The Merge of Electronic Warfare and Cybersecurity Test

Lt Col Jose R. Gutierrez del Arroyo, PhD
Arlington, VA
UNITED STATES

jose.gutierrez.1@us.af.mil

ABSTRACT

Few will question that cybersecurity is the "new kid on the block." Although the Information Technology (IT) community has extensive experience with T&E of cybersecurity systems for applications in the network-centric domain, we are now faced with the extension of cybersecurity to Electronic Warfare (EW) weapon systems on platforms and in systems-of-systems. What does it mean for a weapon system to be cyber-secured? What things are common between IT systems and weapons systems? How do we approach assessments and T&E in a cost- and time-effective way? How do cyber threats impact the evaluation of survivability, suitability, maintainability, and other "-ilities"? This paper uses knowledge gained from recent T&E experiences and policy efforts to provide answers to the aforementioned questions and propose a framework that integrates cybersecurity T&E into current EW T&E practices, minimizing the impact to resources and evaluation times. The overall concept takes the system under study from design through operational evaluation using three distinct but integrated phases, each with unique policy, resource, and outcome requirements. The paper will use a hypothetical study case to walk the reader through a simplified example of the approach.

1.0 INTRODUCTION

The evolution of cybersecurity policy and test practices to date has focused primarily (albeit not exclusively) on information technology (IT) systems and computer networks with the intent to ensure their availability, integrity, authentication, confidentiality and nonrepudiation [1]. In general, policies are in place to protect critical information that would be of great value to adversaries. DoD IT systems are defined as those that receive, process, store, display, or transmit DoD information. Platform IT (PIT) systems, which are also subject to protection in accordance to DoD policy, are defined as "computer resources, both hardware and software, that are physically part of, dedicated to, or essential in real time to the mission performance of special-purpose systems" [1]. It is safe to assume that most, if not all, modern weapon systems are built around some form of IT architecture and as such, contain PIT systems.

The instructions and documents dictating PIT assessment and authorization policies include a long list of references, requirements, and mandatory procedures that would easily compete with the entries of a small-town phone book. Electronic warfare (EW) systems are most definitely PIT systems and their capabilities are generally achieved by the use of several sensors, transmitters, data processors, extensive software, and other hardware. While cybersecurity revolves around the evaluation for authorization to operate within the platform and with other IT and PIT systems, EW test focuses on mission-focused capabilities. That is, how capable is the weapon to achieve its mission in the presence of threats. So the PIT is used for more than just IT functions; it is the backbone of the weapon system and critical to mission assurance. In this context, cybersecurity or the lack thereof, will have an impact on mission effectiveness, and that is the genesis of the ideas presented in this paper.

At the center of cybersecurity, there is the challenge of performing the right test that will provide the right answer to acquisition programs and to operational users. Mr. Frank Kendall, Under Secretary of Defense for Acquisition, Technology, and Logistics wrote:

"Cyber testing and the ability to achieve a "Survivable" rating in an official operational test environment continues to be nearly impossible for a Program of Record (POR) to achieve. Test criteria are not well defined and, even if requirements are met, the standards and scope is [sic] "independently" determined by the OTA or DOT&E for success. The threat portrayal often exceeds the capabilities of a Blue Force Team (i.e., nation-state threat going against a brigade-level formation), focuses more on "insider" threat of unreasonable proportions, and minimizes the importance of "defense in depth" approach. Recommend better definition for standard cyber rules of engagement at operational test, the allowance for external cyber protection teams, and that test reports focus on the program under test (not the overall "network")." [2]

When considering weapon systems, whether aircraft, smart munitions, surveillance systems, or warfare communication networks, among others, one needs to stand back and think about what these systems are designed to do, in what capacity they are employed, and how they could work together to create a tactical or strategic effect. It is very critical to have a clear connection between cyber-intrusion and mission assurance. However, as will be discussed, the problem can become unmanageable when contemplating the number of factors to consider in the test design.

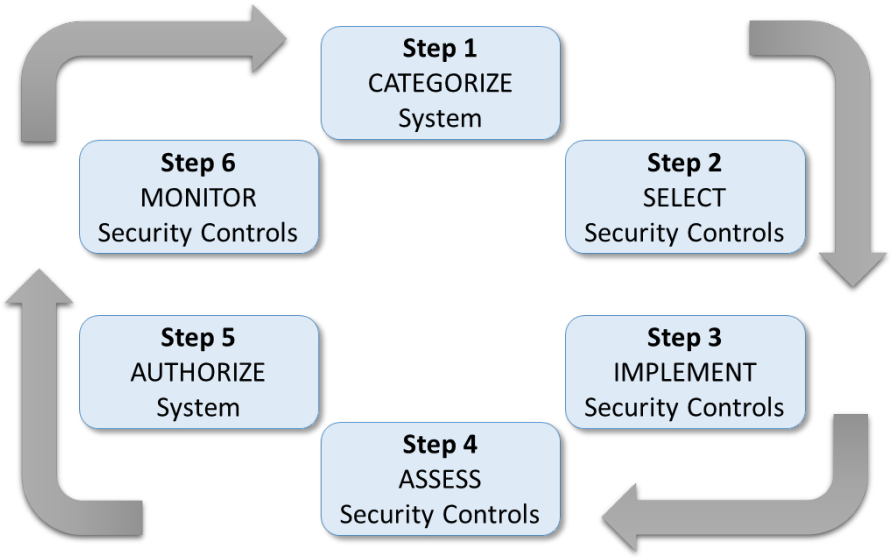

Figure 1: RMF Process

The RMF focuses on the authorization of operation based on risk assessments of vulnerabilities and their associated severity, resulting in decisions that range from *"no action necessary"* to *"stop operation"* mandates. However, the process as described in policy seems very IT-centric and lacks a clear connection to mission effectiveness. In [3], there is only one paragraph dedicated to the alignment of the RMF to the acquisition process where Developmental Test (DT) is associated with the assessment of security controls, and Operational Test (OT) is associated with the authorization of the system. However, the DoD Cybersecurity Test and Evaluation Guidebook [4] addresses the DT and OT requirements of cybersecurity and presents a link between cybersecurity and mission accomplishment through the DT and OT efforts of the acquisition cycle. Two processes described in the guide that are relevant in the merge of EW and cybersecurity test are the description of the cyber-attack surface and the vulnerability identification.

In summary, there are two distinct ways of thinking about cybersecurity test and evaluation (T&E) of a weapon system, each with a different objective. These two T&E paradigms are:

1) Testers must determine whether an information technology system (IT or PIT) is capable of operating in the network in a secure way, without compromising the security of other IT systems that interact with it. The RMF is a framework well-suited for this function and it concludes with an authorization to operate, but it doesn't necessarily addresses mission assurance.

2) Testers must also determine whether a weapons system is able to conduct its mission in a cyber-contested environment. The DoD Cybersecurity T&E guidebook provides some guidelines to accomplish DT and OT while linking cybersecurity to the mission. The outcome should be an assessment that will support the acquisition process as well as the operational user.

Having defined current DoD policies with respect to weapon cybersecurity, the discussion departs from the norm and regulations, and focuses on concepts and ways of thinking about cyber that perhaps can help refine processes, increase effectiveness, and improve efficiencies in DT and OT processes. There is absolutely no

intent to challenge or replace current DoD policies; on the contrary, some of these concepts are analogous to those found in [4]. The intent of "merging" EW and cybersecurity test is to explore T&E concepts from the EW community that could assist the cybersecurity community in managing the complexities associated with these relatively new assessments. First, the paper welcomes cyber to the group of environments where vast DT and OT experience already exists, and then uses EW concepts of survivability to draw parallels between the two. The paper then discusses analogies between the EW and cybersecurity domains and proposes a methodical approach to DT and OT. Finally, a fictitious example is used to demonstrate the ideas presented.

2.0 THE CYBER ENVIRONMENT

The cyber domain can be thought of as another environment where weapon systems need to be able to operate. For example, a fighter aircraft needs to be able to conduct its mission in physical and operational environments, overcoming challenges associated with each. Its performance is verified in the atmosphere environment (i.e., how fast, how high), in a physical threat environment (i.e., surface-to-air and air-to-air kinetics, logistics) and in an EW threat environment (i.e., integrated air defense systems, radar and communication jammers). When a system solution (material or tactical) is proposed and developed, test is designed to verify the performance in all applicable environments. In this context, the cyber environment is no different. The aircraft has to be able to complete its mission in the presence of cyber threats. Figure 2 shows a graphical depiction of the concept.

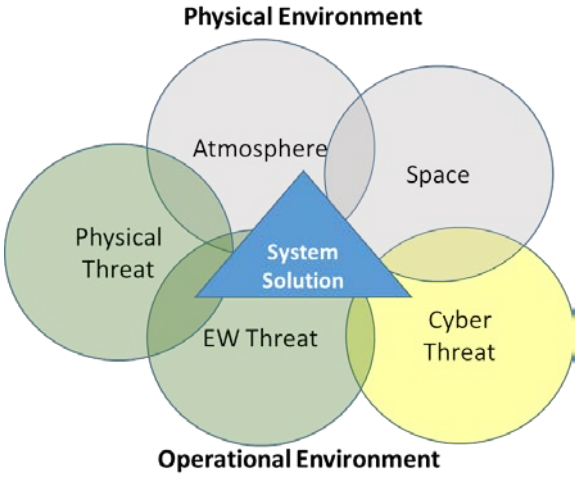

Figure 2: Mission Environments

3.0 EW PLATFORM TEST

EW platform test is focused on the capability of the system under test (SUT) to operate in a RF-contested environment to conduct Suppression and Destruction of Enemy Air Defenses (SEAD/DEAD) and other defensive and offensive missions involving the employment of electromagnetic (EM) energy. The term "EW platform" refers to any ground, air, or sea vehicle that carries EW capabilities on board.

It is very important to realize that an EW platform will rarely accomplish its mission as a standalone actor. Every mission set usually requires the collaboration and support of multiple systems from multiples services through the employment of various networks and communication systems. As the adage goes, the resulting systems-of-systems (SoS) is only as strong as its weakest link. Of course, the mission-criticality of each system varies, and some supporting systems may be "desired but not required." Nevertheless, when evaluating platform EW for mission effectiveness, the entire SoS chain must be considered.

In addition to mission effectiveness, EW platform test evaluates the survivability of the platform by measuring the susceptibility and vulnerability of the weapon system against a threat. Survivability is defined as the capability of the platform to avoid and withstand a man-made hostile environment, susceptibility is the inability to avoid threats, and vulnerability is the inability to withstand threats [6].

The above definitions are used to construct a kill chain model that begins at the existence of a threat, through system "hit," to system "kill." Figure 3 shows a graphical representation of a typical survivability model for an aircraft against a SEAD/DEAD scenario. In this model, EW systems are designed to reduce the susceptibility chain to avoid an aircraft hit.

EW test focuses on minimizing susceptibility of the platform by assessing, among other factors, detection, identification, and tracking by adversaries. It also looks at the effectiveness of counter-missile systems if engaged (flares, chaff, etc.), and the aircraft survivability given a "hit." Note that the entire assessment is based on the existence and capability of a *particular* threat activity, so every scenario requires its own survivability analysis.

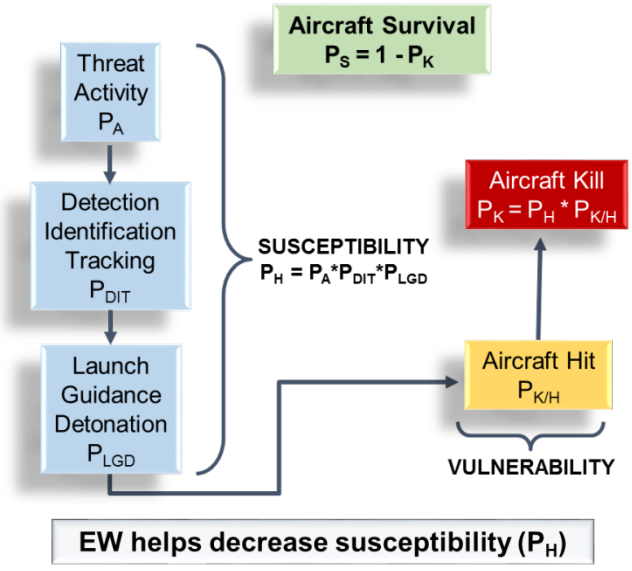

Figure 3: Survivability Model of Aircraft vs. SEAD/DEAD scenario [7]

4.0 THE MERGE

So where does cybersecurity test merge with EW test? Given the above test frameworks of mission effectiveness and survivability, the question becomes: What effect does a successful cyber-attack have on the mission effectiveness or the platform survivability? One immediate and obvious follow-up question is: Are my EW systems cyber-secured? Having unauthorized access to EW hardware and software can indeed alter the functionality of the system, impacting the ability to accomplish a mission and/or the ability to withstand and avoid threats. General John Hyten, Commander, Air Force Space Command, said:

"In cyberspace, we provide pathways for information, we deny adversaries information. It's the same [EW] mission that… we do in different domains." [5]

The above statements are fundamentally true. EW and cyber have analogous missions done in different domains. Consider the EW-to-cyber analogies drawn in Table 1. Although many other analogies can be made, the table suggests that both domains involve the same underlying concept of operation: access and denial operations in the presence of threat. The differences are in the means, modes, and paths.

Table 1: EW and Cybersecurity Analogies

EW Domain	Cyber Domain
Radar Warning Receiver	*Intrusion Detection System*
Track Quality	*Integrity of Data Processes*
Detection and Identification	*Access to operating systems, or hardware*
False Targets, false position/velocity data	*Data Corruption, Hacking, loss of system control*
Threat Activity	*Threat Activity*

However, one important aspect missing is that cyber and EW threats can be reciprocal. Thus cyber becomes a threat to EW systems and the platform itself. Cyber and EW test must not be stove-piped because weapon systems operate in all environments simultaneously (atmosphere, space, physical, EW, and cyber). It becomes critical that both test communities understand each other's missions, capabilities, and vulnerabilities to the extent required to conduct relevant and meaningful test.

Because all EW systems are built around hardware and software, they all have a natural and logical connection to the cyber domain. The susceptibility of the weapon system should also consider the *possibility* of cyber-attacks. For example, adversaries could try to prevent the accomplishment of a mission through the disruption of a radar system by use of radar jammers, physical destruction, or the use of software malware.

Consider the following three statements:

*A platform **EW** system must be able to provide mission assurance by protecting and ensuring the functionality of its on-board systems when encountering **electromagnetic** attacks.*

*A platform **cybersecurity** system must be able to provide mission assurance by protecting and ensuring the functionality of its on-board systems when encountering **cyber** attacks.*

*A platform **EW** system must be able to provide mission assurance by protecting and ensuring the functionality of its on-board systems when encountering **cyber** attacks.*

Note that all three sentences are in concept, identical. The difference been only in the domain (cyber vs EW) and the type of intrusion (electromagnetic vs cyber). A vulnerability could drive an effect on our onboard mission systems capable of disrupting the execution of our mission or worse, decrease our physical survivability.

Avoiding the debate on differences between DT and OT, the goal of the tester is, in essence, exactly the same: ensure the weapon system operates as intended in the contested environment. The survivability model in Figure 3 can be used to draw strong test analogies between cyber and EW. Armed with the aforementioned concepts, a survivability map in terms of cybersecurity is proposed in Figure 4. Note that "Mission Effectiveness" has been added to the survivability block because in addition to a potential system "kill," cyber capabilities could create a very wide range of effects at many system and mission levels.

Just as with EW survivability, cybersecurity helps decrease the susceptibility to threat action, and in turn, unauthorized intrusion by adversaries and thus access to other vulnerabilities. The EW test community has the experience base to evaluate the mission effectiveness and survivability of a SUT when faced with adversities, as long as limitations caused by the threat are understood. In the world of EW test, cyber can be considered to be just one more threat with potential to impact to any platform-based system and hinder the ability to conduct a mission. Conversely, in the cyber world, EW can be considered to be one more vector to the attack surface with potential to impact any aircraft IT system and hinder the ability to conduct a mission.

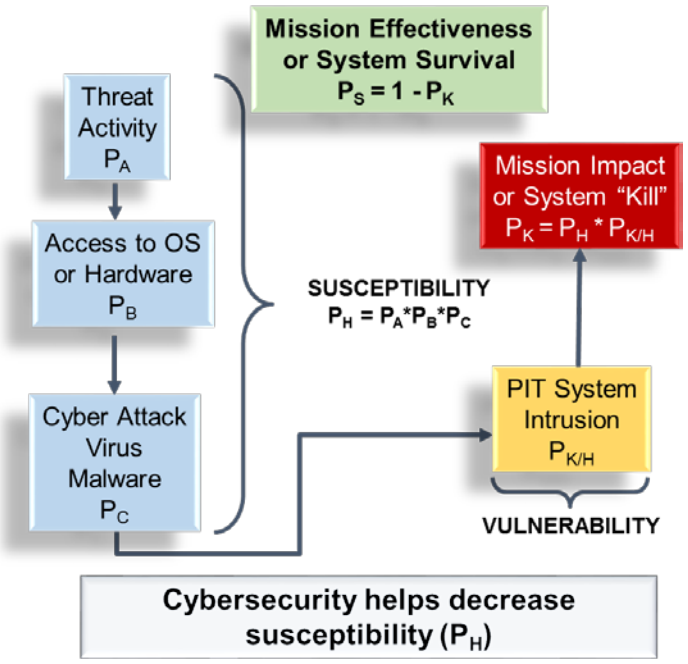

Figure 4: Aircraft vs. Cyber Survivability Model

5.0 WEAPON SYSTEMS CYBERSECURITY T&E

Having established logical connections between cyber and EW, this section proposes a beginning-to-end approach to evaluate cybersecurity of a weapon system in the EW domain. Although a similar approach could also be developed in the opposite direction (evaluate EW effects in cyber domain), this paper is written from the EW point of view.

As technology advances and adversaries get smarter, the threat grows more complex, increasing the burden on test communities to assess systems. There are simply not enough resources or time to develop and test a 100% cyber-proof system. Even after achieving a high degree of cybersecurity and cyber resilience, the rapid evolution of threats soon renders systems vulnerable again. The acquisition and test communities must approach the problem using a risk analysis framework. Just imagine the number of cyber threats in the world today, known and unknown. Every software virus ever written, every piece of malware code, every node of every network in existence, they all pose threats to the operation of a weapon system. It is easy to see how quickly the cybersecurity assessment requirements of a SUT can explode exponentially. It is impossible in both time and cost to test every possible combination at the system and operation levels. However, a robust test can be designed by using a standard risk management process shown in Figure 5.

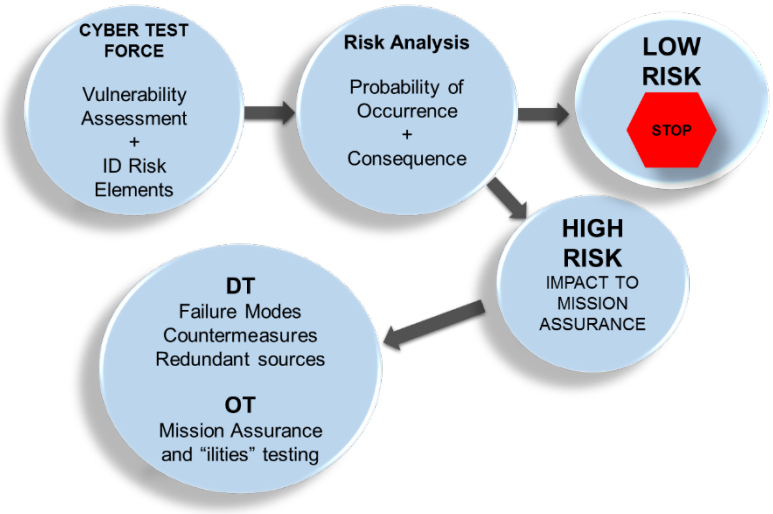

Figure 5: Risk Management Process

Figure 5 shows a proposed risk management process to determine what should and should not be tested based on two criteria: 1) the probability of occurrence and 2) the consequence of that occurrence. Related to the survivability model in Figure 4, the probability of occurrence is the survivability of the system or the probability of mission impact P_K. The consequence of P_K occurring describes the severity of the mission impact. Only those threats with a high probability of significant or severe impact to the mission or the weapon system should be evaluated. For example, if a cyber-attack is successful at infiltrating a SUT subsystem, but it only prevents the user from using one of several communication radios, then the mission remains assured and there is no incentive to spend resources developing further countermeasures or test programs.

Following the survivability model, a mission impact and system kill probability model can be defined as:

$$P_K = P_H * P_{K|H} \quad (1)$$

where P_H refers to the susceptibility of the system and $P_{K|H}$ is the probability of kill or system intrusion given that a susceptibility event took place. It follows that in terms of cyber threats, P_H is defined as:

$$P_H = \prod_{i=1}^{N} P_i \quad (2)$$

where N represents the number of events necessary for a successful cyber-attack and P_i are the probabilities associated with each of those events. Note that the susceptibility model follows a chain of events, and that most of the probabilities will be conditional probabilities given that a prior event has occurred. If any one of them is zero or close to zero, then there is little to no susceptibility and no critical need to evaluate further. It is crucial that the susceptibility model in Equation 2 be designed by a team of cyber experts, system experts, operators, and intelligence professionals. For those likely threats with a P_K greater than a defined threshold, determined to have significant impact to the mission, a formal test and evaluation should be conducted. The definition of a threshold value is beyond the scope of this paper; however, at a minimum, its value should account for the criticality of the mission, other system vulnerabilities, and program resources.

The T&E approach to cyber security in weapon systems, as it relates to EW and survivability, can be broken down into the following events (not necessarily sequential):

1) A thorough system engineering description of all systems, subsystems, the information flow between them, and all the potential interfaces to external data sources.
2) A thorough system engineering description of system functions critical to the aircraft mission set.
3) An analysis of logical connections tying entry points to functions, and those functions to the mission set.
4) Define mission operational requirements in contested area.
5) Identify current and future threats to mission accomplishments.
6) Test SUT operations in presence of threats.
7) Develop tactics, procedures, or counter systems based on results.

Events 1 -3 can be complex, difficult to accomplish, and time consuming. The methodology involved in accomplishing them is beyond the scope of this paper; however, the T&E Cybersecurity Guidebook contains some guidelines to help define it (i.e., characterize cyber-attack surfaces and perform vulnerability assessments) [4]. These comprehensive assessments will have to be done at least once by a team of cyber and system experts, with periodic revisions as systems get upgraded and threats evolve. However, the rest of the required events (4-7) are standard in EW T&E practices.

Of all the aforementioned events, perhaps the third one is the most critical because it connects the cyber threat to an EW function or to mission effects. The reader will note that although this paper addresses the impact of cyber threats to EW systems, mission impact can be easily extended to flight dynamics, weapon employment, logistics, and other systems of systems.

The proposed T&E process can be effectively used to develop countermeasures and tactics that will reduce the susceptibility of the system in face of the cyber threat. Using the events described above, a three-phased T&E approach is proposed:

- During the first phase, a team of cyber, intelligence, and system experts explore vulnerabilities of the SUT to cyber threats. The output of this phase consists of the identification of all potential nodes or attack vectors that an adversary could use to infiltrate the system, and the extent of the access. It should also include other external systems that are critical to mission assurance.

- The second phase requires the development of a SUT functional model where links between SUT functionality and the threat can be established. This phase is critical because it will help the DT and OT testers understand the risk associated with the threat in terms of likelihood of occurrence and severity of the event. There should also be a clear understanding of the difference between functional and mission requirements but the latter is expected to exist as an organic product of the acquisition process. The second phase should provide the risk analysis necessary to determine which of those vulnerabilities will generate high-value test points.

- The third phase should look no different than any other EW test program. Test requirements will be developed, DT and OT teams will perform T&E of the SUT in the threat environment, and a Test Report is provided with recommendations. The development of countermeasures and tactics to handle the threat may also be provided at this time.

6.0 T&E FICTIONAL CASE

A simple, fictional SUT will be used to demonstrate the proposed approach. The Joint Air-Ground Dual-Attack Penetrator (JAGDAP) is a highly maneuverable smart munition system carried aboard the new B-55 bomber. Its guidance and control logic uses targeting data provided by the legacy Omni Munition Ground (OMG) network through a platform RF link which is integrated with the platform's onboard GPS and INS system. The OMG network is controlled by several deployable ground stations and it feeds targeting updates and cueing to both aircraft and munition before and after launch.
The JAGDAP and the B-55 were developed with cyber resiliency from the beginning. An early intelligence assessment drove the design of several countermeasures that will, upon recognition of a cyber intrusion, adapt to the threat by "shutting off" any affected subsystem. The OMG link is a legacy system that connects securely via fiber to a central server with access to the Air Operations network which in turn fuses data from multiple sensor sources. The cyber test team (not the EW team) has been tasked to execute cyber resiliency test for the entire system (JAGDAP, B-55, and OMG). The cyber team has members from the cyber community, intelligence personnel, and engineers from the prime contractor.

Phase 1: Discover vulnerabilities to current and future threats.

Phase 1 relies on the Risk Management Framework (RMF) and assessments from the intelligence community to explore and assess the vulnerabilities to the information systems employed. A team with members from the cyber and avionics test communities makes a comprehensive evaluation of all the access points, the software and hardware architectures, the operating systems, and the RF systems. The team determines that there are 36 possible vectors in the attack surface. Once all attack vectors are identified, they employ blue and red forces to explore the robustness of the counter cyber design. The team reports no serious vulnerabilities in the B-55 or in the JAGDAP and both systems receive full authorization to operate. Prior assessments of the OMG network defined one vulnerability where an individual could access the network and gain access to data and control messages through one of the ground stations. There are no countermeasures developed yet to prevent the OMG vulnerability.

Phase 2: Link mission requirements to vulnerabilities and ID high-value test points.

EW, avionics, and weapon test personnel join the team and perform a functional analysis of the SoS to determine how the identified vulnerability relates to the mission. After rigorous systems engineering processes are applied, the team determines that through the OMG network, corrupted data and control codes could bypass the on-board tracking correlator, injecting false targeting information into the JAGDAP. The success of this intrusion has the potential to transfer complete control of the guidance system to adversaries, jeopardizing the integrity of friendly forces in the area. The team develops the susceptibility model of the system and determines the probabilities shown in Table 2.

Table 2: Susceptibility Analysis

Susceptibility	P_i
Threat exists in area of operation	1.0
Access to OMG ground networks	0.8
Identification of weapon system	0.9
Discovery of vulnerability	1.0
Adversary timely reaction to discovery	0.9
Successful intrusion	0.7
Successful effect given intrusion	1.0
Overall Susceptibility P_H	**0.45**

An assessment is made, and based on the criticality of the mission, the EW DT and & OT teams are tasked to perform a mission effectiveness evaluation considering this particular threat.

Phase 3. Evaluate SUT in a contested environment and use knowledge gained to report performance and develop countermeasures as required.

The DT and OT teams are asked to look at the effectiveness of the mission and the impact to EW operations in the presence of the threat. The team assumes the worst case scenario (successful intrusion) and evaluates the system as is intended to be operated. The final test report shows that:

1) Onboard EW fusion engine will prevent corrupted data and control codes from reaching other onboard EW systems.
2) There are no existing EW or cyber countermeasures that would detect false targeting or false control codes.
3) Physical survivability of the platform is assured since the platform would be out of the Air-to-Ground weapon strike zone as soon as the JAGDAP deploys.
4) The mission effectiveness will be severely reduced. Meeting mission requirements would not be possible.

Based on the test report, a team of operators determines that susceptibility could be significantly decreased by disabling the RF connection to the OMG network and employing a support platform that will provide standoff weapon tracking and targeting information through a different tactical data link. In addition, the OMG developer is directed to increase security of its ground units, and ground forces are ordered to strengthen physical protection measures in high risk areas.

The fictional case study highlights the importance of following a mission-based approach in addition to a SUT-centered one. Even though the SUT had full authority to operate and was built to be the most cyber-

secured system to date, the team found a high risk of complete mission failure through external nodes. The only EW system actor was the platform tracker which was easily disabled by injecting false control codes. In this case, information was the culprit and there was no need to have direct access to the SUT.

7.0 CONCLUSION

The cybersecurity of weapon systems is an extremely complex problem that can easily grow out of bounds given the number of IT systems, networks, and systems of systems required to accomplish a particular mission. The number of known and unknown threats only complicates the problem even further. It is practically impossible to design and test systems to be 100% cyber-proof given resources and time constraints. Drawing from EW T&E survivability and mission effectiveness concepts, a framework to manage the complexity of cybersecurity was introduced. Using a risk-analysis approach it is possible to narrow down a manageable set of test events that will be relevant, affordable and efficient, and that will provide the elusive survivability rating. The process would produce a list of high-value test points addressing only those cases where the likelihood of the threat is high, and the consequence is significant. By so doing, resources would be employed only where it matters, reducing workload, funding, and schedule delays. The fictitious case presented shows how a mission-focused approach will find critical vulnerabilities by linking cyber threats to weapon system functions.

It is important to mention that this process never ends. New threats will emerge, new adversary tactics will be developed, and re-assessment using new assumptions must be made. For the EW DT and OT tester, cyber threats can be added to the already-long list of threats to consider. The merging of cyber and EW in test is inevitable; many test efficiencies can be obtained through smart integration of test, intelligence, and operator communities. Hopefully the views presented herein will contribute to future refinements and efficiencies of an already-complex test process.

8.0 REFERENCES

[1] Department of Defense. 2014. DoD Instruction 8500.01, Cybersecurity.

[2] Kendall, Frank. August 2016. Cybersecurity Testing. Kendall DAU Magazine.

[3] Department of Defense. 2016. DoD Instruction 8510.01, Risk Management Framework for DoD Information Technology.

[4] Department of Defense. 2015. Cybersecurity Test and Evaluation Guidebook, Version 1.0.

[5] Corrin, Amber. 2015. Cyber and EW: It's all about effects, not omissions. C4ISRNET. http://www.c4isrnet.com (accessed 1 August 2016).

[6] Ball, R. 2003. The Fundamentals of Aircraft Combat Survivability Analysis and Design, 2ed. Virginia: AIAA Education Series.

[7] Welch, Martin. 2015. Introduction to Electronic Warfare. EW University, Edwards AFB, CA.