WHITE PAPER

Building Cyber Resilient Technologies

Dr. Ebonése Olfus, Vice President of Cyber Strategy & Emerging Technologies

Introduction

The U.S. government has played a pivotal role throughout history in advancing technological capabilities, which has spurred economic growth and development as well as enhanced national security. As technologies rapidly evolve, the Department of Defense (DoD) will continue to research and develop the most modern and technologically advanced weapon systems, capabilities, and platforms.

Unfortunately, our adversaries employ reverse engineering techniques to exploit weapon systems and technical plans for their benefit. Perhaps even more significant, they also gain insight into operational concepts and system use developed from decades of U.S. operational and developmental programs. Such information provides tremendous benefit to an adversary, shortening time for development of countermeasures by years. The DoD and its contractor base are high priority targets for cyber-attacks which result in staggering losses of system design information incorporating years of combat knowledge and experience. Dr. Gilmore, Office of the Secretary of Defense, Director of Operational Test and Evaluation (DOT&E) stated "Any electronic data exchange, however brief, provides an opportunity for a determined and skilled cyber adversary to monitor, interrupt, or damage information and combat systems."[1] Moreover, adversaries exploit and steal not just military operational systems, but intellectual property relevant to our commercial industries.

> *"You are going to be attacked; your computers are going to be attacked, and the question is, how do you fight through the attack? How do you maintain your operations?" – Lt Gen Ted Bowlds, Commander, ESC, 28 Jan 09*

The Challenge

The Department of Defense (DoD) will continue to operate in a complex environment indefinitely. Competition for wealth, resources, political authority, sovereignty, and legitimacy will produce a variety of conflicts between rapidly evolving and adaptive threats in an increasingly competitive but interconnected world. In an environment of decreasing resources, the DoD will shift in strategic focus while preparing to confront these threats. Furthermore, the distinctions between threats in the future will blur because of the complexity of adversaries, the multiplicity of actors involved, and the ability of threats to adapt rapidly. Adversaries will employ anti-access and area-denial strategies, innovative tactics, and advanced technologies to oppose U.S. security interests.

Unfortunately, the cyber safeguards and countermeasures commonly employed to defend technologies today primarily address low-end threats against our less essential technologies and are often ineffective against most forms of cyber-attacks targeting our mission critical technologies. Given the broad spectrums of threat, intent, and consequence to mission critical functions, determining exactly where our technologies lie in this continuum of dimensions is vital to determining the appropriate level of cyber defense investments.

[1] Pentagon Chief Weapons Tester: Almost All Military Programs Vulnerable to Cyber-Attacks http://observer.com/2015/01/pentagon-chief-weapons-tester-almost-all-military-programs-vulnerable-to-cyber- attacks/#ixzz3W9urEhCG

The notion that we can protect everything is not only unrealistic but also results in a false sense of security that puts our government contractors and DoD missions at serious risk. Subsequently, we have to balance our inability to achieve full cyber protection by ensuring that we can accomplish our missions despite cyber-attacks.

Resiliency is Key

For a computing paradigm, “Resilience is the ability to provide and maintain an acceptable level of service in the face of faults and challenges to normal operation”[2]. Resilience is related to survivability, which builds on the disciplines of security, fault tolerance, safety, reliability, and performance. This paper focuses on cyber security approaches to achieve cyber resilience when developing technologies, systems, networks, and platforms.

For any individual or organization to thrive over a sustained period, some level of resilience is required. How does one build resilience in a rapidly changing environment where emerging cyber threats are taking on increasing sophistication and severity?

The Deputy Secretary of Defense commissioned the Defense Science Board to perform a study. The title of the study was *Resilient Military Systems and the Advanced Cyber Threat*[3]. The research for this study was focused on the following:

- Define meaningful measures and metrics to evaluate and monitor the level of DoD operational system resiliency in the face of a cyber-attack.
- Identify strategies and techniques that could improve DoD system resiliency in the face of a cyber-attack.

The Defense Science Board’s recommendation to the DEPSECDEF was to direct specific actions to introduce cyber resiliency standards and requirements throughout DoD force structure. “These resilience standards should be used to design, build and measure capability against threats”. And the standards should evolve as the cyber threat evolves. Additional recommendations from the Defense Science Board include the following:

- Apply a subset of the cyber resiliency standards developed to all DoD programs (USD(AT&L), DOD CIO, Service Acquisition Executives (SAEs))
- Increase feedback from testing, red teaming, the Intelligence Community, and modeling and simulation as a development mechanism to build-out DoD’s cyber resilient force (USD(AT&L), Undersecretary of Defense for Intelligence (USD(I)), DOT&E, SAEs, CJCS)
- Develop a DoD-wide cyber technical workforce to support the build out of the cyber critical survivable mission capability and rollout to DoD force structure (USD(AT&L), CIO, SAEs, Director, Operational Test and Evaluation (DOT&E), USD(I), USD(P&R))
- Establish secure system design projects with Federally Funded Research and Development Centers (FFRDCs), University Affiliated Research Centers (UARCs), academia, commercial and defense industry (Assistant Secretary of Defense for Research and Engineering (ASD(R&E))
- Initiate a supply chain collection activity (USD(I))

It is at the high end of the continuum that technology resilience will matter most to enable continuity of mission critical operations and support rapid reconstitution of existing or minimally essential capabilities or the deployment of alternative means of accomplishing the mission. When designing a technology, we should incorporate strategies and techniques that support a balanced combination of protections, detections, and adaptive technical and operational responses that dynamically evolve in response to current and future cyber events.

Consequently, we need to design systems that are agile, adaptive, resistant, and resilient to being compromised. Cyber technology resilience is crucial to mission success. Traditional techniques derived from continuity of operations (COOP), disaster recovery (DR), operator training, and red team exercises remain vital to ensure that we are prepared to respond during a failure or natural crisis. They also play a crucial role in validating technical and operational resilience of technologies and systems. However, as implemented and practiced, these techniques must address current cyber-attack threats and techniques.

[2] University of Kansas ResiliNets Wiki and Wikipedia, https://wiki.ittc.ku.edu/resilinets_wiki/index.php/Definitions (accessed on 11 August 2010).
[3] Defense Science Board Task Force Report Resilient Military Systems and the Advanced Cyber Threat January 2013.

> *"Cyber threat is serious, and the United States cannot be confident that our critical Information Technology (IT) systems will work under attack from a sophisticated and well-resourced opponent utilizing cyber capabilities in combination with all of their military and intelligence capabilities."- Defense Science Board Task Force*

The Persistence of Cyber Threats

Cyber threats are persistent and advancing daily; so much so that the President directed the Director of National Intelligence (DNI) to establish the Cyber Threat Intelligence Integration Center (CTIIC). The CTIIC provides "integrated all-source intelligence analysis related to foreign cyber threats and cyber incidents affecting U.S. national interests; supports the U.S. government centers responsible for cybersecurity and network defense; and facilitates and supports efforts by the government to counter foreign cyber threats."[4]

In this sophisticated threat environment, traditional security tactics are failing. How do we leverage cyber threat information to develop technological resilience?

Resilient Networks Not a One Size Fits All Solution

Most analysts, business leaders, and visionaries have arrived at the same conclusion: there is no silver bullet, no one size fits all solution, and in most cases, no single approach that will offer protection from a cyber-attack. Resilience is not defined by a series of checklists, but through evaluations based on the current threat environment and the acceptable risk level for the organization. It is a paradigm shift that uses cyber threat intelligence to guide decisions and support agility.

As threats morph and organizational needs evolve, cyber resilience is, by definition, about continual refinement. With each scheduled cycle of assessments, the security strategy is honed, and since every organization has unique systems and different security needs, the results of each series of assessments is evaluated based on the current threat environment and the acceptable risk level for the organization, rather than a relatively generic series of checklists. The goal of cyber resilience is to sustain mission-critical system capabilities by applying security measures that assure the system can withstand cyber faults, failures, and attacks.

As organizations invest in innovative and adaptable capabilities and technologies to meet the challenges of emerging global threats, we must develop engineering concepts, science, and tools to protect and overcome malicious compromise of weapon systems, capabilities, and technologies to greatly enhance the manufacturability of trusted and assured defense systems across the acquisition life cycle.

The Way Ahead to Build Cyber Resilient Technologies

The impacts of a major cyber-attack can be devastating to any organization. Unfortunately, no silver bullet exists to prevent attacks, and breaches will occur despite an organization's best efforts at preparation and protection. Many customers lack the sophistication and expertise they need to address these new, more advanced threats. To minimize the potential devastation of a cyber-attack, you must change the way you think about cybersecurity; think in terms of not eliminating cyber risk but of creating cyber resilience especially when developing or acquiring technologies.

Since it is impossible to know all the possible threats and to stop all anticipated threats, the architectural design of systems must be inherently less susceptible to such threats, provide an increased level of penetration resistance, and provide engineered-in resiliency so missions and business functions can continue even when systems are operating in degraded or debilitated states.

Recommended services to assist organizations in building cyber resilient technologies include:

System Security Engineering – Develop an integrated approach to building trustworthy resilient systems. Utilizing NIST SP 800-160 guidelines and recommended steps to help develop a more defensible information technology infrastructure, including the component products, systems and services. Systems security engineers can apply the necessary security measures that assure the system can withstand cyber faults, failures, and attacks.

[4] FACT SHEET: Cyber Threat Intelligence Integration Center The White House Office of the Press Secretary

Cyber Threat Analysis – Utilize cyber threat analysts to proactively identify and examine global cyber threat trends by performing research of adversarial threats posed to various systems, technologies, operations, or missions in all appropriate intelligence sources. Examples of such tasks include:

- Analyzing collected data to derive facts, inferences, and projections concerning capabilities, intentions, attack approaches, and likelihood of various adversarial attacks under various situations.
- Researching resource allocations, motivations, tendencies, personalities, and tolerance for detection, attribution and retribution that influence adversarial decisions.
- Contributing to profiling adversarial behavior with respect to identified system attacks in an operational mission context.
- Producing formal and informal reports, briefings, and perspectives of the behavior of adversaries against target systems, technologies, operations, and missions.

Risk identification and technology resilience solutions are achieved through the observation, detection, and mitigation of attacks and exploitation against an organization's critical assets. Employ experts in the collection, aggregation, correlation, and interpretation of cyber threat Tactics, Techniques and Procedures (TTPs) for the establishment and maintenance of cybersecurity countermeasures and technology resilience solutions.

Cyber Assessment Services – Use accredited professionals who support all phases of test evaluation, exercise planning and assessment, test and evaluation planning, business process improvement and requirements analysis. These professionals can support research, testing and analysis to better equip the military and government from adversarial threats and achieve mission assurance. Assessment activities focused on penetration testing, technology exploitation, building cyber range infrastructure, and conducting tests and evaluations of cyber capabilities will further enhance the resiliency of your network.

- Penetration testing activities include threat identification and assessment of weaknesses in U.S. systems, so that they may be improved. To effectively accomplish this mission often requires the characterization of adversary capabilities. From this characterization, a threat model is then constructed and experimentally validated to demonstrate the impact of the threats against U.S. missions.
- Technology exploitation is a part of red teaming. It utilizes skills in reverse engineering, malware analysis, vulnerability discovery, exploit development, forensics analysis, and system characterization to find specific ways to gain and maintain unauthorized control over hardware/software systems. These efforts can improve the resilience and defenses of systems.
- Test and evaluation professionals perform evaluations of cyber systems and capabilities including the development of cyber threat exemplars and corpora, metrics, procedures, and methodologies for testing, and the planning, execution, and analysis of those tests.
- Forensics and reverse engineering are the identification, acquisition, recording and analysis of indicators used to quantify risks and discover the true source of a security attack. Use experts who use vulnerability identification through static and dynamic analysis, bypassing hardware and software security controls, co-opting adversary exploit tools, and quantifying zero-day capabilities. State-of-the-art analysis and system forensic tools can monitor, recover and analyze host and in-transit data for investigation, intrusion detection and service restoral.

The cyber-attacks our society experiences today are happening more frequently and are increasingly more complex. In minutes, an organization's entire IT and communications infrastructure can be compromised, leading to unusable systems and data; and can hinder or shut down operations completely. This is not going to abate anytime soon; and the challenge is for companies to be able to maintain critical functions when faced with these breaches. While we cannot entirely eradicate cyber-attacks on our networks, we can take steps to make our networks and systems more resilient to the devasting effects of these attacks, especially when developing and acquiring technologies. The recipe for an effective resiliency strategy will require technical, procedural and policy changes to the network infrastructure and operations. It is highly worth the time, money and effort to find and utilize those resources that can help organizations put a resiliency program into place.

Dr. Olfus is Vice President of Cyber Strategy and Emerging Technologies supporting a variety of programs within the Department of Defense. She has over twenty-four years of experience in system engineering, system security engineering, cyber technology development, cyber program management, system design and integration, and strategic planning in both the government and commercial markets.