Cyber Risk Assessment in Distributed Information Systems

Dr. Kamal Jabbour
Major Jenny Poisson

ABSTRACT

This paper presents a disciplined approach to cyber risk assessment in distributed information systems. It emphasizes cyber vulnerability assessment in the architecture, specification and implementation—the knowledge of us—as a vital first step in estimating the consequence of information compromise in critical national security systems. A systematic methodology that combines information flow analysis and Byzantine failure analysis allows assessing the effects of information integrity compromises and the development of a Blue Book to guide cooperative Blue Team testing. The analysis of system vulnerability extends to cyber threats—the knowledge of them—leading to the development of a Red Book to inform adversarial Red Team testing. The paper concludes with a notional case study that illustrates this approach.

1. INTRODUCTION

1.1 Risk

In 2002, the National Institute of Standards and Technology (NIST) defined risk to information systems as "a function of the likelihood of a given threat-source exercising a particular potential vulnerability, and the resulting impact of that adverse event" and a threat as "the potential for a particular threat-source to successfully exercise a particular vulnerability." [1] Although the 2012 Guide for Conducting Risk Assessments [2] that superseded the 2002 document redefined risk as "a measure of the extent to which an entity is threatened by a potential circumstance or event, and is typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence," we like the simplicity of breaking risk into three fundamental components: vulnerability, threat and impact.

In complex distributed information systems, such as an aircraft, satellite or an air

Dr. Kamal T. Jabbour, a member of the scientific and technical cadre of senior executives, is Senior Scientist for Information Assurance, Information Directorate, Air Force Research Laboratory, in Rome, New York. He serves as the principal scientific authority and independent researcher in the field of information assurance, including defensive information warfare and offensive information warfare technology. He conceives, plans, and advocates major research and development activities, monitors and guides the quality of scientific and technical resources, and provides expert technical consultation to other Air Force organizations, Department of Defense and government agencies, universities and industry. Dr. Jabbour is an avid distance runner who has run marathons in all 50 states.

operations center, Cyber Vulnerability Assessment (CVA) focuses on identifying architectural features, specification requirements, and implementation artifacts that form an attack surface that a threat adequately resourced in time, talent and treasure can exploit. While a thorough CVA requires an understanding of threat capabilities, a CVA remains essentially an exercise in the knowledge of us.

NIST characterizes a threat source as "the intent and method targeted at the exploitation of a vulnerability." In our cyber risk assessments, we assume intent and we focus on understanding and quantifying the threat capability necessary to exploit a known vulnerability. As such, threat and vulnerability go hand in hand—there is no threat where there is no vulnerability. Granted, we must treat both threat and vulnerability as probabilities, rather than binary zeroes or ones. We analyze a system for vulnerabilities, and we estimate the probability of a threat exploiting each vulnerability, where characterizing the threat requires understanding adversary capability in terms of time, talent and treasure—the knowledge of them, as well as access means—remote, physical and supply chain.

A successful threat exploitation of an information system vulnerability provides the mission owner or commander the third component in the risk calculus, impact, and permits risk management decisions. The risk calculus consists of a vulnerability—which the mission commander owns—a threat capability necessary to exploit the vulnerability—which the adversary owns—and the impact of a successful threat exploitation of the vulnerability—which we measure in terms of disruption, degradation, denial, destruction or deception. In this paper, we use interchangeably the terms impact, effect and consequence based on the context.

Major Jenny M. Poisson is an Executive Staff Officer for the Secretary of the Air Force (SecAF) and Program Manager for SecAF Advisory Board Studies, Air Force Scientific Advisory Board, Pentagon, Washington, D.C. She is responsible for conducting studies on topics deemed critical to the Air Force mission and recommends applications of technologies that can improve Air Force capabilities. Major Poisson also serves as Individual Mobilization Augmentee (IMA), to the Air Force Senior Scientist for Information Assurance, Air Force Research Laboratory Information Directorate, in Rome, NY. In this role, she assists and advises the Senior Scientist in conceiving, planning and advocating for major research and development activities. Major Poisson leads a Total Force Blue team to act as trusted agents and honest brokers to the USAF on cyber vulnerability assessment of weapons and missions. In the process, the team identifies areas for Science & Technology insertion in both the test process and vulnerability mitigation, and informs the development of future systems.

1.2 Information Assurance

Joint Publication 1-02, Department of Defense (DoD) Dictionary of Military and Associated Terms, [3] defines information assurance (IA) as the "actions that protect and defend information systems by ensuring availability, integrity, authentication, confidentiality and nonrepudiation." We differentiate between the actions that apply to information—confidentiality, integrity and availability—and those that deal with users and processes—authentication and nonrepudiation.

Information assurance professionals recognize the first three goals of confidentiality, integrity and availability as the tenets of information assurance. In assessing the cyber risks to distributed information systems, we examine the impact of compromises in the confidentiality, integrity and timely availability of information critical to a mission, regardless of the means by which such compromises occur. This approach permits us to separate vulnerability and impact—the *what*—from threat—the *how*.

1.3 Mission Assurance

DoD Directive 3020.40 defines Mission Assurance (MA) as "a process to ensure that assigned tasks or duties can be performed in accordance with the intended purpose or plan. It is a summation of the activities and measures taken to ensure that required capabilities and all supporting infrastructures are available to the DoD to carry out the National Military Strategy." [4]

In accordance with this directive, the primary responsibility of a commander is to ensure the timely execution of his mission, while assuming a risk commensurate with mission vulnerabilities and the impact of a successful exploitation by a capable threat.

According to Air Force Doctrine Document 3-12 on Cyberspace Operations, "mission assurance entails prioritizing mission essential functions (MEFs), mapping mission dependence on cyberspace, identifying vulnerabilities,and mitigating risk of known vulnerabilities." [5]

Design specification documents provide a list of MEFs that constitute a mission. Prioritizing these MEFs rests with the mission owner, and depends on the operational environment for the mission, steady-state versus contingency, peacetime versus war, or escalation versus restoration.

Mapping mission dependence on cyberspace requires a detailed understanding of the mission. DoD Architectural Framework (DoDAF) Operational Views (OV) and Systems Views (SV) [6] provide good starting points for mapping mission dependence on cyberspace. A fractal approach to mission mapping permits increasing the fidelity and resolution of mapping a priority MEF at the expense of lower priority MEF with lesser mission impact.

Identifying cyber vulnerabilities requires an intimate knowledge of the architecture, specification and implementation of the priorityMEF. First, architecture vulnerabilities result often from the overlap among safety, reliability and security requirements. While reliability requires *at least* this much functionality, security demands *at most* this much functionality, with the potential for excess functionality turning into vulnerability. Second, specification vulnerabilities resulting from policy mandates and protocol choices may increase the risk to an MEF. Third, implementation vulnerabilities, including hardware, software and configuration, open the aperture of vulnerability assessment to supply-chain and user considerations.

Information assurance professionals recognize the first three goals of confidentiality, integrity and availability as the tenets of information assurance.

The final tenet of mission assurance, vulnerability mitigation, follows a three-pronged approach. First, Tactics, Techniques and Procedures (TTP) may suffice to mitigate certain implementation vulnerabilities. However, materiel solutions are often necessary to mitigate architecture and specification vulnerabilities. Where TTP fall short and materiel solutions do not exist, pursuing advanced Science and Technology (S&T) becomes necessary to create adequate mitigations that reduce the vulnerability and the likelihood of threat exploitation, increase the cost of a successful exploitation and reduce its adverse impact on the mission.

1.4 Testing

Cradle to grave mission assurance requires conducting outcomes-based Test and Eval-

uation (T&E) in a realistic threat environment, early and often in the acquisition lifecycle. T&E must include cyber threats that represent current and projected adversary capabilities. Developmental Test and Evaluation (DT&E) during pre-systems acquisition and Operational Test and Evaluation (OT&E) during acquisition and sustainment play vital roles in mission assurance. The earlier a test discovers cyber vulnerability, the lower is the cost of mitigating such vulnerability.

DoD Directives 5000.01 [7] and 5000.02 [8] provide the principles and policies governing T&E and identify the flow of T&E activities within the acquisition lifecycle. According to Defense Acquisition University, DT&E seeks to identify technical capabilities and limitations, stresses the system to ensure robust design, and assesses performance under a number of environmental parameters such as adverse weather, while OT&E seeks to evaluate the operational effectiveness and suitability of a system operating under realistic combat conditions. [9]

Cyber testing leverages the first three steps of mission assurance: prioritizing MEF, mapping MEF dependence on cyber, and identifying architecture/specification/implementation vulnerabilities. Both DT&E and OT&E must take the cyber environment into consideration as both an environmental parameter and as a hostile combat condition. While DT&E may limit its focus to the cyber vulnerabilities in a system and the potential impact of their exploitation, OT&E must examine the capabilities necessary to exploit these vulnerabilities in a manner that creates an adverse impact to the mission of the system.

It is imperative that cyber testing remain outcomes-based, and focus on the impact of a successful threat exploitation of a vulnerability in the architecture, specification or implementation of a mission, rather than compliance-based with a checklist of IA controls. We differentiate between cyber testing—testing a mission or system in a realistic cyber threat environment—from cybersecurity testing—testing for compliance with an arbitrary list of IA controls that are neither necessary nor sufficient for mission assurance.

Identifying cyber vulnerabilities requires an intimate knowledge of the architecture, specification and implementation of the priority MEF.

1.5 Paper Overview

In the following sections, we present a systematic top-down approach to identifying potential cyber vulnerabilities in a complex information system through a disciplined information flow analysis, and estimating the mission impacts of information compromise. We apply Byzantine failure analysis to separate the impact of an information compromise

from the underlying cause of the compromise, whether accidental or malicious. We advocate generating a Blue Book of cyber vulnerabilities at the end of this vulnerability assessment phase to guide the cooperative test activities by a Blue Team.

While a Blue Book of cyber vulnerabilities provides an introspective look at the engineering of the system under test, the subsequent development of a Red Book seeks to quantify the adversary capabilities necessary to exploit the cyber vulnerabilities that the Blue Book identifies. The Red Book provides Red Teams with a roadmap to conduct adversarial testing by a Red Team, and defines the threat capabilities that an aggressor team seeks to understand, replicate and exercise.

We complete our discussion of mission assurance by addressing vulnerability mitigation. We explore first Tactics, Techniques and Procedures (TTP) where applicable, then discuss materiel solutions when TTP fall short. Ultimately, mitigation may require pursuing Science and Technology (S&T) solutions. We conclude the paper with a simplified notional case study to illustrate our cyber testing approach.

2. CYBER VULNERABILITY ASSESSMENT

The 2011 paper on the Science of Mission Assurance [8] introduced the information lifecycle as a construct for representing information evolution in a complex system. It defined the six phases of information:

- Information generation,
- Information processing,
- Information communication,
- Information storage,
- Information consumption, and
- Information destruction.

The paper reasoned about a dozen hypotheses that govern mission assurance in the context of the information lifecycle, and we reached some obvious conclusions, including the fact that a closed system that does not exchange information with the outside world is not vulnerable to external information compromise.

The corollary to this conclusion is that a system that exchanges information with the outside world may be vulnerable to compromises in the confidentiality, integrity and availability of external information. This corollary constitutes the basis for our cooperative CVA.

2.1 Information Exchange Boundary

Defining the Information Exchange Boundary (IEB) constitutes the first step in a cooperative CVA. We interchange the use of the terms Mission under Test (MUT) or System under

Test (SUT), depending on the context, to refer to the distributed information assessment under study. The specificity of the IEB definition depends in part on the form factor of the SUT. It is easier to visualize the IEB for an orbiting satellite than it is for a space operations center with numerous networked radars and ground stations, industrial control systems and power supplies.

2.2 Information Exchange Requirements

System specification design documents define the Information Exchange Requirements (IER) for a platform or a system, and provide a good starting point for an exhaustive enumeration of the information exchanges between a SUT and the outside world through the IEB.

An essential step in a CVA is to characterize in details every information exchange in terms of:

- Protocol: for example Link-16, Voice over Internet Protocol (VoIP)
- Protocol layers in use: transport layer, application layer
- Medium: wired, wireless, optical, infrared
- Modulation scheme: analog or digital, Phase Shift Keying (PSK) or Quadrature Amplitude Modulation (QAM)
- Frequency or band: 2.4 GHz, S-band
- Data rate
- Encryption scheme
- Authentication mode
- Data compression scheme
- Header and payload formats
- Other relevant characteristics

2.3 Adverse Cyber Effects

Estimating the impact of an information compromise presents a significant challenge in cyber risk assessment. We seek to estimate the impact of an information compromise in terms of the D5 effects: disruption, degradation, denial, destruction or deception. We display these effects on a two-dimensional chart along the axes of degree and duration, as show in Figure 1.[11]

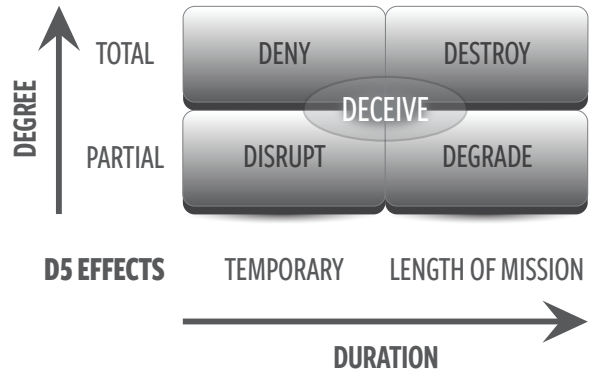

Figure 1. Effects in Relation to Degree and Duration

A thorough assessment of the impact of an information compromise necessitates decomposing the MUT into Mission Essential Functions (MEF), and estimating the effect on each MEF of a compromise in the confidentiality, integrity and availability of information flowing across the IEB.

Of the three IA tenets of confidentiality, integrity and availability, we focus first and foremost on the impact of compromises in information integrity. However, a compromise in confidentiality—someone else reading your good data—can also result in adverse mission impact. By the same token, reliability and safety requirements dictate redundancy in advanced information systems, permitting graceful degradation in the absence of certain critical information. In such a case, the absence of information, or a compromise in the availability of information, may be mitigated through redundancy.

The fifth D-effect, deception, can achieve any of the other four D effects by convincing a user or system of the presence or absence of an effect. We treat deception on par with the D4 effects of disruption, degradation, denial and destruction. While redundancy may mitigate a compromise in information availability, redundancy falls short in mitigating deception due to information integrity compromise. In a later section on S&T for mitigation, we explore trade-offs between information availability and information integrity, and seek to provide the mission owner a decision point: would you choose a radar that is available 100 percent of the time with a random 10 percent of the displayed information inaccurate, or one that is available 90 percent of the time with all the displayed information accurate?

2.4 Byzantine Failures

A reliable computer system deals with the failure of one or more of its components through redundancy and task re-allocation. However, a failure that manifests itself in one computer communicating conflicting information to other computers is referred to as a Byzantine Failure, or as a Byzantine Generals Problem.[12]

In a distributed computing system, Byzantine failures manifest themselves through errors of omission or commission, rather than total equipment failure. Byzantine failures may occur due to hardware failure, software bugs (register overflow), architecture limitations (propagation of round-off errors among consecutive computations) or malicious attacks. The impact of a Byzantine failure is independent of the cause, allowing us to focus on vulnerability and impact, and disregard the threat at this stage of analysis.

We apply Byzantine failure analysis to estimate the impact of a compromise in information flow across the IEB of a SUT. For example, an incorrect Global Positioning System (GPS) signal to an electric power generator, combined with a hardware failure in an atomic reference clock, may cause an erroneous frequency reference that disconnects the generator from the electric grid.

2.5 Classes of Vulnerability

Estimating the mission impact of information compromise is by far the most complex step in the cyber risk assessment process. Mission impact may be deterministic in nature, although it may manifest itself in a stochastic or probabilistic manner. The impact of an information compromise may depend on the operational environment of a mission, and certainly on the architecture, specification and implementation of the MEF that uses the compromised information.

A fractal mapping of mission dependence on cyber starts at the IEB of the SUT, showing a block diagram with information ingress and egress. Figure 2. shows a simplified IEB for a notional remotely-controlled aircraft. At the highest logical level, the IEB shows two classes of information exchange: wired when the aircraft is on the ground and wireless during flight. Further refinement may identify wireless communication, GPS signal, LASER ranging and camera.

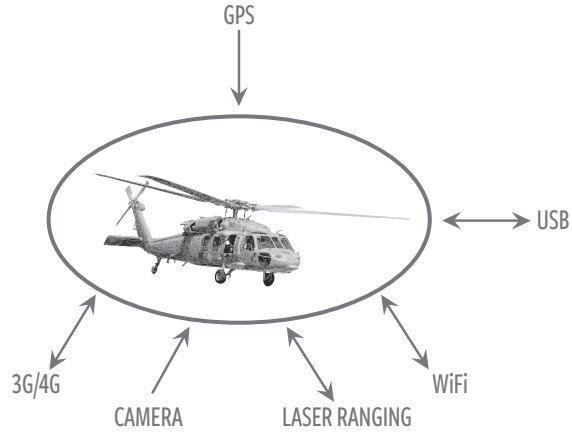

Figure 2. Notional Information Exchange Boundary

A higher fidelity mapping identifies the MEF depending on each of information exchange, outlines the architecture of the MEF, enumerates the specification requirements, and itemizes the details of the implementation. In accordance with our premise that functionality leads to vulnerability, we distinguish among three classes of design features that lead to cyber vulnerabilities:

i. Architecture vulnerabilities: these result from resource sharing inherent to distributed computer systems, as well as redundancy intended for reliability and safety.

ii. Specification vulnerabilities: these result from higher-level requirements for specific protocols, data formats, operating systems, authentication schemes, commercial off-the-shelf (COTS) sub-systems, and common standards.

iii. Implementation vulnerabilities: these include hardware, software and configuration errors.

A systematic information flow analysis that depicts all information generation, processing, communication, storage, consumption and destruction in each critical MEF may reveal inherent vulnerabilities in the architecture, specification and implementation of the MEF.

Subject Matter Experts (SME) with the right engineering education on the fundamentals of the MUT, working in close collaboration with cyber SME educated on the science of information assurance and trained on the art of cyber warfare, provide the minimum skill set necessary to identify the mission impact of a vulnerability to information compromise.

2.6 Blue Book of Cyber Vulnerabilities

We advocate generating a Blue Book that documents the cyber vulnerabilities in a SUT, coupled with the estimated impact of a Byzantine exploitation of each vulnerability. In addition to enumerating all information exchanges across the IEB of the SUT and detailing the properties of each information exchange, a Blue Book must include a detailed information flow diagram from the IEB into the system, highlighting those subsystems and components that constitute an MEF, and identifying the potential impact of an information compromise.

The potential impact of a compromise in information integrity and information availability on an MEF does not address the question of a compromise in system authentication. The designer of the Blue Book possesses the latitude to treat compromises in authentication as integrity compromises, or to create a separate class of vulnerabilities that deal with authentication, and potentially non-repudiation.

2.7 Cooperative Blue Team Testing

The ultimate objective of a Blue Book is to advise a cooperative Blue Team on the design of tests to validate or repudiate the hypotheses relating information compromises to mission impacts. While we must not mistake the absence of evidence of vulnerability for the evidence of absence of vulnerability, cooperative Blue Team testing seeks primarily to connect vulnerability to impact, independent of threat.

When designing Blue Team test experiments, the testers have unfettered access to the IEB of the SUT. This access permits them to replicate the information compromises detailed in the Blue Book, and observe whether the predicted impacts occur under a representative testing environment. The results of the Blue Team testing serve three purposes. First, they inform the adversarial Red Team on which information compromises to pursue maliciously. Second, they advise the mission owner on cyber risk to the mission. Third, they establish a roadmap for mitigation efforts based one the intent of the mission owner.

3. CYBER THREAT CHARACTERIZATION

The success of a cooperative Blue Team in demonstrating the mission impact of an information compromise accounts for two components in the risk equation: vulnerability and impact. The third component, threat, represents the capability—time, talent and treasure —necessary to replicate the impact in an adversarial manner, the access means—remote, physical, supply chain, and the intent—which we assume is there.

Estimating the mission impact of information compromise is by far the most complex step in the cyber risk assessment process.

While the Blue Team enjoys direct access to the IEB, we elevate the stakes to the Red Team by forcing it to replicate and exercise a realistic threat. Threat characterization is a complex undertaking due to a continuously evolving operational environment driven by new technologies available to both mission owner and attacker, and the insatiable thirst for new capabilities with unforeseen vulnerabilities that expand the attack surface.

While our vulnerability assessment focused on the consequence of an exploit—answering the *what* question, threat characterization focuses on capabilities and means to carry out an exploit—asking the *how* question. Separating Blue Team Testing—the *what*—from Red Team Testing—the *how*—eliminates the constant need for adaptive solutions to test for and mitigate evolving threats, and allows Red Team composition to consists solely of cyberattack experts without the requirement for mission experts.

We characterize a peer nation state cyber threat by the following attributes:

a. Highly educated on the science of information assurance

b. Doctrinally trained on the art of cyber warfare

c. Adequately resourced in time, talent and treasure

d. Thoroughly briefed on our target missions and systems

e. Mathematically specialized in architectural properties

f. Superiorly skilled in Byzantine failure analysis

g. Intricately involved in protocol specification and analysis

h. Critically embedded in the supply chain

i. Strategically postured in our command and control

j. Conveniently situated for access and persistence.

As a Red Team of aggressors attempt to understand, replicate and exercise a realistic peer nation state cyber threat, we grade on a scale of zero to ten their success in replicating the above ten characteristics, cautioning against the trap of projecting onto adversaries our way of thinking about cyberattack.

3.1 Cyber Kill Chain

A United States Air Force (USAF) centric model of air war decomposes the kill chain into the six phases of Find, Fix, Track, Target, Engage and Assess (F2T2EA)[13]. This model of the kill chain contains subtle differences from the traditional cyber kill chain that Lockheed Martin introduced in 2011[14], and which consisted of the seven steps of reconnaissance, weaponization, delivery, exploitation, installation, command and control, and exfiltration/effects.

> We seek to estimate the impact of an information compromise in terms of the D5 effects: disruption, degradation, denial, destruction or deception.

Both models require access to the target as a necessary step to delivering effects. While the Blue Team conducting cooperative vulnerability assessment enjoyed access to the IEB, a Red Team replicating a realistic cyber threat must achieve access in an adversarial or malicious manner, and escalate that access into generating D5 effects against the mission. The ten threat characteristics that we outlined earlier provide a realistic challenge, as well as a roadmap, to the Red Team to exploit a mission or system.

We note that access is neither necessary nor sufficient for generating an adverse impact to a mission. On the necessary argument, many cyberattack techniques do not require access to the target system, and have the ability to generate an adverse impact through remote or intermediate components such as man-in-the-middle attacks. On the sufficient argument, access alone to a target system does not guarantee the ability to deliver an adverse impact. This is where testing plays a role in proving or disproving the ability to produce an adverse impact by exploiting a vulnerability.

3.2 Risk Decomposition

Once a Blue Team demonstrates the impact of a cooperative information compromise, the job of the Red Team boils down to replicating that information compromise in an adversarial manner. Risk decomposition reduces the mission-specific engineering expertise required of the Red Team, and limits the required skill set to cyberattack against critical information. This deliberate distinction between a Blue Team of mission SME and a Red Team cyber SME places the mission owner at a significant advantage against an adversary who must demonstrate combined mission and cyber expertise. The end product of Red Team testing is a Red Book documenting validated threat replication to exploit the vulnerabilities identified in the cooperative Blue Book.

Estimating the mission impact of information compromise is by far the most complex step in the cyber risk assessment process.

3.3 Modeling and Simulation

Modeling of modern complex information systems and simulating their operation provides both Blue Team and Red Team a safe environment to validate and verify the perceived impact of information compromises. However, modeling and simulation (M&S) suffers from the limitation of the user perception of how a system must behave, rather than how it behaves in the real world. In many instances, partial differential equations with no exact solution model the real world, and many simulators enforce desired properties and behaviors that fail in the real world. If a model designer chooses wrong parameters or makes trivializing assumptions, simulation gives incorrect results. [15]

Defense Acquisition University (DAU) defines Validation, Verification & Accreditation (VV&A) as the process of determining that a model or simulation implementation and its associated data accurately represent the developer's conceptual description and specifications (verification); the process of determining the degree to which a model or simulation and its associated data accurately represent the real world from the perspective of the model's intended uses (validation); and the official certification that a model or simulation and its associated data are acceptable for a specific purpose or use (accreditation). DoD

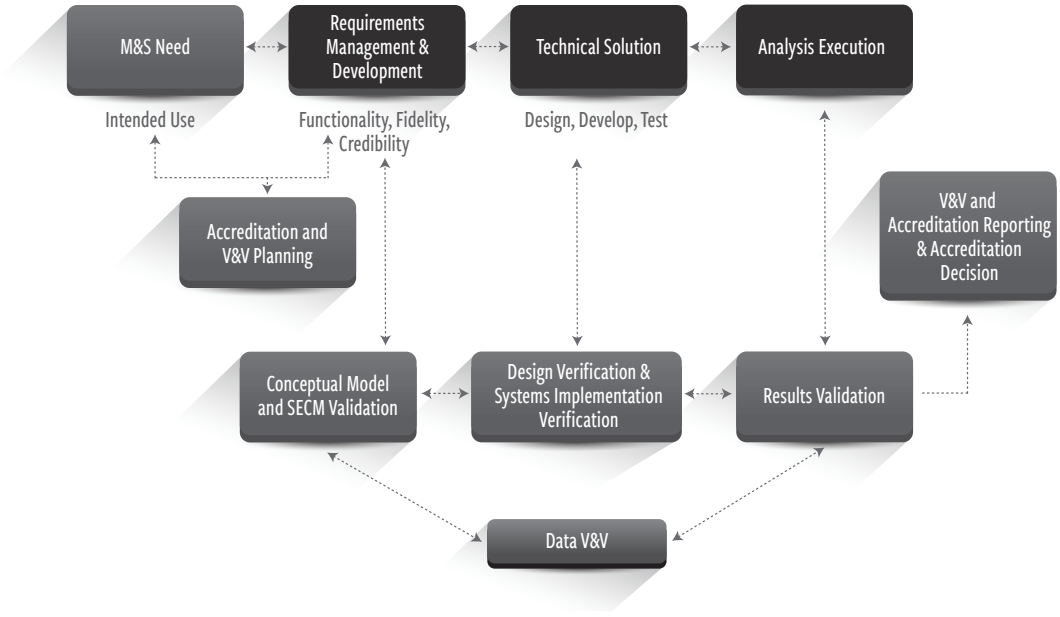

Figure 3. DoD representation of Validation, Verification and Accreditation Approach Process

Instruction (DoDI) 5000.61 mandates the use of the VV&A process as part of any M&S-based solution to risk assessment of defense systems. Given its predominantly compliance-based approach, VV&A falls short of increasing the fidelity of impact estimation of cyber vulnerability.

4. TESTING

Testing presents an opportunity for a cooperative Blue Team and an adversarial Red Team to act as trusted agents and honest brokers advising commanders on cyber risk to critical missions and systems, and identifying areas for S&T insertion in both the test process and vulnerability mitigation, and informing subsequently the development of future systems.

4.1 Cooperative Blue Team Testing

Following the identification of a potential vulnerability to information integrity compromises and the resulting mission impact, Blue Team testing seeks to validate such a hypothesis. We view the members of a cooperative Blue Team as mission experts schooled in the technology and engineering of the MEF. This *knowledge of us* approach seeks to answer the *what* question—what is the mission impact of a compromise in the integrity of information entering or exiting the IEB of the MUT.

Blue Team testers enjoy unfettered access to the MUT, allowing them to inject bad data

into the MUT through the IEB. The goal of the Blue Team is to estimate the impact of accidental or intentional information compromise in terms of disruption, denial, degradation or destruction of the mission, or deception. By applying Byzantine failure analysis to information flowing across the IEB, as well as information flowing among components within the IEB, we focus Blue Team testing on consequence independent of cause.

The set of all the vulnerabilities whose exploit results in adverse impacts to the mission makes up the vulnerability surface. The testing literature uses attack surface interchangeably with vulnerability surface, both terms referring to characteristics and properties under the control of the mission owner.

4.2 Adversarial Red Team Testing

Since the cooperative Blue Team focuses on assessing the mission impact of vulnerability exploitation—the *what*—the Red Team seeks to effect this exploitation through adversarial means—the *how*. Segregating the roles of the Blue and Red Teams allows building highly qualified Blue Teams of mission SME with limited cyber expertise, and conversely highly qualified Red Teams of cyber SME who lack mission expertise.

Once the Blue Team quantifies the impact of a cooperative information compromise, the job of the Red Team becomes to effect the same information compromise in a malicious manner. A Red Team of information aggressors develops the knowledge of them—understand the threat, replicate the threat, exercise the threat. The threat knowledge includes adversary capability in terms of time, talent and treasure, as well as attack means and intent.

A validated threat against a known vulnerability constitutes an attack vector, with the origin of the vector in the adversary camp and the destination in the mission camp. The total set of validated threats against identified vulnerabilities form the attack vectors.

We quantify in terms of talent, time and treasure the adversary capability necessary to compromise an information flow leading to the exploit of a vulnerability with an adverse mission impact. The talent of a realistic nation state adversary includes formal college education on the science of information assurance and extensive doctrinal training on the art of cyber warfare. The time element of the threat refers to the planning necessary to exploit a vulnerability, including the intelligence preparation of the environment for successful exploitation. Treasure refers to the cost in manpower and resources for successful exploitation, such as computing power to break passwords by brute force.

The attack means include the required tools to complete the attack kill chain, including access, persistence, generating effects and conducting damage assessment. Access may be remote over the Internet, local through physical access, supply chain of software or hardware, or access-less through man-in-the-middle attacks.

Traditional threat estimation considers the likelihood of a threat as a function of capability, access and demonstrated intent. For cyber risk assessment purposes, we assume intent given capability and access. In other terms, we exclude the qualitative assessment of intent from the quantitative estimate of threat, and consequently risk.

Lastly, we must ensure that the Red Team of aggressors understand, replicate and exercise a realistic cyber threat, not the projection of our idea of what the threat ought to look like. The USAF and the Lockheed Martin models of the kill chain reflect a narrow concept of how cyberattacks should be conducted, and falls woefully short of an accurate reflection of the global cyber threat environment. We must also ensure that we look at not just the current threat, but the projected threat across the lifecycle of the system under test.

5. MITIGATION STRATEGY

Mitigation seeks to reduce the risk to a mission by manipulating both ends of an attack vector: reducing vulnerability and increasing the cost to a threat, while reducing the potential impact of a successful exploitation. We observe one key lesson learned from safety investigation of aviation mishaps: to prevent a recurrence of a serious mishap, safety investigation reports recommend materiel solutions to augment plausible changes in tactics, techniques and procedures (TTP).

Many in the network security community seek to train users not to open attachments, click on web links or insert thumb drives into computers. In the meantime, several companies introduced materiel solutions that can mitigate the vulnerability of user actions, where training and TTP alone have failed.

One of the mitigation challenges of critical missions is the tradeoff between integrity and availability. It is often easier to assure a mission against the loss of available resources, but a lot harder to assure against covert compromises in information integrity.

Mitigation follows the normal sequence of vulnerability assessment, threat estimation, testing and mitigation, and represents the culmination of the mission assurance process. When Blue Team testing validates the hypothesis of mission impact of an information compromise and Red Team testing validates adversary capability to exploit such vulnerability, mitigation seeks to eliminate the vulnerability or reduce its impact, while increasing the cost of adversary exploitation.

We advocate a three-phase approach to vulnerability mitigation: TTP where practical, materiel solutions to augment or enforce TTP, and the pursuit of S&T solutions when no materiel solution exists. It is important to note the role of cyber security in vulnerability mitigation. While firewalls and virus scanners may play a role in mitigating configuration vulnerabilities, they often fall short in mitigating architectural and specification vulnerabilities, and may create additional vulnerability that increases the attack surface.

5.1 Tactics, Techniques and Procedures

One might argue that TTP are the tactical extension of strategy and policy, and that a disconnect between cyber policy and technology presents a threat to corporate and national security. Consequently, regulators and mission owners may increase the risk to their missions through policies and the resulting TTP. Having said that, not all TTP are ineffective. The Bell-LaPadula Model of access control [16] protects information in a multilevel security system through a policy that prohibits "reading up or writing down." Failure to enforce this fundamental TTP enabled well-publicized breaches of classified information.

In complex distributed computing systems, we view the role of TTP as mitigating vulnerability caused inadvertently by policy and guidance. For example, a measure or policy that applies equally to *all information systems* may ignore the different impacts of information compromise of a national security system versus an IT office automation system, and may require TTP to distinguish between these two classes of impacts.

One of the mitigation challenges of critical missions is the trade-off between integrity and availability.

Similarly, policies that trade away security for convenience, efficacy for efficiency, quality for cost, and integrity for availability, have an adverse effect on mission risks. Lastly, common misconceptions in cybersecurity practices mistake monitoring for defense, absence of evidence for evidence of absence, detection for protection, and projection for prediction.

5.2 Materiel Solutions

When reversing harmful policies and TTP fall short of mitigating cyber risk to a mission, disruptive materiel solutions may mitigate vulnerability. We provide several examples to illustrate our point, but we caution against viewing them as universal solutions looking for problems.

Quantum sensing and quantum communication eliminate the vulnerability of radio frequency (RF) transmission to eavesdropping, information manipulation or information spoofing. Read-Only Memory (ROM) reduces the vulnerability of a piece of software to accidental or malicious modification. Different size nozzles reduce the likelihood of diesel fuel filling a gasoline tank.

For supply chain management, split fabrication of integrated circuits provides a disruptive paradigm to reduce the risk of malicious backdoors in hardware, at significantly lower cost and higher potential success than detection.

5.3 Science & Technology

In cyber risk management, mathematics is the friend of the defender and the nemesis

of the attacker. The Rivest-Shamir-Adelman (RSA) Cryptosystem for public key cryptography [17] provides a compelling example. The difficulty in factorizing the product of two very large prime numbers provides the strength to the algorithm. The computational cost of multiplying two numbers will always be lower than the cost of factorizing the resulting product. Mathematical specification of the security requirements of a function allows the formal verification that the eventual implementation satisfies those requirements. In theory, this approach may yield an error free, vulnerability free, unhackable implementation. In practice, we can increase disproportionately the cost to a threat, and reduce the impact of an exploit.

The proliferation of cloud computing and its benefits in cost and redundancy drive the research on trading off information availability for information integrity. Mitigating cyber vulnerabilities caused by MEF architecture and single points of failure lead inevitably to public cloud computing, raising the traditional IA issues of confidentiality, integrity and availability. Atomic computing—where a computation either completes or does not—combined with homomorphic encryption [18]—where functions can operate on encrypted data and yield encrypted results—can guarantee trust and integrity of a completed transaction, but not its availability. Implementing national security missions in public clouds with some form of homomorphic encryption provides S&T challenges and fascinating prospects that deserve thorough study.

6. NOTIONAL CASE STUDY

In this section, we bring together the concepts of risk assessment, testing and mitigation into a notional case study. We examine the cyber risk to the mission of a Remotely Piloted Aircraft (RPA) used for power line inspection. [19] The vast expanse of High Voltage (HV) power transmission lines makes them vulnerable to inclement weather. HV lines are particularly susceptible to lightning, and their design provides circuit breakers and fuses to prevent propagation to generators and transformers. Regardless of the built-in protections, lightning may damage the insulators that hold mechanically the lines to the towers. Visual, infrared and RF inspection may detect electrons leaking at the periphery of a damaged insulator. This leakage generates a corona effect, predictive of a likely catastrophic failure. Therefore, inspecting HV transmission lines following a thunderstorm has become a prudent preventive practice in the industry.

6.1 Helicopter Characterization

The JR GSR260Z is a gas-powered remote controlled helicopter with a 26cc engine that provides the power to carry an 11lb payload. Depending on the payload, a full tank of gas provides up to 30 minutes of flight time with a range of 10 miles. A recent demonstration in Eastern Finland used the following helicopter configuration:

- Aircraft: JR GSR260Z, combustion engine
- GPS receiver: NEO M8N
- Doctrinally trained on the art of cyber warfare
- Take-off and landing controlled by manual controller
- Actual flight piloted by autopilot using GPS satellite navigation information.
- Real time video for flight control 720p IR camera
- Surveillance camera: Sony α7R, 36.4 megapixel full area (35.9 × 24mm) CMOS image sensor, objective 70mm zoom, firing control via autopilot. Memory card 128GB SDXC
- LIDAR: Hokuyo UXM-30LXH-EWA for vegetation and clearance analysis
- Control communications: 16 channel radio controller and 3G/4G public mobile networks
- Mission Planner GCS open source software for mission planning
- Finnish basic land maps and Google maps

6.2 Mission Decomposition

We decompose the mission of the JR GSR260Z into the following MEF:

i. take off and navigate to the power line
ii. achieve stable flight over the target with positive control by the operator
iii. establish a reliable return video feed from the RPA to ground control
iv. store surveillance video on internal SD card for further processing
v. land safely at the end of the mission.

We make the following assumptions to bound the solution space for this case study:

i. no onboard processing of the video surveillance signal for damage identification
ii. autonomous flight operation in areas with weak 3G/4G cellular signal
iii. GPS waypoint return home feature in the event of Command and Control (C2) loss.

6.3 Test Design

Figure 2. depicts a notional information exchange boundary. We analyze the mission impact of a compromise of two information exchanges, namely the GPS and the 3G/4G cellular signal.

If GPS signal availability is compromised by nearby mountains that block satellite signals or parasitic electromagnetic interference from electric power equipment that result in a jamming effect, direct operator C2 of the aircraft permits successful mission accomplishment.

The loss of 3G/4G cellular communication due to the absence of nearby cell towers can be mitigated through GPS waypoint navigation augmented by automatic power line tracking via pattern recognition of the navigation camera.

The simultaneous loss of both GPS signal and 3G/4G signal denies the aircraft the ability to complete the mission of recording surveillance video, and may even result in the destruction of the aircraft.

Given the hypothesis of the vulnerability of the mission to compromises in the availability of GPS and 3G/4G information flows allows the design of a cooperative Blue Team testing. Turning off the GPS and the 3G/4G cell phone in a controlled flight environment demonstrates the desired impact.

On the Red Team side, estimating the adversary capability necessary to deny the two signals leads to considering jamming signal directed against the aircraft. However, a priori knowledge of the 3G/4G communication protocol may permit a man-in-the-middle attack (such as temporary jamming) to drop a connection, and substitute it with a rogue connection that can divert or destroy the aircraft. Similarly, an attack on the integrity of the GPS signal through spoofing may have similar consequences.

6.4 Vulnerability Mitigation

A sample materiel solution to mitigate the vulnerability of simultaneous loss of GPS and 3G/4G cellular signals involves electro-optical and infrared (EO/IR) navigation. If the aircraft carried on board adequate computing capability, alternative navigation means may become possible. For example, storing video footage of the terrain under examination, an EO/IR navigation algorithm permits accomplishing the mission of recording surveillance video of the area under test, and successfully returning to base, even in the absence of GPS and 3G/4G signals.

7. CONCLUSION

We presented a systematic top-down approach to identifying cyber vulnerabilities in a complex information system through a disciplined information flow analysis, and estimating the mission impacts of information compromise. We applied Byzantine failure analysis to separate the impact of an information compromise from the underlying cause of the compromise, whether accidental or malicious. We advocated generating an introspective Blue Book of cyber vulnerabilities at the end of this vulnerability assessment phase to guide the cooperative test activities by a Blue Team. The subsequent development of a Red Book sought to quantify adversary capabilities necessary to exploit the cyber vulner-

abilities that the Blue Book identified. The Red Book provided Red Teams with a roadmap to conduct adversarial testing by a Red Team, and defined the threat capabilities that an aggressor team sought to understand, replicate and exercise.

We completed our discussion of mission assurance by addressing vulnerability mitigation. We explored first TTP where applicable, discussed materiel solutions when TTP fell short, and advocated the pursuit of S&T solutions. We concluded the paper with a notional case study.

The views expressed are those of the author and do not reflect the official policy or position of the Air Force, Department of Defense, or the U.S. Government.

Product names are trademarks of their respective owners. Mention of product names does not constitute endorsement by the United States Air Force, the Department of Defense, or the U.S. Government.

NOTES

1. Risk Management Guide for Information Technology Systems, National Institute of Standards and Technology, NIST Special Publication 800–30, July 2002.

2. Guide for Conducting Risk Assessments: Information Security, National Institute of Standards and Technology, NIST Special Publication 800–30-revl, September 2012.

3. Department of Defense Dictionary of Military and Associated Terms, Joint Publication 1-02, 8 November 2010 (As Amended Through 15 November 2015).

4. DoD Policy and Responsibilities for Critical Infrastructure, Department of Defense DoD Directive 3020.40, July 2010.

5. Cyberspace Operations, Air Force Doctrine Document AFDD 3-12, 15 July 2010, Incorporating Change 1 30 November 2011.

6. Department of Defense Architectural Framework, DoDAF version 2.02, 2011.

7. The Defense Acquisition System, Department of Defense Directive 5000.01, 12 May 2003.

8. Operation of the Defense Acquisition System, Department of Defense Directive 5000.02, 12 May 2003.

9. Test and Evaluation Overview, Defense Acquisition University, Lesson 18, 2006.

10. The Science of Mission Assurance, Dr. Kamal Jabbour and Dr. Sarah Muccio, Journal of Strategic Security, Volume IV Issue 2 2011, 61-74.

11. On Mission Assurance, Dr. Kamal Jabbour and Dr. Sarah Muccio, Conflict and Cooperation in Cyberspace: The Challenge to National Security, Editors: Panayotis A. Yannakageorgos and Adam B. Lowther, Taylor Francis CRC Press, 21 July 2013.

12. The Byzantine Generals Problem, Leslie Lamport, Robert Shostak and Marshall Pease, ACM Transactions on Programming Languages and Systems, Vol. 4, No. 3, July 1982, 382-401.

13. Deterrence in Cyberspace, Dr. Kamal Jabbour and E. Paul Ratazzi, Deterrence: Rising Powers, Rogue Regimes, and Terrorism in the Twenty-First Century, Editor: Adam B. Lowther, Palgrave Macmillan, December 2012.

14. Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains, Hutchins, Cloppert, et al. Lockheed Martin Corporation, 2011, 4-5.

15. On the Partial Difference Equations of Mathematical Physics.Courant, R.; Friedrichs, K.; and Lewy, H. IBM J. 11, 1967, 215-234.

16. Secure Computer Systems: Mathematical Foundations, David Elliott Bell and Leonard J. LaPadula, MITRE Corporation, 1973.

17. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, Ronald Rivest, Adi Shamir and Leonard Adleman, Communications of the ACM 21 (2): 120–126, February 1978, 120-126.

18. Fully Homomorphic Encryption Scheme, Craig Gentry, PhD Dissertation, Standofrd University, 2009.

19. Demonstration of Unmanned Aircraft for Powerline Inspections, Ville Koivuranta, LiDAR News Magazine, Vol. 5 No. 2, 2015.