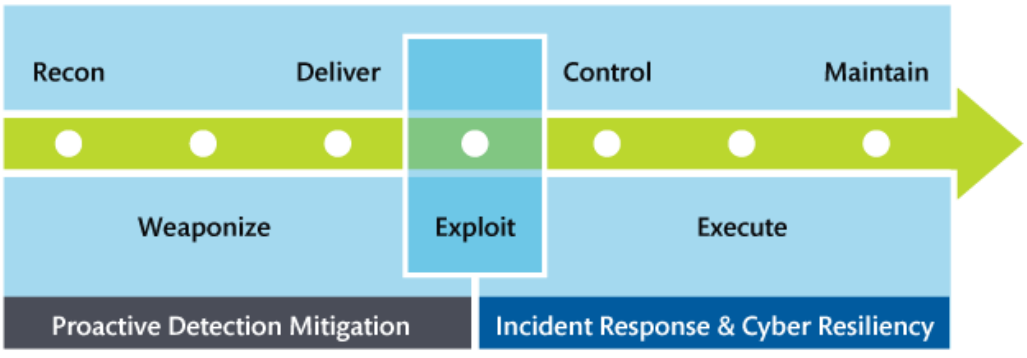

Figure 2. The Cyber Attack Lifecycle

Variant attack lifecycles are common. Most focus on exfiltration of sensitive information as the adversary's objective. For example, an ARDA Workshop designed a version to characterize activities by insiders [85]: reconnaissance, access, entrenchment, exploitation, communication,

manipulation, extraction & exfiltration, and counter intelligence. Raytheon [43] uses a six-phase model: Footprint, Scan, Enumerate, Gain Access, Escalate Privileges, and Pilfer. Dell Secureworks identifies 12 stages: define target, find and organize accomplices, build or acquire tools, research target infrastructure/employees, test for detection, deployment, initial intrusion, outbound connection initiated, expand access and obtain credentials, strengthen foothold, exfiltrate data, and cover tracks and remain undetected [42]. HP uses a five-phase structure: research, infiltration, discovery, capture, and exfiltration [86].

Other attack lifecycles do not specify the adversary's objectives, and thus enable cyber attacks that directly impact organizations and their missions (e.g., via denial of service, via data corruption or falsification) to be represented. Microsoft researchers have identified a set of ten "base types" of actions: reconnaissance, commencement, entry, foothold, lateral movement, acquire control, acquire target, implement / execute, conceal & maintain, and withdraw [41]. Mandiant [38] describes an attack lifecycle consisting of Initial Recon; Initial Compromise; Establish a Foothold; a cycle of Escalate Privileges, Internal Recon, Move Laterally, and Maintain Presence; and Complete Mission. Threat reports also describe different lifecycle structures; for example, Sophos [23] outlines Blackhole and Andr/Boxr campaigns.

B.1.4 Modeling Adversary Characteristics

Game-theoretic, attack graph, and cyber attack lifecycle models assume (implicitly or explicitly) characteristics of the adversary. Models of adversary characteristics can be high-level, for example, capability, intent, and targeting [35] [17]. Levels or tiers of adversaries can be characterized [87], differentiated by such characteristics as commitment and resources (for which component attributes can be defined) [88]. To be useful and internally consistent, any discussion of effects on the adversary needs to be grounded in clear assumptions about adversary characteristics.

The Cyber Impact Effects (CIE) language has been developed to describe the mission impacts of cyber attacks [49] [50]: degradation, interruption, modification, fabrication, unauthorized use, and interception. Those impacts can be used to describe adversary objectives, a key component of intent reflected in the Execute stage of the cyber attack lifecycle. To a lesser extent, the impacts can also be viewed as intended effects of defender activities on the adversary; however, that view is most relevant in the context of Offensive Cyber Operations (OCO) or Computer Network Attack (CNA), which is outside the scope of this document.

Appendix C Detailed Analysis of Effects of Cyber Resiliency Techniques on the Adversary

This Appendix provides details on the mapping of cyber resiliency techniques to stages in the cyber attack lifecycle presented in Table 6. Each technique – described as something an architecture, service, system, network, or system-of-systems does – includes functional capabilities as well as architectural (and, to a lesser extent, operational) approaches. For each phase (or set of phases), intended or potential effects of the capability or approach on the adversary are described, using the proposed vocabulary. It must be emphasized that this is a notional mapping; for a given instance or implementation, a more specific description of the effects on the adversary can be given, analyzed to identify potential evidence, and then evaluated in light of evidence gathered in an evaluation environment.

Table 7. How Adaptive Response Could Affect Adversary Activities

Adaptive Response: Take actions in response to indications that an attack is underway based on attack characteristics		
Capability or Approach	**Phase of Cyber Attack Lifecycle**	**Effect on Adversary**
Dynamic Reconfiguration: Make changes to an element or constituent system while it continues operating	Recon	Curtail: The adversary's knowledge of resources and configuration becomes outdated. Contain: The resources against which the adversary can conduct recon are restricted.
	Weaponize	Degrade: The adversary's development or acquisition of exploits is based on outdated or incorrect premises, making the exploits less effective.
	Deliver	Curtail: The adversary's delivery mechanism stops working.
	Exploit	Prevent: The adversary's exploit is based on outdated premises.
	Control, Maintain	Contain: The adversary's activities are limited to resources that have not been reconfigured. Curtail: Reconfiguration (e.g., changing internal communications or call paths) renders the adversary's activities ineffective.
	Execute	Prevent: Reconfiguration (e.g., blocking ports and protocols) renders ineffective the activities the adversary could take to achieve mission.
Dynamic Reallocation: Make changes in the allocation of resources to tasks or functions without terminating functions or processes	Control, Execute, Maintain	Curtail: Resource reallocation removes resources from the adversary's control.
	Execute	Degrade: Resource reallocation enables mission continuity at some level, reducing the effectiveness of the adversary's goal of denying mission capabilities. Recover: Resource reallocation enables recovery of mission functions when the adversary's goal is denial of service.
Dynamic Composability: Replace software elements with equivalent functionality without disrupting service	Control, Execute, Maintain	Contain: The adversary's activities are limited to resources that conform to behavioral templates (e.g., interfaces, call sequences, implementation languages and libraries) that existed when the adversary began probing; thus, lateral movement is restricted.

Table 8. How Analytic Monitoring Could Affect Adversary Activities

Analytic Monitoring: Gather and analyze data on an ongoing basis and in a coordinated way to identify potential vulnerabilities, adversary activities, and damage		
Capability or Approach	**Phase of Cyber Attack Lifecycle**	**Effect on Adversary**
Monitoring: Monitor and analyze behavior and characteristics of elements to look for indicators of adversary activity	Recon, Deliver, Control, Maintain	Detect: Monitoring provides indications and warning (I&W) or attack sensing and warning (AS&W), making the adversary's activities visible to defenders.
Malware and Forensic Analysis: Analyze artifacts left by adversary activities, to develop observables, indicators, and adversary TTPs	Deliver	Prevent: The use of a detonation chamber for suspected malicious emails or attachments can prevent delivery.
	Deliver Exploit, Control, Maintain	Analyze: The adversary's TTPs and capabilities are better understood.
Damage Assessment: Analyze behavior, data, and system artifacts to determine the presence and extent of damage	Exploit, Execute	Detect: Damage assessment reveals the extent of the effects of adversary activities.
Sensor Fusion and Analysis: Fuse and analyze monitoring data and preliminary analysis results from different elements, together with externally provided threat intelligence, to look for indicators of adversary activity that span elements; to identify attack trends; and (in conjunction with Malware and Forensic Analysis) to develop threat intelligence	Recon, Control, Maintain	Detect: Sensor fusion enables enhanced I&W or AS&W, making the adversary's activities visible to defenders. Analyze: Sensor fusion enables more complete and comprehensive analysis of adversary activities.

Table 9. How Coordinated Defense Could Affect Adversary Activities

Coordinated Defense: Manage adaptively and in a coordinated way multiple, distinct mechanisms to defend critical resources against adversary activities		
Capability or Approach	**Phase of Cyber Attack Lifecycle**	**Effect on Adversary**
Technical Defense-in-Depth: Make use of multiple protective mechanisms, applied at different architectural layers or locations	Weaponize	Impede: The adversary must develop or acquire exploits effective against multiple defensive technologies to be successful.
	Exploit	Impede: The adversary must use multiple exploits to obtain a foothold.
Coordination and Consistency Analysis: Apply processes, supported by analytic tools, to ensure that defenses are applied and cyber courses of action are defined and executed in a coordinated, consistent, and non-disruptive way	Control, Maintain	Detect: Inconsistencies (e.g., in configurations or in privilege assignments) provide indications of adversary activities.
Adaptive Management: Change how defensive mechanisms are used based on changes in the operational and threat environment	Control, Maintain	Impede: The adversary must adapt to changing processes.

Table 10. How Deception Could Affect Adversary Activities

Deception: Use obfuscation and misdirection (e.g., disinformation) to confuse or mislead an adversary		
Capability or Approach	**Phase of Cyber Attack Lifecycle**	**Effect on Adversary**
Masking: Obfuscate data or system behavior (e.g., via encryption or function hiding)	Recon	Prevent: The adversary cannot make the observations needed to inform further activities.
	Execute	Degrade: The adversary cannot reliably determine which targets are valuable, and hence must either try to affect more targets (e.g., exfiltrate more files, bring down more VMs) than necessary to achieve objectives, or accept more uncertainty as to effectiveness.
Repackaging: Transform data using closely held mechanisms	Recon	Impede: The adversary must perform additional analysis to determine or acquire the utility of repackaged data (e.g., configuration files).
	Execute	Degrade: The adversary cannot make as effective use of target data (e.g., the adversary must make additional transformations, possibly with data loss).
Misdirection / Simulation: Create and maintain false target environments (e.g., deception environments) and direct adversary activities to them	Recon	Divert: The adversary is directed to false targets; the adversary's efforts are wasted. Deceive: The adversary develops false intelligence about the defender's cyber resources, mission / business function dependencies, or TTPs. Analyze: Analysis of adversary activities increases understanding of adversary TTPs, capabilities, intent, and targeting.
	Weaponize	Deceive: The adversary develops or acquires exploits compatible with the deception environment rather than the operational environment; the adversary's efforts are wasted.
	Exploit	Deceive: The adversary's exploits falsely appear to succeed and grant access to targets; the adversary's efforts are wasted. Analyze: Analysis of the adversary's exploits increases understanding of adversary TTPs and capabilities.
	Deliver, Control, Execute, Maintain	Divert: The adversary's efforts are wasted on false targets. Analyze: Analysis of adversary activities increases understanding of adversary TTPs, capabilities, intent, and targeting.
Dissimulation / Disinformation: Create false target data (e.g., fabricating documents or data stores, creating false target data or simulating a non-existent application) or operational data (e.g., simulated traffic, simulated configuration data), or provide deliberately confusing responses to adversary requests	Recon, Control, Execute, Maintain	Detect: The adversary's use of fabricated control data (e.g., configuration, network topology, or asset inventory data) serves as an indicator of adversary activity. Deceive: The adversary's knowledge about mission or defender activities is incomplete or (if defenders place false information on C3 paths to which the adversary has access) false.
	Recon, Execute	Detect: Attempts to access fabricated targets provides an indication of adversary activities. Divert: The adversary directs efforts at fabricated targets (e.g., fabricated mission, configuration, or topology data).
	Weaponize	Deceive: The adversary's efforts are based on false information (e.g., configuration data) and thus are wasted. Impede: The adversary must develop or acquire exploits effective against multiple technologies. Analyze: Analysis of adversary activities increases understanding of adversary TTPs, capabilities, intent, and targeting.
	All phases post-Recon	Deter: Adversary reconnaissance falsely indicates that the expected value of carrying out a cyber attack does not justify the expected costs or risks.

Table 11. How Diversity Could Affect Adversary Activities

Diversity: Use a heterogeneous set of technologies (e.g., hardware, software, firmware, protocols) and data sources to minimize the impact of attacks and force adversaries to attack multiple different types of technologies		
Capability or Approach	**Phase of Cyber Attack Lifecycle**	**Effect on Adversary**
Architectural Diversity / Heterogeneity: Use multiple sets of technical standards, different technologies, and different architectural patterns, thereby accommodating different components that provide the same functionality	Control, Maintain	Degrade: The adversary must control a set of compromised resources with different characteristics (requiring greater expertise and effort). Contain: The adversary is limited to controlling compromised resources about which they have expertise and for which they have control tools.
	Execute	Recover: Recovery from the mission effects of adversary activities can create opportunities for further adversary activities. Secure recovery is facilitated by using components against which the adversary does not have exploits or control tools.
	Weaponize	Impede: The adversary must develop or acquire exploits effective against variant implementations.
Design Diversity / Heterogeneity: Use different designs to meet the same requirements or provide equivalent functionality	Weaponize, Control, Execute, Maintain	Same as for Architectural Diversity / Heterogeneity.
Dynamic or Synthetic Diversity: Transform implementations so that for no specific instance is the implementation completely predictable	Control, Maintain	Degrade: The adversary must control a set of compromised resources with different characteristics.
Command, Control, and Communications (C3) Path Diversity: Provide multiple paths, with demonstrable degrees of independence, for information to flow between elements	Control, Execute, Maintain	Recover: Recovery from the mission effects of adversary activities is facilitated by the use of C3 paths to which the adversary lacks access (e.g., out-of-band communications among defenders).
Information Diversity: Provide information from different sources or transform information in different ways	Control, Execute, Maintain	Degrade: The adversary must modify or replace multiple different versions of information in order to corrupt mission or system information without detection. Recover: Reconstruction of mission or system information is facilitated by having multiple sources.

Table 12. How Dynamic Positioning Could Affect Adversary Activities

Dynamic Positioning: Use distributed processing and dynamic relocation of critical assets and sensors to change the attack surface		
Capability or Approach	**Phase of Cyber Attack Lifecycle**	**Effect on Adversary**
Functional Relocation of Sensors: Relocate sensors, or reallocate responsibility for specific sensing tasks, to look for indicators of adversary activity, and to watch for adversary activities during recovery and evolution	Recon, Control, Execute, Maintain	Detect: The adversary's ability to remain hidden, assuming a fixed monitoring infrastructure, is decreased.
Functional Relocation of Cyber Assets: Change the location of assets that provide functionality (e.g., services, applications) or information (e.g., data stores), either by moving the assets or by transferring functional responsibility	Recon, Control, Execute, Maintain	Divert: The adversary focuses activities on defender-chosen resources. Curtail: The period in which adversary activities are effective against a given location or instance of an asset is limited.
	Control, Execute, Maintain	Expunge: Compromised running software is deleted, if relocation involves re-instantiating software from a clean version.
Physical Asset Mobility: Physical assets (e.g., platforms or vehicles, mobile computing devices) are physically relocated	Recon, Control, Execute, Maintain	Curtail: The period in which adversary activities are effective against a given location or instance of an asset is limited.
Distributed Functionality: Functionality (e.g., processing, storage, communications) is distributed across multiple elements	Control, Execute, Maintain	Impede: The adversary must compromise more elements in order to deny or corrupt functionality.

Table 13. How Dynamic Representation Could Affect Adversary Activities

Dynamic Representation: Construct and maintain dynamic representations of components, systems, services, mission dependencies, adversary activities, and effects of alternative cyber courses of action		
Capability or Approach	**Phase of Cyber Attack Lifecycle**	**Effect on Adversary**
Dynamic Mapping and Profiling: Maintain current information about resources, their status, and their connectivity	Control, Maintain	Expunge: Discovered software or components that do not fit asset policy requirements can be removed.
Dynamic Threat Modeling: Maintain current information about threat activities and characteristics (e.g., observables, indicators, TTPs)	Recon, Control, Maintain	Obviate: Information about threat activities and characteristics enables selection of cyber courses of action to prevent the adversary from achieving (what the defender perceives as) their objectives or to take preemptive action.
Mission Dependency and Status Visualization: Maintain current information about mission dependencies on resources, and the status of those resources with respect to threats	Execute	Recover: Recovery of mission capabilities from adversary activities is facilitated by knowledge of which resources were or will be needed.
CoA Analysis: Maintain a set of alternative CoAs, with supporting analysis of resource requirements, contingencies for meeting those requirements, and effects of CoAs on current and future mission capabilities	Recon, Control, Execute, Maintain	The effects are indirect; by defining adequately-resourced CoAs, cyber defenders can identify intended effects and select CoAs to achieve those effects.

Table 14. How Non-Persistence Could Affect Adversary Activities

Non-Persistence: Retain information, services, and connectivity for a limited time		
Capability or Approach	**Phase of Cyber Attack Lifecycle**	**Effect on Adversary**
Non-Persistent Services: Services are refreshed periodically and/or terminated after completion of a request	Exploit	Curtail: The adversary's attempt to exploit a vulnerability is curtailed when the attacked service is terminated.
	Control, Execute Maintain	Curtail: The period during which adversary activities are effective against a given instance of a service is limited.
	Exploit, Control, Maintain	Expunge: Compromised services are terminated when no longer needed; if re-instantiated from a clean version, new instances will not be compromised.
Non-Persistent Information: Information is refreshed to a known trusted state and deleted when no longer needed	Execute	Curtail: The period during which the adversary can acquire mission or control information is limited, as the information is deleted when no longer needed.
Non-Persistent Connectivity: Connections are terminated after completion of a request or after a period of non-use	Control, Execute, Maintain	Curtail: The period during which the adversary can make use of a C3 channel is limited.

Table 15. How Non-Persistence Could Affect Adversary Activities

Privilege Restriction: Restrict privileges required to use cyber resources, and privileges assigned to users and cyber entities, based on criticality and trust, to minimize the potential consequences of adversary activities		
Capability or Approach	**Phase of Cyber Attack Lifecycle**	**Effect on Adversary**
Privilege Management: Define, assign, and maintain privileges associated with end users and cyber entities (e.g., systems, services, devices), based on established trust criteria, consistent with principles of least privilege	Exploit, Control, Execute, Maintain	Contain: Privilege-based usage restrictions limit the adversary's activities to resources for which the false credentials the adversary has obtained allow use. Delay: The adversary's lack of credentials delays access to restricted resources. Prevent: The adversary's lack of credential prevents access to restricted resources.
Privilege-Based Usage Restrictions: Define, assign, maintain, and apply usage restrictions on cyber resources based on mission criticality and other attributes (e.g., data sensitivity)	Exploit, Control, Execute, Maintain	Prevent: Privilege-based usage restrictions prevent the adversary from accessing critical or sensitive resources. Contain: Privilege-based usage restrictions limit the adversary's activities to non-critical resources, or to resources for which the false credentials the adversary has obtained allow use. Degrade: The adversary's lack of credentials delays access to restricted resources or requires the adversary to invest more effort to circumvent access controls.
Dynamic Privileges: Elevate or deprecate privileges assigned to a user, process, or service based on transient or contextual factors (e.g., using RAdAC)	Exploit, Control, Execute, Maintain	Delay: The adversary must obtain additional privileges in order to perform activities.

Table 16. How Realignment Could Affect Adversary Activities

Realignment: Align cyber resources with core aspects of mission/business functions, thus reducing the attack surface		
Capability or Approach	**Phase of Cyber Attack Lifecycle**	**Effect on Adversary**
Purposing: The mission purposes of functions, services (including connectivity as well as processing), information, and systems are identified, to prevent uses that increase risk without any corresponding mission benefit	Deliver, Exploit	Impede: The adversary cannot take advantage of unnecessarily risky uses of resources (e.g., exposure of services to the Internet without offsetting mission benefits).
Offloading / Outsourcing: Supportive but non-essential functions are offloaded to a service provider that is better able to support the functions	Deliver, Exploit	Impede: The set of opportunities the adversary can take advantage of is reduced.
Customization: Critical components are custom-developed or re-implemented	Weaponize	Prevent: The adversary lacks insight into critical customized components, and thus cannot develop exploits. Impede: The adversary must develop exploits against customized components.
Restriction: Risky functionality or connectivity is removed, or replaced with less-risky implementations	Deliver, Control, Execute, Maintain	Prevent: The functionality or connectivity can no longer be used by the adversary. Impede: The set of opportunities the adversary can take advantage of is reduced.
Agility / Repurposing: System elements are repurposed to provide services, information, and connectivity to meet new or changing mission needs	Recon, Control, Maintain	Impede: The adversary must invest additional resources to maintain a current visualization of system elements.

Table 17. How Redundancy Could Affect Adversary Activities

Redundancy: Maintain multiple protected instances of critical resources (information and services)		
Capability or Approach	**Phase of Cyber Attack Lifecycle**	**Effect on Adversary**
Surplus Capacity / Resources: Extra capacity for information storage, processing, or communications is maintained	Execute	Degrade: The extent to which the adversary causes mission functions (e.g., data retrieval, processing, communications) to cease or slow is limited. Recover: Recovery from the effects of adversary activities is facilitated.
Backup and Restore: Functionality is maintained to back up information and software (including configuration data) in a way that protects its confidentiality, integrity, and authenticity, and to restore it in case of disruption or destruction	Execute	Curtail: The time during which the adversary causes mission functions (e.g., data retrieval, processing, communications) to cease or slow is limited. Recover: Recovery from the effects of adversary activities is facilitated.
Replication: Information and/or functionality is replicated (reproduced exactly) in multiple locations	Execute	Degrade: The extent to which the adversary causes mission functions (e.g., data retrieval, processing, communications) to cease or slow is limited. Recover: Recovery from the effects of adversary activities is facilitated.

Table 18. How Segmentation / Separation Could Affect Adversary Activities

Segmentation / Separation: Separate components, subsystems, and systems (logically or physically) based on criticality and trustworthiness, to limit the spread of damage		
Capability or Approach	**Phase of Cyber Attack Lifecycle**	**Effect on Adversary**
Modularity / Layering: Define and implement services and capabilities in a modular way, and in a way that respects the differences between layers in a layered architecture, to enable separation, substitution, and privilege restriction based on criticality	Exploit, Control, Execute, Maintain	Impede: The adversary must do additional work (e.g., obtain additional privileges) to gain access to protected regions (e.g., in a ring architecture).
Predefined Segmentation: Define enclaves, segments, or other types of resource sets based on criticality and trustworthiness, so that they can be protected separately and, if necessary, isolated	Recon, Control, Execute, Maintain	Contain: The adversary's activities (e.g., perform network mapping, propagate malware, exfiltrate data or bring down servers) is restricted to the enclave on which the adversary has established a presence.
	Deliver	Degrade: The number of possible targets to which malware can easily be propagated is limited to the network segment.
	Control, Execute	Detect: Adversary activities involving C3 across network segments that violate policies enforced at barriers between segments are detected.
	Control, Execute, Maintain	Delay: The adversary's ability to perform C3 is delayed, as the adversary must find ways to overcome barriers between network segments.
Dynamic Segmentation / Isolation: Change the definition of enclaves or protected segments, or isolate resources, while minimizing operational disruption	Recon, Exploit, Control, Execute, Maintain	Contain: The adversary's activities (e.g., observe characteristics of running processes, insert malware into running process, control compromised process, use compromised process to achieve mission objectives, maintain covert presence in running process) are limited to the set of processes or services within a segment (e.g., with a specific set of characteristics or context).

Table 19. How Substantiated Integrity Could Affect Adversary Activities

Substantiated Integrity: Ascertain that critical services, information stores, information streams, and components have not been corrupted by an adversary		
Capability or Approach	**Phase of Cyber Attack Lifecycle**	**Effect on Adversary**
Integrity / Quality Checks: Apply and validate checks of the integrity or quality of information, software, or devices	Deliver	Prevent: Malware payloads the adversary tries to deliver (e.g., counterfeit software updates, email attachments) or embed in apparently harmless objects (e.g., documents) are discarded or quarantined before the malware can exploit a vulnerability. Detect: The attempted delivery of malware payloads is detected.
	Execute	Recover: Contaminated data is removed, restoring mission or control data to a known good state.
	Control, Maintain	Detect: The presence of contaminated data or compromised software that the adversary seeks to maintain is detected. Expunge: Software or data that does not meet integrity requirements is removed, thus removing or reducing the adversary's foothold.
Provenance Tracking: Identify and track the provenance of data, software, and/or hardware elements	Deliver	Detect: The adversary's attempts to deliver compromised data, software, or hardware are detected.
	Execute	Expunge: Compromised elements are identified so they can be removed.
Behavior Validation: Validate the behavior of a system, service, or device against defined or emergent criteria (e.g., requirements, patterns of prior usage)	Control, Execute, Maintain	Detect: The presence of adversary-controlled processes is detected by peer cooperating processes. Curtail: Adversary-controlled processes are isolated or terminated by peer cooperating processes.

Table 20. How Unpredictability Could Affect Adversary Activities

Unpredictability: Make changes frequently and randomly, not just in response to actions by the adversary[19]		
Capability or Approach	**Phase of Cyber Attack Lifecycle**	**Effect on Adversary**
Unpredictable Behavior: Changes are made to reduce an adversary's ability to predict future behavior	Recon, Control	Deter: The adversary is frustrated by uncertainty about possible targets. Delay: The adversary must observe targets over an extended period to gain knowledge of possible attack vectors.
	Weaponize	Impede: The adversary must invest more effort, or try more variations over time, to handle unpredictable implementations or configurations.
	Exploit	Delay: The adversary must make repeated attempts before one succeeds.

[19] Note that Unpredictability is used in conjunction with Dynamic Positioning, Non-Persistence, and Diversity, to enhance the effectiveness of those techniques.