Threat Assessment and Remediation Analysis (TARA)

Jackson Wynn
MITRE Corporation
1 October 2014

Abstract

Threat Assessment and Remediation Analysis (TARA) is an engineering methodology used to identify and assess cyber vulnerabilities and select countermeasures effective at mitigating those vulnerabilities. TARA is part of a MITRE portfolio of systems security engineering (SSE) practices that contribute to achievement of mission assurance (MA) for systems during the acquisition process. The TARA assessment approach can be described as conjoined trade studies, where the first trade identifies and ranks attack vectors based on assessed risk, and the second identifies and selects countermeasures based on assessed utility and cost. Unique aspects of the methodology include use of catalog-stored mitigation mappings that preselect plausible countermeasures for a given range of attack vectors, and use of countermeasure selection strategies that prescribe the application of countermeasures based on level of risk tolerance. This paper outlines the SSE-MA portfolio and describes the TARA methodology.

This technical data was produced for the U.S. Government under Contract No. FA8702-14-C-0001, and is subject to the Rights in Technical Data-Noncommercial Items Clause (DRARS) 252.227-7013 (NOV 1995). The author's affiliation with The MITRE Corporation is provided for identification purposes only, and is not intended to convey or imply MITRE's concurrence with, or support for, the positions, opinions or viewpoints expressed by the author.

1 Introduction

1.1 The SSE-MA Capability Portfolio

MA is the ability of operators to achieve their mission, continue critical processes, and protect people and assets in the face of internal and external attack (both physical and cyber), unforeseen environmental or operational changes, and system malfunctions. SSE-MA is the art of engineering into systems:

1. Capabilities for operators to be aware of different and changing adversarial tactics as well as environmental and system conditions
2. Options and alternatives to accomplish a mission under different circumstances
3. Tools to assess and balance advantages and risks of available response options and alternatives
4. Ability to transition to a selected option while simultaneously continuing the mission [1]

Systems exposed to an adversary are more susceptible to compromise. Security features and capabilities such as firewalls, access control lists, intrusion detection, etc., serve to limit this exposure by surrounding or embedding the system with security perimeter(s). The starting point for mission assurance is to assume that a mid-range or high-end, state-sponsored adversary [2] will possess the skills and resources needed to breach that security perimeter to gain access. The objective is to find ways for the mission to continue despite the presence of the adversary.

Two engineering practices in the SSE-MA portfolio applied in an acquisition program are Crown Jewels Analysis (CJA) [3] and TARA [4][5]. These practices seek to influence programs and promote MA early in the acquisition lifecycle where the cost of change is minimized.

1.1.1 CJA

Crown Jewels Analysis is a process for identifying mission-critical cyber assets, enabling us to focus risk mitigation measures where they will be most effective. CJA offers a methodology to help understand what is most critical—beginning during systems development and continuing through system deployment. Leveraging established techniques including Analytic Hierarchy Process, Failure Modes and Effects Analysis, and Quality Function Deployment with expert input, CJA supports mission decomposition and evaluation of dependencies on operational tasks, system functions, and cyber assets. CJA then includes a Mission Impact Analysis to predict the impact from loss of availability of a given cyber asset. The result is a clear view of the cyber assets most critical to a unit's operational tasks and mission objectives. The interested reader is referred to [3] for additional details on CJA.

1.1.2 TARA

TARA is an engineering methodology used to identify and assess cyber vulnerabilities and select countermeasures effective at mitigating those vulnerabilities. The methodology utilizes a catalog of attack vector and countermeasure data, together with web-based tools used to search and process catalog data.

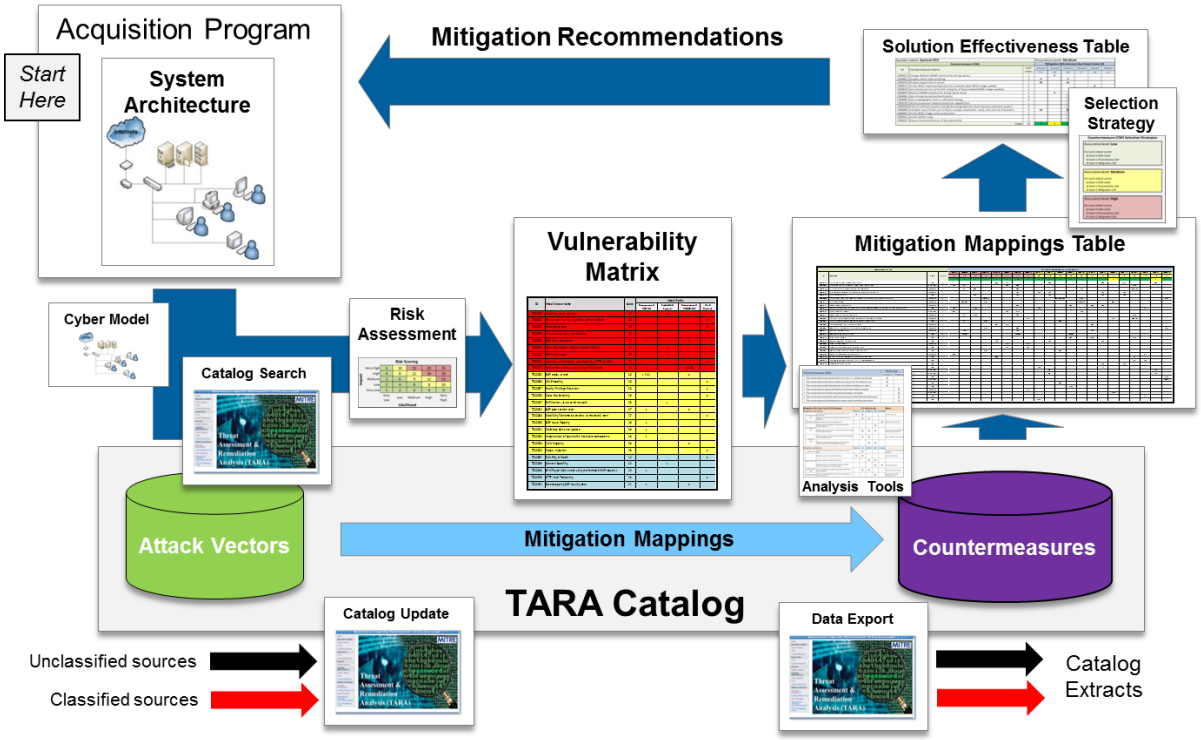

Figure 1 TARA Assessment Workflow

Figure 1 depicts the TARA assessment workflow, which is summarized as follows. System technical details are used to construct a cyber model of the system architecture, which provides a basis for searching the catalog for plausible attack vectors. The list of attack vectors is filtered

and ranked based on assessed risk, producing a vulnerability matrix. The list of vulnerabilities is combined with mitigation mapping data from the catalog to identify an initial list of countermeasures, which is filtered and ranked based on assessed utility and lifecycle cost, producing a mitigation mapping table.

A countermeasure selection strategy is used to select countermeasures that provide a collective response to the range of vulnerabilities based on cost and level of risk tolerance. Mitigation recommendations are conveyed back to the acquisition program using a solution effectiveness table, which lists recommended countermeasures and provides details on the effectiveness of each countermeasure over the range of vulnerabilities assessed. Not reflected in this description are workflows for developing and maintaining catalog data, which are discussed later in this paper.

The methodology can be described as conjoined trade studies, where the first trade identifies and ranks vulnerabilities based on assessed risk, and the second identifies and selects countermeasures based on assessed utility and cost. This paper uses the term mitigate or mitigation in a risk management context to mean reducing the likelihood or severity of attack, and the term prevent or prevention to mean eliminating conditions that made an attack possible or practical.

TARA is similar to other threat modeling and analysis methodologies including MORDA and STRIDE [4]. Unique aspects of the TARA approach include use of catalog-stored mitigation mapping data to preselect plausible countermeasures, and use of countermeasure selection strategies that prescribe the volume of countermeasures based on the level of risk tolerance. These features are discussed later in the paper.

Over a dozen TARA assessments have been conducted since 2011 for a variety of Air Force, Navy, and Army acquisition programs with the objective to influence how systems are designed and implemented. Variations of this methodology have been used to support vulnerability and penetration test planning, program protection planning, and cyber resiliency analysis objectives. This paper describes the TARA methodology.

2 TARA Methodology Overview

2.1 Application of SSE-MA to DoD Acquisition Programs

Figure 2 illustrates application of CJA and TARA by acquisition programs seeking to meet mission assurance goals and objectives or to satisfy applicable DoD Certification and Accreditation (C&A) policies. When applied together, CJA identifies mission critical assets within the system architecture while TARA assesses risk and identifies mitigations to reduce likelihood or impact of a successful attack. The selection of mitigations to reduce risk to mission critical cyber assets or to enhance a system's cyber resilience [6] helps satisfy mission assurance goals and objectives.

DoD acquisition policy may also require programs to perform criticality analysis and/or threat modeling in order to meet Program Protection Planning requirements [7], to satisfy NIST Risk Management Framework (RMF) requirements [8][9][10], or to comply with Security Technical Implementation Guidance (STIG) [11]. This paper contends that CJA and TARA, respectively, are viable approaches to satisfy these requirements.

The figure reflects scenarios in which TARA may be conducted separate from or as a follow-on to CJA. A TARA assessment performed in the absence of mission impact details applies traditional risk models to assess impact in terms of loss of confidentiality, integrity, or availability. A TARA performed as follow on to a CJA produces recommendations that integrate CJA mission impact details. This promotes mission assurance by helping program managers better understand sources of mission risk so that they may make informed choices as to the security posture and resilience of the system being developed.

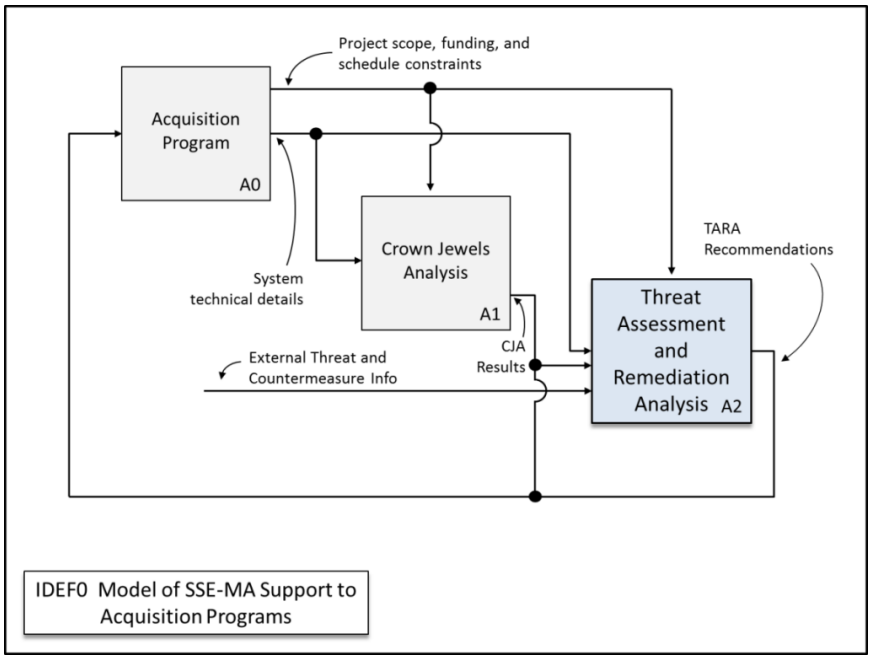

Figure 2 SSE-MA Support to Acquisition Programs

A TARA assessment evaluates system technical details and produces recommendations that influence a system acquisition program by identifying countermeasures that improve security posture, cyber resilience, or prevent or mitigate risk from cyber attack once the system is deployed. The kinds of system technical data reviewed during a TARA assessment will vary with the acquisition program and may include the following:

- Logical and physical architecture,
- Management interfaces,
- External interfaces,
- Mission data stored and processed,
- Mission capabilities,
- Critical program information,
- Security perimeters,
- Security capabilities,
- Operational TTPs,
- Security incident data,
- User roles and permissions, and
- Use of Commercial-Off-the-Shelf (COTS) products

The availability of such technical details will depend on the timeframe in the acquisition lifecycle that TARA is applied and also on the engineering deliverables, documents, etc. put on contract. Operational TTP and security incident data would exist only for fielded systems, for example. The litmus test for useful documentation applies the adversary mindset, i.e., what system details would an adversary find useful if intending to deny, degrade, corrupt, destroy, etc. the ability to use a system or capability.

Additional inputs to TARA include external threat and countermeasure data, which can come from a variety of unclassified and classified sources. Threat data can include adversary tradecraft derived from analysis of attempted penetrations or security incidents. Countermeasure data may include security best practices, NIST security controls, and research publications detailing new security engineering solutions or approaches.

2.2 Conducting a TARA

Figure 3 illustrates the TARA methodology, which is comprised of the following activities:

- Cyber Threat Susceptibility Analysis (CTSA)
- Cyber Risk Remediation Assessment (CRRA)
- Knowledge Management (KM)

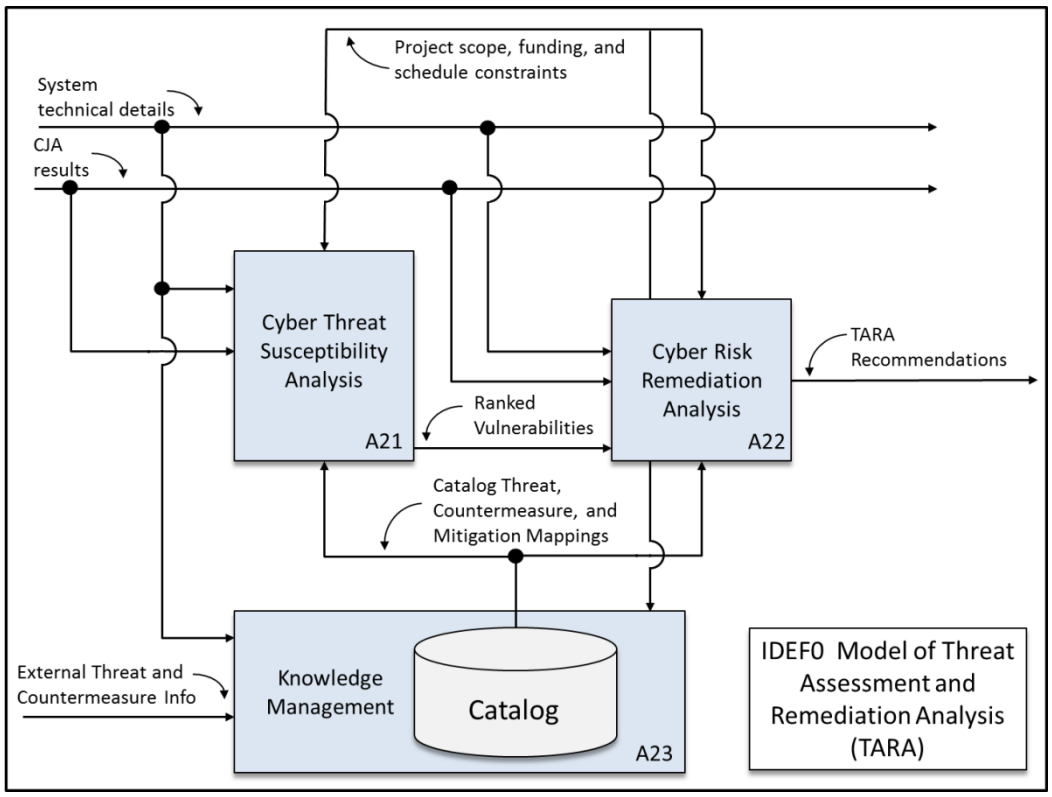

Figure 3 TARA Process

CTSA [12] evaluates system architecture and technology details to identify and select a representative collection of vulnerabilities. CTSA produces a vulnerability matrix that serves as input to CRRA. CRRA evaluates and selects catalog countermeasures to mitigate vulnerabilities from the vulnerability matrix. CRRA delivers TARA recommendations identifying countermeasures that provide an optimized, collective response to the list of vulnerabilities. KM

develops catalog content, ensures that catalog data is internally consistent, and reflects the ever-changing landscape of threat and countermeasure information.

2.2.1 TARA Catalog

The TARA catalog stores attack vectors, countermeasures, and mitigation mapping data used for assessments. An attack vector summarizes the tradecraft or steps performed by an adversary in the course of conducting a cyber attack. The attack vector also characterizes the adversary, potential attack objective(s), and the technologies or system components exploited.

A countermeasure refers to an "action, device, procedure, or technique that opposes or counters a threat, vulnerability or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken" [13]. A catalog countermeasure provides a general description that also characterizes its maturity, cost, and mitigation goal(s).

A mitigation mapping is an association between an attack vector and a countermeasure indicating whether the countermeasure would be effective at opposing or countering the attack vector. Mitigation mappings may be derived from incident response lessons learned, security best practices, modeling and simulation studies, or the judgment of Subject Matter Experts (SMEs).

In the catalog, a mitigation mapping is represented as a 3-tuple: <Countermeasure ID, Attack vector ID, Countermeasure effect>, where the effect is characterized as either preventative or mitigating, depending on when in the cyber attack life cycle [14] or cyber kill chain [15] the countermeasure intercedes. Preventative countermeasures are those that counter or oppose reconnaissance, weaponization, delivery, or exploitation. Mitigating countermeasures are those that take effect after an attack is launched to blunt the scope of the attack, to limit its damage, and/or to facilitate recovery.

Mitigation mappings represent many-to-many relationships between attack vectors and countermeasures, where a given attack vector may be mitigated by any number of countermeasures and a given countermeasure may be effective against any number of attack vectors. This many-to-many relationship is key to assessing the utility of a countermeasure over a select range of attack vectors.

2.2.2 CTSA

CTSA analyzes system technical details to identify a representative set of vulnerabilities based on attack vector data from the catalog. A risk assessment is performed to produce a vulnerability matrix, which serves as input to CRRA. Figure 4 illustrates CTSA, which is comprised of the following sequence of steps:

- Develop a cyber model of the system
- Identify plausible attack vectors
- Perform risk assessment

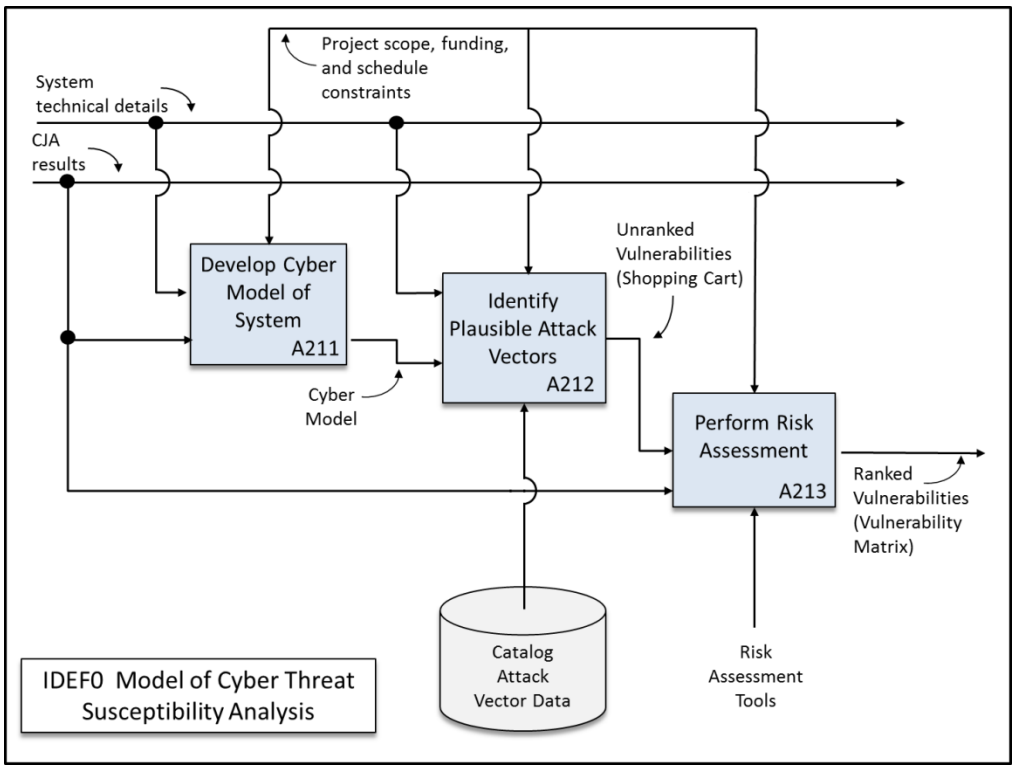

Figure 4 CTSA Process

Develop Cyber Model of System

CTSA starts by developing a cyber model representing the system's attack surface, which is used to identify different ways that an adversary might gain access and compromise a system. The cyber model is based on system technical details and CJA results, and provides the "hooks" used to search the catalog of attack vector data.

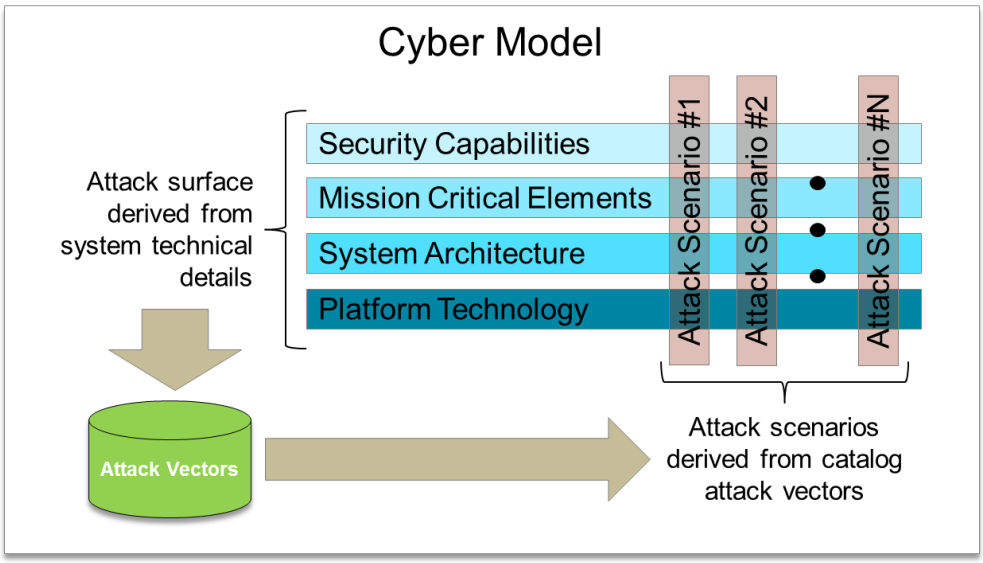

Figure 5 Cyber Model Definition

Figure 5 reflects a system's attack surface that includes architectural features and technologies containing vulnerabilities that can be exploited by an adversary. Mission critical and mission

essential subsystems and components identified by CJA are key elements of a system's attack surface. In keeping with the mission assurance perspective, the cyber model assumes minimal effectiveness of system security features. System security features are viewed as part of the attack surface, being vulnerable to exploitation by high-end, nation state adversaries.

The cyber model reflects a collection of attack scenarios overlaying the attack surface. Each attack scenario provides a narrative description of a cyber attack that characterizes the adversary, the attack objective, the mission timeframe, the attack surface element(s) targeted, and the tradecraft used.

In an attack scenario the adversary may correspond to a mid-level or high-end, nation state actor with varying degrees of sophistication and resources, or to an insider operating with varying permissions and authorities. The attack objective may be generic, i.e., to compromise the availability, integrity, or confidentiality of a system, or mission focused, i.e., the impact from compromise of a mission critical system leading to mission failure or loss of mission readiness. Mission timeframe may be relative to some system operational or mission event.

Using catalog data, tradecraft that may initially provide only a generalized description of adversary activities can be developed into detailed descriptions of specific adversary Tactics, Techniques, and Procedures (TTPs). General descriptions of the attack surface provide context for searching the catalog for specific adversary techniques, e.g., SQL injection, buffer overflow, etc., that an adversary might use to achieve its objective. The more detailed the tradecraft description, the easier the task of assessing the effectiveness of potential countermeasures.

Identify Plausible Attack Vectors

The initial catalog search identifies a range of attack vectors based on aspects of the system attack surface. The resulting unordered list of attack vectors is collected into shopping carts, one shopping cart for each attack surface feature being evaluated.

A shopping cart is a temporary catalog structure used to collect attack vectors. Several shopping carts may be created for an assessment, each representing a different facet of the attack surface and each filled with dozens of attack vectors. Not all will be reflected in attack scenarios. As the assessment progresses shopping carts are culled to eliminate attack vectors deemed implausible or duplicative.

The catalog provides tools to search catalog data and to create and manage shopping carts. Catalog search capabilities include keyword search as well as search filters over a range of fields. Shopping cart management includes capabilities to add and delete shopping carts and to add and remove attack vectors in shopping carts.

Perform Risk Assessment

Attack vectors in the shopping cart are scored and ranked using a risk-scoring model. TARA doesn't prescribe use of a particular risk-scoring model, and has applied both standard risk cubes and weighted risk scoring in past assessments. Risk cubes [16] qualitatively assess risk relative to likelihood and impact. Weighted risk scoring quantitatively assesses risk over a range of potential risk factors. Either approach can be tailored to reflect mission impact provided by a CJA.

Risk scores provide an effective means for ranking attack vectors, which is a first step towards performing triage. Depending on schedule and funding constraints, triage may be needed to identify lower risk attack vectors that can be deferred to a follow-on assessment or accepted as

residual risk. Figure 6 depicts a vulnerability matrix containing a ranked list of vulnerabilities. If multiple shopping carts are used, separate columns can be added to the matrix to reflect the allocation of vulnerabilities across shopping carts.

Attack Vector			Shopping Carts		
ID	Name	Risk Score	Mission	Management	Physical
T000016	Simple Script Injection	2.6	X	X	
T000024	Malicious Software Update	2.4	X	X	
T000100	Forceful Browsing	2.3	X		
T000181	Malicious software implantation through 3rd party bundling	2.3	X	X	
T000008	Unsecured SNMP agent	2.1		X	
T000096	Poison Web Service Registry	2.1	X		
T000107	XSS attack on router web interface	2.1		X	
T000129	Directory traversal to access router configuration data	2.1		X	
T000163	Implantation of counterfeit hardware components	2.1			X
T000077	SOAP Parameter Tampering	2.0	X	X	
T000026	Accessing Functionality Not Properly Constrained by ACLs	1.9	X		
T000046	Device DoS using crafted SNMP messages	1.9		X	
T000122	Adversary intercepts hardware in distribution channel	1.8			X
T000121	Compromise design and/or fabrication of hardware components	1.5			X
T000123	Man in the Middle (MITM) Supply Chain	1.3			X

Figure 6 Vulnerability Matrix

2.2.3 CRRA

CRRA evaluates, ranks, and selects catalog countermeasures based on mitigation mapping data that associates catalog countermeasures with vulnerabilities listed in the vulnerability matrix. CRRA delivers TARA recommendations identifying countermeasures that provide collective response to a given list of vulnerabilities. Figure 7 illustrates the CRRA activity, which is comprised of the following sequence of steps:

- Identify plausible mitigations
- Assess mitigation utility and cost
- Perform mitigation selection

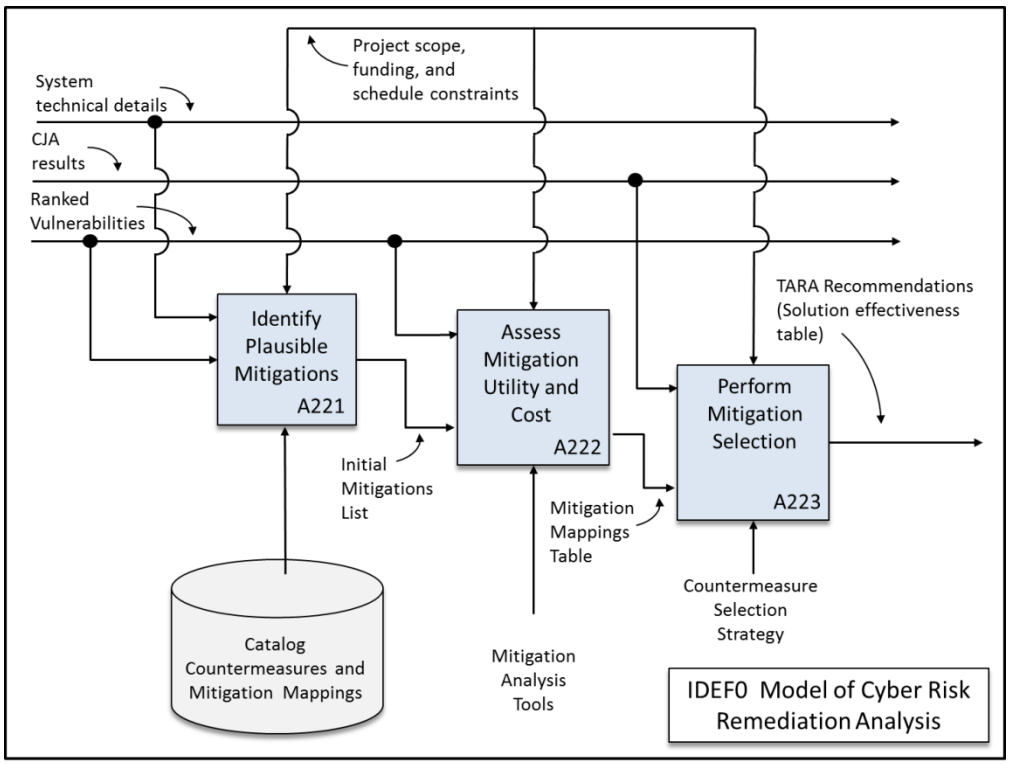

Figure 7 CRRA Process

Identify Plausible Mitigations

Vulnerabilities from the vulnerability matrix together with mitigation mapping data from the catalog are used to identify an initial, unordered list of countermeasures. As with shopping carts, this initial set may be large and must be filtered to eliminate implausible or duplicative countermeasures.

A countermeasure may be deemed implausible for a variety of reasons including lifecycle stage, applicability, maturity, or cost. One reason might be that the countermeasure is implemented at an earlier stage in the system development lifecycle. A countermeasure that prescribes use of a programming language to minimize software defects, e.g., Java, C++, etc., wouldn't be actionable for a program engaged in verification testing, for example.

Assess Mitigation Utility and Cost

A TARA assessment computes a score for each countermeasure, which is used to rank countermeasures in the mitigation mappings table prior to countermeasure selection.

Countermeasures			Mitigation Mappings (by Attack Vector ID)					
ID	Name	LCC Estimate	T000016	T000024	T000100	T000181	T000008	T000096
C000169	Do not follow unsolicited hyperlinks	Very Low	P					
C000132	Use sandboxing to isolate running software	Medium	P	M		M		
C000117	Apply principle of least privilege	Low	M	M	M			P
C000168	Utilize checksums to detect unauthorized modifications to files	Medium		P				M
C000010	Restrict physical access to device	Low		P			M	
C000022	Isolate network management traffic to internal network	Medium					M	
C000051	Use digital signatures/checksums to authenticate source of changes	Medium		M				M
C000152	Conduct penetration testing	Medium	P		P		P	P
C000105	Apply static code analysis tools to identify software defects	Medium			P	P		

Figure 8 Unscored Mitigation Mapping Table

Figure 8 depicts the mitigation mapping table for the top six vulnerabilities from the matrix in Figure 6. Rows in the table correspond to catalog countermeasures, while table columns correspond to attack vectors from the vulnerability matrix. Table cells convey the mitigation effects that countermeasures have on attack vectors, either preventative or mitigating. An empty cell signifies no mitigation effect for an attack vector.

A utility-to-cost (U/C) ratio is calculated for each countermeasure. Utility refers to the overall effectiveness of a countermeasure over a range of attack vectors. A countermeasure that is mapped to 5 attack vectors has greater utility than a countermeasure that is mapped to 2 attack vectors, for example. The utility score is calculated for each countermeasure as a weighted sum of preventative and mitigating mappings, where weightings can be assigned that increase the relative value of preventative or mitigating countermeasures.

Using a 3:2 weighting scheme that favors preventative over mitigating effects, the utility score of countermeasure C000168 in the table above is 3 + 2 = 5 while the utility score for countermeasure C000051 is 2 + 2 = 4. Both countermeasures are effective against the same two attack vectors. However C000168 provides a preventative effect, which has a higher weighting in this example. Using a 1:1 weighting scheme these two countermeasures would have the same utility score.

The mitigation mapping table includes an estimate for the Life Cycle Cost (LCC) of each countermeasure over the discrete range [very low, low, medium, high, and very high]. The LCC estimate reflects the cost of ownership of a countermeasure when there is insufficient information to arrive at a dollar cost estimate. The LCC Estimator tool depicted in Table 8 is used to develop LCC cost estimates based on a range of life cycle costs drivers.

Mitigation Life Cycle Cost (LCC) Estimator			LCC tends to be….					Notes
Acquisition cost factors			Very Low	Low	Medium	High	Very High	
1	Procurement cost	Commodity mitigation widely used and supported by mature industrial base	X	X				Commodity pricing
2		Mitigation makes use of commercially developed products and capabilities		X	X			
3	Research cost	Mitigation applies latest, cutting-edge research				X	X	Capability maturity issues
4	Development cost	Mitigation requires development of specialized hardware or software capabilities				X		
5		Mitigation has limited shelf life, i.e., effectiveness diminishes quickly or technology obsolescence		X	X			Low cost example: A/V signature updates replaced monthly
6	Integration cost	Mitigation supports a standardized interface to facilitate integration into existing infrastructure		X	X			Drop in capability, loose coupling
7		Mitigation requires extensive changes to current hardware or software baseline, standard operating procedures, etc.			X	X		
Utilization cost factors			Very Low	Low	Medium	High	Very High	
8	Training cost	Mitigation requires periodic or extensive training to operate or apply		X				Training costs are not cost drivers generally
9	Operating cost	Mitigation requires a minimal staff to operate	X	X				automated capabilities
10		Mitigation requires a sizeable staff to operate			X	X		
11		Mitigation requires use of specialized or custom developed capabilities, facilities, etc. to install or operate				X	X	Outsourced services?
12	Maintenance cost	To remain effective the mitigation requires periodic hardware or software upgrades		X	X			Depends on hardware MTBF
13	Disposal cost	Disposal requires disassembly of components containing toxic or hazardous substances				X		Example: AT "energetic" countermeasures

Figure 9 LCC Estimator

Before U/C ratios can be calculated, LCC estimates in the range [very low, low, medium, high, and very high] must be converted to a numeric scale. Conversion can be to a linear scale [1…5] or to an exponential scale [1,2,4,8,16] to institute a bias favoring lower cost countermeasures. Figure 10 applies a 3:2 utility bias and a linear cost scale to calculate U/C scores for the mitigation mapping table in Figure 8.

Countermeasures			Scoring				Mitigation Mappings (by Attack Vector ID)					
ID	Name	LCC Estimate	Utility	Cost	U/C Ratio	Rank	T000016	T000024	T000100	T000181	T000008	T000096
C000117	Apply principle of least privilege	Low	9	2	4.5	1	M	M	M			P
C000152	Conduct penetration testing	Medium	12	3	4.0	2	P		P		P	P
C000169	Do not follow unsolicited hyperlinks	Very Low	3	1	3.0	3	P					
C000010	Restrict physical access to device	Low	5	2	2.5	4		P			M	
C000132	Use sandboxing to isolate running software	Medium	7	3	2.3	5	P	M		M		
C000105	Apply static code analysis tools to identify software defects	Medium	6	3	2.0	6			P	P		
C000168	Utilize checksums to detect unauthorized modifications to files	Medium	5	3	1.7	7		P				M
C000051	Use digital signatures/checksums to authenticate source of changes	Medium	4	3	1.3	8		M				M
C000022	Isolate network management traffic to internal network	Medium	2	3	0.7	9					M	

Figure 10 Scored and Ranked Mitigation Mapping Table

Perform Countermeasure Selection

A countermeasure selection strategy is used to select a set of countermeasures that provide collective response for the range of vulnerabilities identified in the vulnerability matrix. A solution effectiveness table is prepared to identify the selected countermeasures together with mitigation mapping details that establish traceability between the selected countermeasures and the vulnerabilities they resolve. This table is used to develop TARA recommendations.

The countermeasure selection strategy defines the minimum number and type of countermeasures required for each attack vector in the mitigation mapping table. For example, a medium assurance countermeasure selection strategy might require at least 3 countermeasures for each attack vector, including at least one preventative and one mitigating countermeasure, while a high assurance strategy might require at least 5 countermeasures for each attack vector, including at least 2 preventative and 2 mitigating.

The program's level of risk tolerance informs the selection of the minimum number of countermeasures required by the countermeasure selection strategy. These minimums relate directly to the defense in depth strategy being applied, where the more countermeasures applied to a given attack vector the less likely that attack would be successfully executed.

Two important considerations for the countermeasure selection strategy include the balance between preventative and mitigating countermeasures and the cumulative LCC cost to maintain or operate the countermeasures over the life of the system. Having an imbalance of preventative and mitigating countermeasures provides for a lopsided security posture. In a mission assurance context keeping the adversary out is as important as having the capacity to respond to adversaries, even with the assumption that they will eventually get in.

The second objective is for the selection strategy to balance the level of protection with the level of risk tolerance required for the system. Under engineering a security solution not to include sufficient countermeasures to satisfy the selection strategy results in one or more coverage gaps. These are highlighted in the solution effectiveness table. Conversely, over engineering a security solution to include more countermeasures than needed can drive operational and maintenance costs over a system's operational lifetime.

In the example that follows, a selection strategy requiring a minimum of 3 countermeasures with at least 1 preventative and 1 mitigation countermeasure for each attack vector is applied to the mitigation mapping table in Figure 10 to produce the solution effectiveness table in Figure 11. Alternative countermeasure selection strategies would set these minimums, or possibly apply higher minimums to higher risk attack vectors. Methodology tailoring choices are considered in section 3.

Countermeasures			Scoring				Mitigation Mappings (by Attack Vector ID)					
ID	Name	LCC Estimate	Utility	Cost	U/C Ratio	Rank	T000016	T000024	T000100	T000181	T000008	T000096
C000117	Apply principle of least privilege	Low	9	2	4.5	1	M	M	M			P
C000152	Conduct penetration testing	Medium	12	3	4.0	2	P		P		P	P
C000010	Restrict physical access to device	Low	5	2	2.5	4		P			M	
C000132	Use sandboxing to isolate running software	Medium	7	3	2.3	5	P	M		M		
C000105	Apply static code analysis tools to identify software defects	Medium	6	3	2.0	6			P	P		
C000168	Utilize checksums to detect unauthorized modifications to files	Medium	5	3	1.7	7		P				M
C000022	Isolate network management traffic to internal network	Medium	2	3	0.7	9					M	
		Total Utility and Cost	46	19		Total Ps	2	2	2	1	1	2
						Total Ms	1	2	1	1	2	1
						Total Mitigations	3	4	3	2	3	3

Figure 11 Solution Effectiveness Table

The solution effectiveness table is derived from the mitigation mapping table by omitting unselected countermeasures and by adding cumulative utility and cost scores and preventative and mitigation countermeasure totals. Coverage gaps are highlighted in yellow to indicate where the selection strategy is not fully satisfied.

In the Figure 11 example, countermeasures C000169 and C000051 are omitted and total utility (46) and cost (19) scores are added. A coverage gap is identified for attack vector T000181 for failing to satisfy the selection strategy minimum of 3 countermeasures per attack vector. When a coverage gap occurs during a TARA assessment, the object is to identify additional countermeasure(s) in the catalog to eliminate that gap.

Coverage gaps, cumulative utility and cost scores provide a quantitative basis for comparing alternative solutions. Different selection approaches may produce alternative solution sets. Sensitivity analysis conducted to evaluate alternative solution sets would use these measures to assess and compare results.

TARA recommendations to an acquisition program summarize the countermeasures selected and their effects over the range of vulnerabilities assessed. If CJA results are available, then the mission impact attributed to each vulnerability is used to develop compelling justification for implementing each recommendation.

2.3 KM

KM develops catalog content. KM also ensures that catalog attack vector, countermeasure, and mitigation mapping data are internally consistent and reflect the ever-changing landscape of threat and countermeasure information. Figure 12 illustrates the KM activity, which is comprised of the following sequence of steps:

- Prioritize information needs
- Identify and evaluate external data sources
- Update catalog data

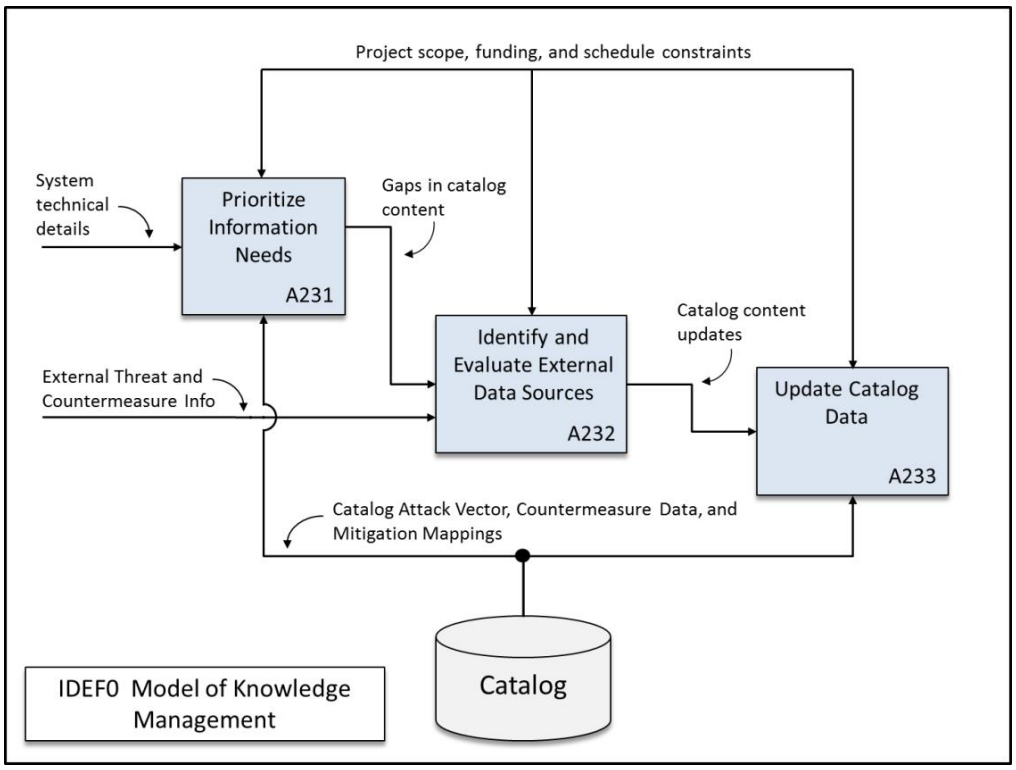

Figure 12 KM Process

Prioritize Information Needs

System technical details are used to identify areas in the catalog where additional attack vectors and countermeasures are required. These knowledge gaps surface when a TARA assessment is scoped to include never-previously-seen systems or technologies. Knowledge management is used to fill these gaps when they occur.

Identify and Evaluate External Data Sources

Known sources of cyber threat information are evaluated to identify attack vectors and countermeasures to add to the catalog. New sources of cyber threat information are also discovered and validated. Examples of external, open source cyber threat data that are routinely consulted include MITRE CAPEC [17] and CVE [18]. A separate catalog containing classified cyber threat data is maintained based on classified data sources.

Update Catalog Data

Attack vector and countermeasure data is added to the catalog to fill identified knowledge gaps. Existing catalog content is updated to reflect additional details. Attack vectors and countermeasures are rarely removed from the catalog except when duplicates are found.

Mitigation mappings often need to be added for an assessment when a coverage gap is identified. Figure 13 depicts a Countermeasure Effects Estimator, which can be used to support this analysis. Mitigation mappings developed for one assessment are incorporated into the catalog where they can be reused in subsequent assessments.

ID	Countermeasure Effect	*Tends to be…*	
		Preventative	Mitigating
1	*The countermeasure disrupts the attack's sequence of activities*	X	
2	*The countermeasure eliminates condition(s) necessary for the attack to occur*	X	
3	*The countermeasure facilitates detection of conditions leading to an attack*	X	
4	*The countermeasure reduces the likelihood of the attack being successful*		X
5	*The countermeasure minimizes the extent of damage or disruption*		X
6	*The countermeasure facilitates rapid recovery/reconstitution after the attack occurs*		X
7	*The countermeasure facilitates forensic analysis and/or attribution following an attack*		X

Figure 13 Countermeasure Effects Estimator

3 Tailoring the Methodology

Tailoring refers to adaptation of an organization process or standard to meet the needs of a project [19]. Aspects of the TARA methodology can be tailored to better align the process with program or sponsor needs. Variations of the methodology have been developed to support specific applications within a systems acquisition context.

TARA provides a flexible framework that can be modified or replaced in order to align the methodology with sponsor needs. For CTSA, aspects of the cyber model can be revised to focus on specific features of the system attack surface. Programs may replace attack scenarios with attack trees, for example, in order to represent more specific or detailed adversary tradecraft. Alternative risk scoring approaches, alternative risk factors or risk weighting schemes can also be applied.

For CRRA, a program can tailor the methodology to select the utility scoring and/or cost-scoring model used to rank countermeasures. Alternative countermeasure selection strategies can be applied to apply a more reactive or proactive defense in depth strategy. The countermeasure selection strategy can provide a means to fine tune the level of risk tolerance being applied in which the minimum number of countermeasure can be indexed to the level of risk associated with an attack vector.

Variations of the TARA methodology have been developed for specific Systems Security Engineering (SSE) uses. One variation of the methodology has been to focus on CAPEC and CVE-derived attack vectors and deliver artifacts conforming to DoD guidelines for Program Protection Planning (PPP). Another has been to use TARA analysis to plan vulnerability and penetration test plan objectives. TARA has also been applied in conjunction with cyber red team analysis to identify systemic vulnerabilities, and assesses NIST 800-53 IA controls supporting resilience as potential countermeasures.

4 Areas for Further Research

4.1 Metrics for Measuring Influence

The objective of TARA is to deliver recommendations that influence programs early in the acquisition lifecycle where the cost of change is minimized. However recommendations developed in the early phases of a system acquisition through TARA may not be acted upon for

months or even years after the assessment has been completed, making it difficult to assess what concrete impact an assessment provides.

Better metrics are needed to establish the value TARA provides to programs. Changes in a program's system security engineering approach, schedule, budget, etc. may occur of a variety of reasons, least of which may be TARA assessment results. Metrics such as the number of recommendations provided or the range of attack vectors and countermeasures analyzed do not adequately assess the extent to which TARA influences the course of an acquisition program or the security architecture being developed.

While direct measures of influence remain elusive, indirect measures include program requests for follow-on assessments, requests for TARA training and/or requests for access to TARA catalog data. Program requests for TARA training, especially training for support contractors, signify interest in applying a systematic methodology for assessing and mitigating cyber risk. In this case, the measure reflects how application of TARA has influenced the sponsor, regardless of what effect the recommendations may someday have on the direction of the program.

4.2 Assessing Countermeasure Effects

This paper only considers mitigation mappings that have preventative or mitigating effects based on when they are effective in the cyber attack lifecycle. This gross simplification is consistent with application of TARA in cyber risk management applications.

Countermeasure effect is the basis for assessing the utility and rank of a countermeasure. A countermeasure that effects 5 attack vectors has greater utility than a countermeasure that effects 2 countermeasure, all other factors being equal. There is no assumption or requirement that all countermeasures that effect a given attack vector are equally effective. A given countermeasure may have a preventative effect on one attack vector and a mitigating effect on another.

The characterization of countermeasure effect is an evolving research topic. A countermeasure effect is minimally represented as a binary state, i.e., the countermeasure is effective or it is not. TARA originally represented countermeasure effects in terms of both type of effect, i.e., detect, neutralize, limit, recover, and magnitude [low, medium, high], producing 4 x 3 = 12 possible effects. In [20] a vocabulary is developed to express countermeasure effects and identifies 13 possible effects, i.e., deter, divert, deceive, expunge, etc. over the 6-step, cyber attack lifecycle. Simplifying this provided clarity for the paper. However tailoring can be used to develop and apply a more sophisticated cyber effects model for use with TARA.

Different source of countermeasure effects have various strengths and weaknesses. However no source is irrefutable. Countermeasure effects can be derived from security best practices, incident response lessons learned, modeling and simulation studies, or the judgment of SMEs. Establishing consensus on what qualifies as a security best practice is often difficult to achieve. Countermeasure effects derived from modeling and simulation depend on validation of the underlying security model.

Further research is needed to explore use of incident response data derived in an operational context [21] to inform acquisition programs, and to define a competency model for security SMEs. With respect to mitigation mappings, engineering verification through inspection, demonstration, or testing cannot readily substantiate the effect that a countermeasure has for an attack scenario, especially for systems in development.

5 References

[1] MITRE, “Systems Engineering Guide (SEG)”, ISBN 978-0-615-97442-2, The MITRE Corporation, 2014. [Online] Available: http://www.mitre.org/publications/technical-papers/the-mitre-systems-engineering-guide

[2] H. Goldman, J. Woodward, “Defending Against Advanced Cyber Threats,” The MITRE Corporation, 2008.

[3] MITRE SEG, p167.

[4] J. Wynn, J. Whitmore, G. Upton, L. Spriggs, D. McKinnon, R. McInnes, R. Graubart, L. Clausen, “Threat Assessment and Remediation Analysis (TARA) Methodology Description, version 1.0, MITRE Technical Report, MTR110176, October 2011. [Online] Available: http://www.mitre.org/sites/default/files/pdf/11_4982.pdf

[5] MITRE SEG, p175.

[6] Bodeau, D., Graubart, R., “Cyber Resiliency Engineering Framework,” MTR110237, MITRE Corporation, September 2011. [Online] Available: http://www.mitre.org/sites/default/files/pdf/11_4436.pdf

[7] DoDI 5200.44, “Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)”, DoD CIO/USD(AT&L), November 2012.

[8] National Institute of Science and Technology, “Guide for Applying the Risk Management Framework to Federal Information Systems,” NIST SP 800-37, Revision 1, U.S. Dept. of Commerce, 2010.

[9] National Institute of Science and Technology, “Security and Privacy Controls for Federal Information Systems and Organizations,” NIST SP 800-53, Revision 4, U.S. Dept. of Commerce, 2013.

[10] Committee on National Security Systems, “Security Categorization and Control Selection for National Security Systems,” CNSS Instruction 1253, March 2014.

[11] DISA, “Application Security and Development Security Technical Implementation Guide (ASD STIG), Version 3, Release 5, July 2013.

[12] J. Wynn, L. Montella, “Cyber Threat Susceptibility Analysis,” MITRE Technical Report, MTR100379, 2010.

[13] Committee on National Security Systems, “National Information Assurance (IA) Glossary,” CNSS Instruction 4009, April 2010.

[14] MITRE, "Threat-based Defense.” [Online]. Available: http://www.mitre.org/capabilities/cybersecurity/threat-based-defense

[15] E. Hutchins, M. Cloppert, R. Amin, “Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains,” Lockheed Martin, 2009.

[16] National Institute of Science and Technology, “Guide for Conducting Risk Assessments,” NIST SP 800-30, Revision 1, U.S. Dept. of Commerce, 2012.

[17] MITRE, Common Attack Pattern Enumeration and Classification (CAPEC) [Online] Available: http://capec.mitre.org/.

[18] MITRE, Common Vulnerabilities and Exposures (CVE) [Online] Available: http://cve.mitre.org/

[19] International Council of Systems Engineering, "Systems Engineering Handbook," version 3.2.2, INCOSE-TP-2003-002-03.2.2, 2011.

[20] Bodeau, D., Graubart, R., "Characterizing Effects on the Cyber Adversary," MTR130432, MITRE Corporation, November 2013. [Online]
Available: http://www.mitre.org/sites/default/files/publications/characterizing-effects-cyber-adversary-13-4173.pdf

[21] Barnum, S. "Standard Cyber Threat Intelligence Information with the Structured Threat Information eXpression (STIX)", Version 1.1, Revision 1, MITRE Corporation, February 2014. [Online] Available: https://stix.mitre.org/about/documents/STIX_Whitepaper_v1.1.pdf