Global Information Assurance Certification Paper

Tackling DoD Cyber Red Team Deficiencies Through Systems Engineering

GIAC (GPEN) Gold Certification

Author: John Schab, JSchab@mastersprogram.sans.edu
Advisor: Sally Vandeven
Accepted: TBD

Abstract

Red teaming is an essential capability in preparing and assessing the Department of Defense's (DoD) ability to execute their mission in a contested cyber environment. The identified deficiencies in DoD's overall red team capability resulting from their ad-hoc implementation creates unknown mission risk to the Combatant Commands and Services leading to a significant threat to national security. Unfortunately, many senior DoD officials are citing a lack of resources as the reason for the deficiencies and believe an increase in funding will solve the issues. However, funding alone is not scalable to address DoD's gaps in red team capability, and throwing more money to the existing ad-hoc process is quickly becoming a huge money pit for the DoD. This paper analyzes the deficiencies and concludes the primary cause to be a lack of a structured process needed to define, design, build, and sustain the required DoD red team capability. The solution presented is to treat the overall DoD cyber red team function as a complex system operating within a system of systems and apply the systems engineering process. Implementing a systems engineering process will eliminate some of the identified deficiencies through design and will identify feasible solutions or alternatives to the deficient areas which design cannot eliminate. The systems engineering process can help DoD build an effective and efficient red team capability which is needed to ensure the military can successfully execute its missions in the contestant cyber environment.

1. Introduction

In an August 1, 2014, memo, the Director, Operational Test & Evaluation (DOT&E) for the Department of Defense (DoD) specified an Adversarial Assessment as one-half of a two-phased approach for operational cybersecurity testing. The Adversarial Assessment "should be conducted by an operational test agency employing a National Security Agency certified adversarial team to act as a cyber aggressor presenting multiple cyber intrusion vectors consistent with the validated threat" (Director O. T., Procedures for Operational Test and Evaluation of Cybersecurity in Acquisition Programs, 2014). For this paper, the term "DoD cyber red team" or any variation implies a National Security Agency (NSA) certified adversarial team employed during an Adversarial Assessment.

1.1. DoD Definition of Red Teams

A DoD cyber red team is a group of people (military, civilian, contractor) who emulate an adversary's tactics, techniques, and procedures against a targeted mission or capability (Maunual, 2013). The Department of Defense Manual 8570.01M defines a red team as "An independent and focused threat based effort…based on formal; time bounded tasking to expose and exploit information operations vulnerabilities of friendly forces as a means to improve readiness" (Officer A. S., 2015). The key point of the definition is that red team activity is focused and threat-based with a formal bounded tasking.

The Joint Chiefs of Staff's Department of Defense Cyber Red Team Certification and Accreditation manual details the purpose of a cyber red team. The tasks include identifying exposed information and vulnerabilities; supporting information assurance readiness; creating a degraded, disrupted, or denied cyber environment; developing the skills and exercise capabilities of cyber forces; participating in the evaluation of Computer Network Defense Service Providers (CNDSPs); and providing Protect Services for CNDSPs (Maunual, 2013). Although numerous cyber red teams are utilized in various ways across the DoD as the above definitions state, only National Security Agency certified and U.S. Strategic Command (USSTRATCOM) accredited red teams

are authorized to operate on live DoD operational networks (Maunual, 2013). This paper focuses on the use of National Security Agency certified DoD cyber red teams used during Adversarial Assessments, not all cyber red teams used across DoD. However as the paper will explain, the "catch-all" definition above results in DoD trying to build an unrealistic and unfeasible "be-all" capability.

1.2. DoD Use of Cyber Red Teams

DoD has long recognized and used red teams as part of their test and evaluation (T&E) and training strategy. DOT&E requires an Adversarial Assessment as part of cybersecurity testing on "all oversight information systems, weapons systems, and systems with connections to information systems, including major defense acquisition programs (MDAP), major automated information systems (MAIS), and special access programs" (Director O. T., Procedures for Operational Test and Evaluation of Cybersecurity in Acquisition Programs, 2014). The Adversarial Assessment evaluates the ability of the system to support its missions while facing a validated and representative cyber threat portrayed by a DoD cyber red team. The red team is perhaps the most critical piece of the Adversarial Assessment since, without accurate threat portrayal, the Adversarial Assessment cannot accomplish its goal.

The red team's objective is to induce mission effects through fully exploiting any vulnerability per the tactics, techniques, and procedures (TTPs) a validated threat would use. Utilizing the threat's TTPs is often a challenge as time and manpower are often lacking for red teams. In cases where there is insufficient time for the red team to perform thorough reconnaissance to identify vulnerabilities, they may use data found during earlier vulnerability and penetration testing, prior credentials gained on other connected systems, or be white carded into a starting position to realistically emulate the access a persistent advanced adversary may have gained (Director O. T., Procedures for Operational Test and Evaluation of Cybersecurity in Acquisition Programs, 2014). In the rare cases where red teams are not constrained by time, they will implement their attacks based on the intelligence information contained in threat folders. The threat folders

contain the TTPs and tools a threat is known to utilize along with the threat's desired objectives for attacking the system.

Understanding DoD's use of National Security Agency certified cyber red teams during Adversarial Assessments yields two significant points. First, the red team's mission is to portray a threat that is validated by the intelligence community. Second, the red team's actions during the Adversarial Assessment should be consistent with the validated threat. If these two points are followed, red teams will not be free playing. Instead, they will be focused and mirroring a specific threat actor. Free playing activity should be conducted by a penetration tester, not a red team during an Adversarial Assessment.

1.3. Cyber Red Team Certification and Accreditation

The Chairman of the Joint Chiefs of Staff Manual on the Department of Defense Cyber Red Team Certification and Accreditation provides guidance on certifying and accrediting DoD cyber red teams (Maunual, 2013). DoD red teams need to be certified and accredited to evaluate Computer Network Defense Service Providers before conducting activity on DoD networks. The Evaluator Scoring Metrics focuses on administration, operations planning and reporting, training, processes and procedures, operations support, and tools. Additional details about the metrics are classified. This process certifies and accredits the entire team versus individuals of a team.

As a quality control attempt, the DoD requires each red team to complete the Certification and Accreditation (C&A) process every three years. The focus of the C&A process is to ensure each red team operating on live networks can do so without causing harm to government systems (Buchanan, 2010). However, this process does not evaluate a red team's ability to portray validated threat actors which is a process that is lacking across DoD. Since DoD has not developed a process to evaluate a red team's ability to portray validated threats, inconsistency has developed across red teams where some red teams are noticeably better at portraying advanced threats than others. This inconsistency is a major flaw in the test and evaluation process since operational testing is occurring in an environment without a properly validated threat. The current Certification and

Accreditation process is essential as DoD needs to ensure red teams do no harm to live systems, but it does not address the need to validate a red team's ability to portray realistic threats.

1.4.Red Team Structure

A red team must comprise of high-level specialists with a broad range of skill-sets who can provide an adversarial view. An ideal member possesses the technical skills along with an adversarial mindset, perseverance, and imagination (Derene, 2008). The team should be made up of professionals from different areas of expertise to include ethical hackers, network engineers, social media specialists, and even psychologists (Pascal Brangetto, 2015). The size of each DoD red team typically varies in size from 8 to 15 members (Chabrow, 2009). The team makeup is a mix of military, government, and contractors. The military members, usually two-thirds of the team, are the ones pounding the keyboard doing the actual hacking, while the government and civilian members write code to support the team's objectives (Derene, 2008).

This structure alone creates challenges for red teams to portray validated threats. The small size of the team makes it difficult to incorporate the breadth and depth of expertise needed to portray a state sponsored threat which employs armies of hackers. Additionally, in this structure, the military members are key in executing the red team's attacks, but military members are frequently rotated. By the time the military members are trained to a sufficient level of competency, they are rotated to a different assignment resulting in the red team having to indoctrinate new members regularly.

2. Red Team Deficiencies

DoD Cyber Red Teams play a critical role in cybersecurity testing as they portray the realistic cyber threats that DoD's systems face. Previous DOT&E Director, Dr. Michael Gilmore, stated their importance:

> DoD units cannot train to, or be assessed against, the critical cyber defense functions of 'Detect' and 'Respond' without Red Team capabilities to penetrate the network and system defenses, and attack mission systems commensurate with the capabilities of our adversaries. Unfortunately, chronic red team shortfalls continue to put the Combatant Commands' and Services' ability to 'fight through' a contested cyber environment at risk. (Director O. T., Department of Defense (DoD) Cyber Red Teams Deficiencies, 2016)

Even though DoD recognizes the importance of red teams and shortfalls were documented by DOT&E over fours years ago, DoD has not taken appropriate action to fix the chronic red team shortfalls. The primary reason cited for the lack of action is limited financial resources. Senior DoD leaders view additional funding as the solution as additional money will be used to hire, train, and retain the required personnel. However, as the deficiencies are analyzed, the data shows a financial solution alone will not solve all the deficiencies as the total amount of funding to do so is not available to the DoD. Instead, the data points to a lack of requirements and planning needed to build the DoD red team capability.

2.1. Capacity

The demand for red teams is already greater than DoD's capacity and continues to grow. The DOT&E memo states the capacity shortage becomes even larger with the requirements of Section 1697 of the 2016 National Defense Authorization Act. Section 1647 calls for additional operational assessments of DoD network security to include each major weapon system by December 31, 2019 (Congress, 2016). To compound the issue, subject matter experts continually identify new cybersecurity testing needs which place even more demand on DoD cyber red teams. A recent Defense Science Board

(DSB) report on cyber deterrence recommends the Secretary of Defense immediately directs the Director of the National Security Agency (NSA) to establish a Strategic Cyber Security Program (SCSP) to perform red teaming on offensive cyber, long-range strike and nuclear deterrent systems (Board, 2017). The DSB report identifies the need for a top performing red team to meet this mission and recommends cannibalization of talent from across DoD and National Laboratories to meet this newly identified need.

DoD continues to increase the budget for cybersecurity. However, there is currently no detailed plan to increase the number of DoD Cyber Red Teams to ease the workload on each red team. DoD needs to calculate the current and future demand for red teams and prepare a detailed plan to meet it which accounts for member training and vacation.

2.2. Threat Portrayal

DoD faces a vast array of cyber adversaries from script kiddies to nation states. Each threat has its doctrine, tactics, and capabilities. DoD cyber red teams are being asked to portray this full spectrum of threats. Considering the number of threats that are unique, a single red team cannot possibly represent the entire range. Typically, the time a red team has on a system is limited that they naturally gravitate to the low hanging fruit available and rarely portray a specific validated threat actor. Additionally, the effects a red team can create are severely limited in the Rules of Engagement (ROE) along with their most critical commandment "do no harm to the system." These limitations result in unrealistic threat portrayal. Finally, to aid in defender training, red teams are often instructed to intentionally create noisy effects to gauge the defenders' threshold of detection. A validated threat would do everything to remain undetected while the red teams are being instructed to intentionally create artifacts and effects to see if they are detected.

2.3. Training

There is minimal time for training since red teams are in such high demand. DOT&E's Annual Report explains the issue stating, "The personnel shortage has

drastically increased the operational tempo of red team members, reducing their training opportunities to the extent that they are not able to keep pace with the tool and skill sets of advanced cyber adversaries" (Director O. T., 2016 Cybersecurity Annual Report, 2016). Red team members may be able at most to take one to two weeks of training per year which is inadequate to be able to keep current with the latest tools and techniques. Most of the training red team members receive is informal. They frequently spend their time learning new tools and techniques out of personal interest and passion.

There is consistent staff turnover especially among military members which means regular loss of knowledge. Military members are rotated into different assignments every few years by design. Civilian members frequently leave for higher paying industry jobs once they gain a few years of DoD experience which is highly coveted by industry. The turnover can make the investment in training an individual worthless if that individual leaves the red team without being able to transition the knowledge to his replacement or other team members.

There are no training standards for individual team positions or overall team operations to support required threat emulations. The lack of initial training requirements to ensure new red team members can perform the essential mission tasks can make integrating new team members challenging. As with industry, DoD does acknowledge certifications in the field, but frequently sees the limitations of translating a certification into job performance. There is no defined continuous training plan which outlines how a red team member will continue to stay current with an evolving adversary. A universal training program across red teams in nonexistent. Each team, therefore, has various levels of skill sets resulting in no consistency across the red teams. Finally, there is almost no collaboration across red teams which produces very minimal cross pollination of knowledge. The lack of collaboration results from a lack of time and funding to sponsor the exchanges, no one authoritative owner who can drive the collaboration, and the competition between red teams hinders the desire to share knowledge.

2.4. Reluctance Limiting Red Team Actions

Cyber security is unfamiliar to most senior DoD leaders, so they approach it with apprehension and reluctance. Military leaders are well versed in traditional warfare tactics, yet cyber presents a whole new and different warfighting domain which they don't understand or feel comfortable operating in. For most military commanders, experience facing cyber threats is minimal, so the idea of a person on a computer in a far-off land who can kill them through their computer isn't believable. Therefore, they place cyber on the back burner and treat cyber as an annoyance as they train to accomplish their mission. Because of this view, Combatant Commanders don't allow red teams to fully participate in major exercises because they don't want the red teams to interrupt the command's mission training objectives (Serbu, 2016). Unfortunately, this action produces negative training for the warfighter as an advanced cyber adversary can most certainly interrupt or defeat the mission through the cyberspace domain.

During off-the-record discussions, commanders admit to placing additional restrictions on red teams for fear of looking bad if the red teams are too successful. Flag officers are afraid of a subpar assessment resulting from red team activity during an exercise which will hurt their chance of promotion. Therefore, they attempt to "game" the exercise by ensuring red team activity is announced and constrained as much as possible (Buchanan, 2010).

Currently, DoD personnel still treat cybersecurity defense as an administrative function and not a warfighting capability (Director O. T., 2016 Cybersecurity Annual Report, 2016). Until this thinking changes and the constraints are taken off, red teams are going to be continually falling short of their goal of portraying a validated threat. DoD needs to recognize the military's reluctance and uncertainty about the cyber domain and account for this constraint in their planning.

2.5. Funding

Funding for cyber activities continues to grow. The requested 2017 DoD cyber budget was $6.7 billion which was a 15.5% increase over 2016 (Officer O. o., 2016).

Additionally, DoD requested an additional $7.2 billion in cyber funding in their 5-year spending plan increasing the total cyber spending to $34.6 billion from 2017-2021 (Matthews, 2016). Former Secretary of Defense Ash Carter justified the increase by stating it would further improve DoD's network defenses. Since DoD cyber red teams play a critical role towards improving the network's defense, one could rationally assume funding would be available to address red team deficiencies. During 2016, DoD's budget planned about $500 million towards compensating cybersecurity professionals out of the $5.5 billion in requested cyber spending (Sternstein, 2016). However, the consensus among the red teams from personal interviews was none of this additional funding filtered down to them in the form of salary increases or additional budget lines to buy capabilities.

Senior DoD leaders are still citing funding shortage as the primary limitation in providing the adequate red team capability. DoD recognizes the difficulty recruiting, training, and retaining red members with limited pockets as industry often lures top performers away with lucrative compensation packages. Even though adequate funding to build the red team capability is lacking, funding is not the primary cause of the deficiencies. Red teams will continue to grow as a money pit without fixing the current ad-hoc composition of the capability.

In addition to hurting DoD's ability to recruit, train, and retain key personnel, inconsistent and insufficient funding to the red teams affects the red team's ability to purchase hardware and software to accomplish their mission. DoD needs to allocate a consistent and appropriate budget line to supply the red teams with the tools they need.

2.6. Tools

DOT&E's memo states red teams are too dependent on commercial tools and are unable to develop new and effective ones (Director O. T., Department of Defense (DoD) Cyber Red Teams Deficiencies, 2016). From observing DoD red teams in action, Cobalt Strike appears to be their favorite hacking tool. Although Cobalt Strike is a very versatile and flexible hacking tool, red team members can become overly reliant on the tool's methods which can make detection easier. An advanced adversary would likely use

customized tools designed to exploit a particular system making detection hard. Also, Cobalt Strike may not have the functionality to exploit highly specialized and customized systems resulting in the red team members needing the ability to write their own tailored exploits.

DoD vets and approves any tool before use which does limit the red team's ability to create their own. Red teams cannot download the newest exploit for a recently announced unpatched vulnerability for their use. Any exploit code would have to be thoroughly reviewed and likely be rewritten to ensure the code only does what it claims to do before red team use. This process results in the red team not being able to be as adaptable in exploiting newly found vulnerabilities as the adversary would be. Resources are not readily available to develop new or specialized tools which limit red team actions.

A shared database among DoD red teams of any customized tools would be helpful. However, the lack of sharing across red teams prevents this. Individual red teams that invest their resources into a customized tool will want to hold onto it closely for fear of burning that tool out if shared across all red teams. There is no incentive or reason for the red teams to share their tools. A potential solution is to have a Federally Funded Research and Development Center (FFRDC) build and maintain a centralized database of approved tools for Red Team shared use. Any tools created by an FFRDC would be available for use by all red teams since they would be owned by the DoD. Since FFRDCs do not compete against industry who design and build the systems, FFRDCs are free of any conflict of interest when creating tools which would show security weaknesses in a system built by industry. Additionally, FFRDCs have the capacity and resources if tasked to continually develop new tools as the threat evolves.

2.7. Competition from Commercial Industry

Commericial industry has the unfair advantage of deeper pockets when recruiting highly skilled cybersecurity professionals. DOT&E's Annual Report acknowledged the unlevel playing filed by stating, "DOD had an enviable share of master-level operators seven years ago, but a significant number of these cyber experts accepted positions in the private sector in the ensuing years, often because of the increased wages and more

relaxed work environment" (Director O. T., 2016 Cybersecurity Annual Report, 2016). A former intelligence officer who headed a red team now earns more than $300,000 per year in industry which is more than triple his military salary (Harris, 2015). Even if the pay were equivalent, some skilled cyber professionals would choose against working for the government based on public perception that the government infringes upon personal privacy with its cyber activities.

The DoD is attempting to find ways to hire and retain skilled employees by offering higher pay, but they are still finding it difficult to provide highly competitive wages within the government system. The Federal Cybersecurity Workforce Strategy issued in July 2016 outlined guidance for special pay rates for IT and computer professionals, as well as other incentive tools (bonuses, relocation incentives, student loan repayment). Under the special pay rates, a GS-11 IT manager in D.C. at the highest compensation level would earn ~$81,000 while an equivalent IT manager in the private sector would earn a median base salary of $100,00 (Cordell, 2016). Although the higher pay rates are a step in the right direction, the government still will not be able to compete for top cyber talent based upon salary alone. This salary constraint needs to be acknowledged and designed into the capability solution.

2.8. Time

Real world adversaries can spend multiple years in the reconnaissance phase searching for a crack in the defense. They typically do not have a time constraint on their activities. In fact, time is usually seen as an asset for the attacker as the attacker will always be successful if given enough time (Harold F. Tipton, 2010). On the other hand, DoD cyber red teams have significant time constraints to attack any one system. Most exercises run around two weeks. If the red team is lucky, they may have a week or two to prepare for execution. However, this short time frame falls well short of the months or years that an advanced adversary would spend gathering reconnaissance and finding a vulnerability to exploit. The limited timeframe the red team has attacking any one system is a combination of capacity and funding along with scheduling. With regards to scheduling, many commanders only have a short duration period they can set aside from

their "real world missions" for test and training exercises. This restriction naturally limits the time a red team can attack their systems unless the commanders approve a persistent red team where a red team is allowed to persist on the network for longer durations.

The DoD recognizes the limited time allotted to the red team is unrealistic to the time an adversary would have to attack the system. Red teams are often white carded into positions or given credentials due to the lack of time a red team has on a system. Military personnel who don't understand cyber and the red team limitations often immediately claim foul to these actions believing the red team was given an unfair advantage for success. As a result, many military leaders dismiss the red team findings based on the belief the red teams cheated.

Over the past several years, DOT&E has tried to implement the use of persistent red teaming on Combatant Command networks. DOT&E has established a Persistent Cyber Opposing Force (PCO) and asserts the PCO better represents the advanced nation-state threat while utilizing scarce Red Team resources more efficiently. The 2016 DOT&E Annual Report states, "PCO activities have identified, and rapidly addressed, serious vulnerabilities that had not previously been discovered during more than a decade of short-duration, less realistic exercise events" (Director O. T., 2016 Cybersecurity Annual Report, 2016). However, the use of the PCO still appears to be limited by the Combatant Commander's willingness to allow consistent red teaming of networks which are simultaneously being used to support critical live missions. From publicly released information, U.S. Pacific Command (USPACOM) and U.S. Northern Command (USNORTHCOM) are the only two Combatant Commands which allow PCO activity (Director O. T., 2016 Cybersecurity Annual Report, 2016).

2.9. Consistency & Standards

DOT&E also documented an inconsistency of capability among the red teams resulting from varying backgrounds, experience, retention levels, and individual skills (Director O. T., Department of Defense (DoD) Cyber Red Teams Deficiencies, 2016). Although there is no need for each red team to have the same skills, each red team does

need to have enough capabilities to portray validated threats. Currently, not all red teams operate at this level. DOT&E internally recognizes there are some red teams which can only work at an elementary level, well below the capabilities of advanced nation-state threats.

The cyber community has not defined standards for a red team which would help ensure some level of uniformity across them. Government leadership judges red teams by their ability to gain access to a system and the damage they can cause. Neither are suitable criteria. Standards are needed that specify the fidelity which a red team mirrors adversarial behavior.

2.10. Network IP-based Focused

DoD Cyber Red Teams have mostly focused on Internet Protocol (IP)-based networks and rightly so as the big enterprise networks provide attackers with low hanging fruit. As the large enterprise networks become better defended and adversaries evolve their skills, other specialized systems will increasingly become critical to protect. Currently, DoD red teams are unable to conduct attacks on specialized interfaces and protocols due to a lack of these skill sets (Director O. T., Department of Defense (DoD) Cyber Red Teams Deficiencies, 2016). For example, Link 16 is an encrypted, jam-resistant, nodeless tactical digital link network used by DoD and NATO (Thales Group, n.d.).

DOT&E has created an Advanced Cyber Opposing Force (ACO) to assist DOD Red Teams with more advanced skills (Director O. T., 2016 Cybersecurity Annual Report, 2016). The success and exact mission of the ACO are unclear from the publicly releasable information so there can be no determination if the ACO is a potential solution to this recognized deficiency.

2.11. Safely Conducting Attacks

Especially when testing Industrial Control Systems (ICS), Supervisory Control and Data Acquisition (SCADA) networks, along with other critical operational systems, red teams need a way to conduct attacks safely. Most red teaming is severely limited or not conducted because testers cannot safely conduct the attacks against these systems (Director O. T., Department of Defense (DoD) Cyber Red Teams Deficiencies, 2016). The safety constraint drastically limits what a red team can attempt. The result is not truly knowing the effects the adversary can implement.

Virtual environments along with cyber test ranges have been discussed and debated for years. There is some use of virtual environments and ranges across the DoD, but these facilities are often very limited themselves toward mimicking realistic conditions. Inconsistent and uncertain funding streams make building and sustaining the ranges difficult. Currently, the DoD separates testing and training ranges per direction from the FY15 National Defense Authorization Act which established an Executive Agent for cyber training ranges and an Executive Agent for cyber testing ranges (Representatives, 2014). Many including DOT&E believe combined test and training uses of the ranges are needed, and the two separate Executive Agents with different responsibilities and funding may hinder their development (Director O. T., 2016 Cybersecurity Annual Report, 2016).

2.12. Ownership & Lack of Authorities

There is no central ownership of DoD Cyber red teams. Each red team reports up through their chain of command. There are some pros with this structure, but the lack of one authority overseeing all DoD red teams does negatively affect collaboration, uniformity, and efficiency. Without one authority enforcing collaboration, red teams do not want to share tactics and tools for fear of overuse and burn out which would allow the defenders to create signatures to prevent the attacks. Additionally, since collaboration is limited, each red team ends up utilizing their tactics and tools which create variation across red team skill sets. Finally, the lack of one authority also results in inefficiency as

each red team invests in building identical tools from the absence of collaboration. Centralized ownership has been discussed and debated within DoD for years with Cyber Command or DOT&E being potential homes for the red teams, but DoD has no planned actions to move the red teams under one authority.

Red teams typically do not have authorities to attack and operate on connected networks owned by different organizations, limiting their abilities to portray realistic adversaries. In today's DoD which is highly interconnected, there remains a wall between DoD and the Intelligence Community (IC) networks. The Intelligence Community does not allow DoD red teams to traverse their networks to attack DoD systems although an adversary could potentially do this. Additionally, IP address space is typically severely constrained during testing limiting attack paths available to the red teams. Finally, red teams cannot touch public cellular networks to attack mobile devices as adversaries would resulting in another limitation.

3. Addressing Deficiencies Through Systems Engineering

Designing, building, and sustaining DoD cyber red teams is a growing money pit running astray with no sound engineering plan. To date, DoD has created red teams in an ad-hoc manner resulting in a lack of efficiency while only being marginally effective in meeting DoD's overall need. Throwing additional money and bodies at this problem will not be able to address all the chronic deficiencies identified above. DoD needs to recognize an unstainable money pit has emerged from the ad-hoc approach for a capability that continues to become more critical towards ensuring mission success.

DoD knows the benefits of applying systems engineering and have published reports documenting systems engineering successes. Systems engineering benefits include cost avoidance, risk avoidance, improved efficiency, and better products (Joseph P. Elm, 2013). A report written by the Software Engineering Institute at Carnegie Mellon, which is a Federally Funded Research and Development Center (FFRDC) sponsored by the DoD, documents the effectiveness of systems engineering best practices. The figure

below shows that projects deploying higher levels of systems engineering, measured by assessing the quantity and quality of system engineering products, delivered better project performance.

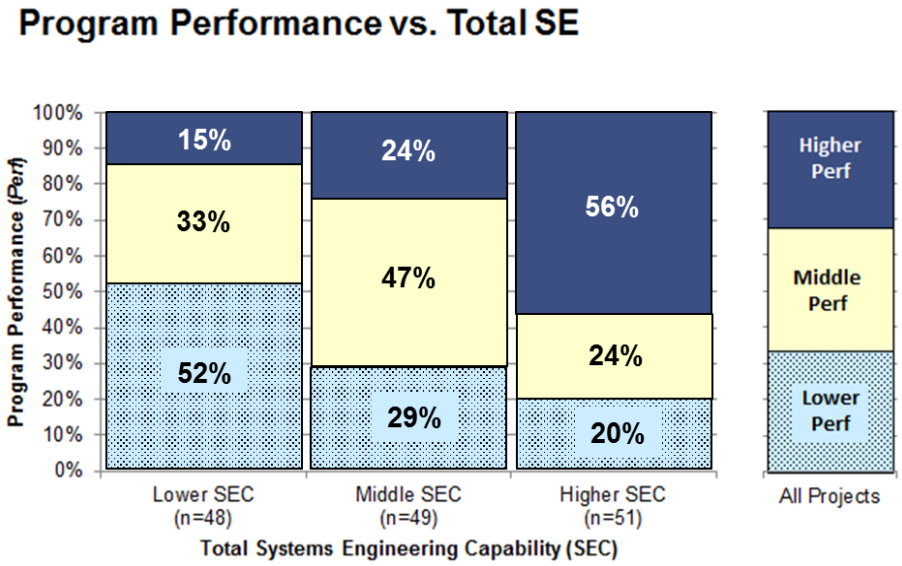

Figure 1: Program Performance vs. Total SE (Goldenson, 2012)

3.1. Systems Engineering

Systems Engineering (SE) implements an interdisciplinary approach to problem-solving. SE focuses on defining customer needs and required functionality from the beginning of the development cycle, documenting all requirements, exploring alternate solutions, designing, and validating the solution while continually considering the whole problem.

Systems engineers follow these basic core concepts: (What is Systems Engineering?, n.d.)

- Understand the entire problem before you try to solve it.
- Translate the problem into measurable requirements.
- Explore all feasible alternatives before selecting a solution.
- Consider the total system life cycle. The birth-to-death concept extends to maintenance, replacement and decommission.
- Test the total system before delivering it.

- Document everything.

Without a flexible, structured, and rigorous approach to building the DoD cyber red team capability, resources will continue to be wasted by developing incomplete solutions or worse, solving the wrong problems. Since the parameters that affect the red team problem definition are consistently changing, DoD needs to use the systems engineering process which is adaptable to changing requirements.

3.2. Viewing DoD Cyber Red Teams as a System

To those without extensive systems engineering expertise, viewing the DoD cyber red team capability as a system which engineers can design and optimize performance with the systems engineering process is a novel thought. However, applying systems engineering towards building successful team capabilities is not original. Systems engineers have previously used baseball as an analogy to describe systems engineering principles. Moneyball documented perhaps the most widely known example where the Oakland Athletics' management used systems engineering principles to build championship teams despite having a minimum payroll (Valerdi, 2008). System engineers can cite additional examples as well. Alessandro Migliaccio and Giovanni Iannone presented how systems engineering can be used to optimize the performance of a sports team at an International Council on Systems Engineering (INCOSE) conference in 2014 (Iannone, 2014).

Just as a baseball team can be considered a system (Clotier, 2016), the cyber red team capability can also be. The accepted definition of a system is "an integrated composite of people, products, and processes that provide a capability to satisfy a stated need or objective" (College, 2001). The DoD cyber red team capability certainly meets this definition. The subsystems that comprise the red team capability system consists of the threat intelligence (threat profiles), the processes (tactics, techniques, and procedures), the hacking tools used, and the personnel. The output of the system is the validated threat portrayal which emulates a potential adversary's attack tactics against a targeted mission or capability. Figure 2 below displays the red team capability system.

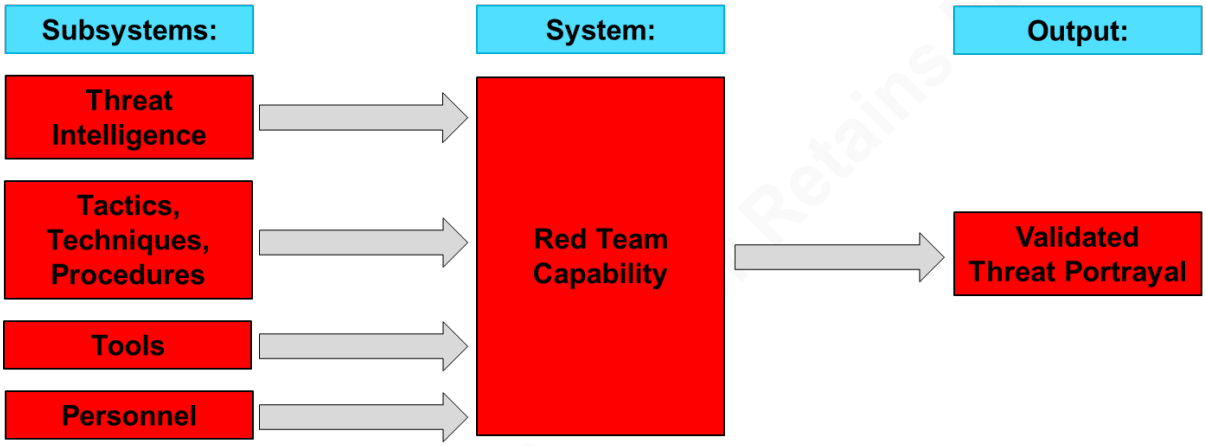

Figure 2: The Red Team Capability System

The Office of the Deputy Assistant Secretary of Defense for Systems Engineering (ODASD(SE)) is the focal point for all DoD systems engineering activity. As stated on their website, "ODASD(SE) works to ensure the Department of Defense applies effective systems engineering principles and strong technical management in defense acquisition programs" (ODASD(SE) Organization, 2016). Since the red team capability is not an acquisition program, DoD systems engineering expertise is not being utilized towards building the red team capability. Considering how systems engineering has been successfully used to increase the performance of sports teams, DoD should expand ODASD(SE)'s mission to applying effective systems engineering principles to increase the performance of cyber red teams which are critical to ensuring mission success.

3.3. The Systems Engineering Process

DoD systems engineering process is a group of technical and management processes. Figure 3 below is the 2014 DoD Systems Engineering Process Model (Defense Acquisition University, 2017).

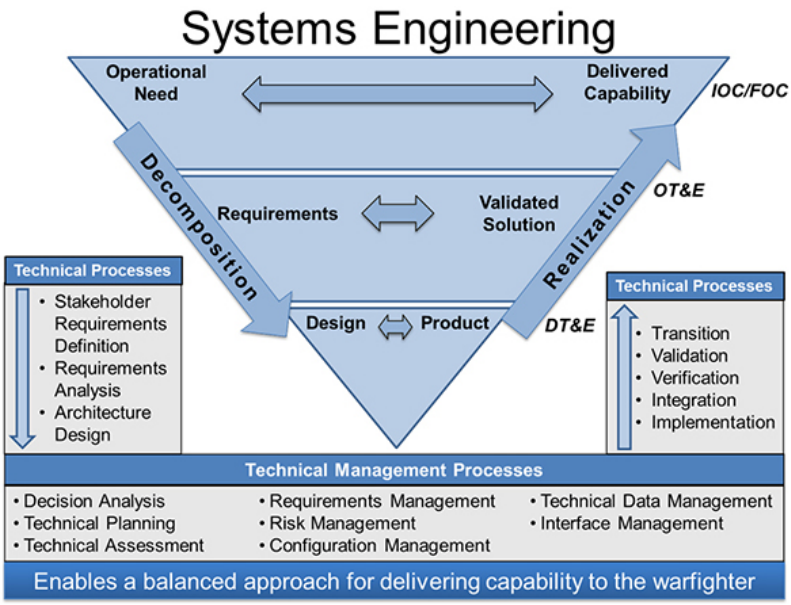

Figure 3: The 2014 DoD Systems Engineering Process Model

The Defense Acquisition University (DAU) ACQuipedia website gives a detailed explanation of the DoD Systems Engineering process (Defense Acquisition University, 2017). Here is a brief description of the first three technical processes from that website as a discussion of the full implementation of the systems engineering process to DoD cyber red teams is beyond the scope of this introductory paper.

The stakeholder requirements definition is the first and a critical step in the systems engineering process. Table 1 below shows requirement development and management has the second strongest positive impact on project performance next to overall project planning than any other systems engineering capability.

Table 1: Summary of Project Performance versus Systems Engineering Capabilities (Goldenson, 2012)

Systems Engineering Capability	Gamma	Relationship
Total Deployed SE	+ 0.49	Very Strong Positive
Project Planning	+ 0.46	Very Strong Positive

Requirements Development and Management	+ 0.44	Very Strong Positive
Verification	+ 0.43	Very Strong Positive
Product Architecture	+ 0.41	Very Strong Positive
Configuration Management	+ 0.38	Strong Positive
Trade Studies	+ 0.38	Strong Positive
Project Monitoring and Control	+ 0.38	Strong Positive
Product Integration	+ 0.33	Strong Positive
Validation	+ 0.33	Strong Positive
Risk Management	+ 0.21	Moderate Positive
Integrated Product Team Utilization	+ 0.18	Weak Positive

The requirements definition step takes all inputs from users and stakeholders and translates them into requirements. Time and thought must be taken to fully define and articulate what is needed in the form of requirements so engineers can design and build the "right" system. The requirements must be understandable, unambiguous, compressive, complete and concise.

Once requirements are defined, engineers put them through an analysis process which results in a better understanding of what the system must do, in what ways it can do it, and the priorities and conflicts associated with lower-tiered functions to higher and other lower-tiered functions. This step provides output essential to optimizing the solution. After engineers complete the analysis, they reconsider and refine the requirements followed by another round of analysis. Engineers reiterate the loop until they reach a consensus while compromising on any conflicts.

The architecture design process translates the output from the stakeholder requirements definition and the requirement analysis processes into alternate design solutions. Engineers should consider all options initially at the beginning of this step. As engineers follow the systems engineering process, they will compare the options in selecting an optimal solution.

3.4. Poor and Missing Requirements

Delivering an effective system through the systems engineering process hinges on the first steps of requirement definition, analysis, and management. The adage, "garbage in, garbage out" holds true. If engineers do not spend the time at the beginning defining and refining the requirements, the outputted system will likely fall short of expectations and may be unbuildable, nonfunctional, or unsustainable. Project management consultancy services report 80% of new products fail due to poor requirements (Stevbros Training and Consultancy, 2017).

Although the DoD widely knows this, time after time they jump right into building a system without thoroughly identifying what exactly they need to build out of urgency for the capability. A recent example of a DoD acquisition program that according to Senator John McCain has a shameful list of failures is the Navy's Littoral Combat Ship. Senator McCain in a speech on the Senate floor stated undefined requirements as a key factor for the failures (McCain, 2014).

The deficiencies noted above in the red team capability is another prime example of the DoD building a system without proper requirement definition and analysis. Although there would still be trade-offs due to constraints, the above deficiencies could have been reduced if engineers completed sound requirement definition and analysis. In the absence of following a sound systems engineering approach, the DoD finds itself with an inadequate system which has potential to waste millions of dollars as the DoD attempts to apply band-aid solutions.

In DoD's defense, red team requirements are unchartered waters for the Department and are difficult to define. There is a noticeable lack of official strategic documents in the field of cyber red teaming (Pascal Brangetto, 2015). The shortage is likely a result of the DoD still being in the early phases of understanding cyber as a warfighting domain while trying to develop both offensive and defensive capabilities in this new domain. Since red team actions are dependent on knowing how the adversary will use cyber as a warfighting domain, it is understandable why red teaming strategic documentation is lacking and not high on the priority list.

3.5. Defining Requirements

If DoD wants to address the red team deficiencies efficiently, they need to start at the beginning of the systems engineering process and establish the requirements they need for the red team capability. The Systems Engineering Guide states, "requirements define the capabilities that a system must have (functional) or properties of that system (non-functional) that meet the users' needs to perform a specific set of tasks (within a defined scope)" (MITRE, Systems Engineering Guide, 1997). During this process, all aspects of the system lifecycle need to be considered to include operations, performance, sustainability, costs, training, quality, and certification.

Requirement gathering is an essential to project success, so engineers need to understand what makes a good requirement (Haughey, n.d.). Each requirement should have the following characteristics (MITRE, Systems Engineering Guide, 1997):

- Traceable back to an operational need
- Unambiguous
- Specific and singular
- Measurable either quantitatively or qualitatively
- Testable
- Consistent without conflict with any other requirement
- Design-free stating what the system shall do, not how

3.6. The Real Need and Mission

As the requirements definition process begins, engineers must completely understand the real need that the DoD cyber red team capability is intended to address. Often, a perceived need is identified rather than the real need which leads engineers down the path of solving the wrong problem. A perceived need is based on the awareness that something is wrong, something is lacking, or something can be improved upon. A real need lies behind perceived needs (Guide to the Systems Engineering Body of Knowledge, 2015). For example, a perceived need could be the need to improve cancer detection rates where the real need would be the need for early cancer detection and

identification in patients. Accurately identifying the real need versus perceived needs will keep the requirement definition process focused.

Once the real need is determined, DoD can formulate the red team's mission. The mission should state the red team's purpose and serves as the foundation for determining what the red team should and shouldn't do. Currently, there is no concise and accepted red team mission statement across the DoD. As covered in Section 1, the definition of a red team and its purpose is documented but references multiple potential missions from testing to training to supporting cyber defense activities. The November 16, 2016 DOT&E memo requests DoD Services, Cyber Command, the National Security Agency, and the Defense Information Services Agency, to develop doctrine defining cyber red team missions which still has not happened. (Director O. T., Department of Defense (DoD) Cyber Red Teams Deficiencies, 2016). The lack of a well-formulated mission creates conflicting and unmeetable requirements given DoD's funding constraint.

DoD cyber red teams need a stated mission and shouldn't be asked to perform activities outside of their mission. Without a clear mission, the red teams are asked to "be everything." Per DOT&E's Procedures for Operational Test and Evaluation of Cybersecurity, a National Security Agency certified red team's mission should be to "act as a cyber aggressor presenting multiple cyber intrusion vectors consistent with the validated threat" (Director O. T., Procedures for Operational Test and Evaluation of Cybersecurity in Acquisition Programs, 2014). They shouldn't be trainers who are asked to increase or decrease "noise" to see if the defenders can catch them. They shouldn't be penetration testers who seek to identify and exploit any vulnerability for the sake of identifying and exploiting any vulnerability. Their actions should include those resulting from the tactics, techniques, and procedures of the validated threat they are portraying.

3.7. The Path Forward

Once DoD agrees on the real need and mission of cyber red teams, engineers can start documenting requirements. Stakeholder requirement definition is a lengthy process, and DoD needs to invest the time and resources in completing it. Using the systems engineering process, engineers start the definition process with documenting the scope of the red team capability by identifying the needs, goals and objectives, business case, high-level operational concepts, customer input, constraints, schedules, budgets, authority, and responsibility. Next, they develop operational concepts which are scenarios for how DoD would use the red team capability. Finally, engineers identify the interfaces between the red team and the world clarifying boundaries, inputs, and outputs. Using all this information, they can then begin writing system level requirements followed by subsystem requirements.

Once an initial pass is complete, the stakeholder requirements feed the analysis process that starts an iterative process. If completed thoroughly, requirements will be defined which will allow engineers to design the red team capability that eliminates the chronic deficiencies identified above. For example, a red team personnel subsystem requirement would likely state "each red team member shall attend x days of training per year." This requirement feeds up to the system level requirement which says that red teams must stay current with the latest attack methods of adversaries. The requirement also influences capacity and funding requirements. As engineers refine more and more requirements, an optimal design for the capability will emerge which will guide DoD on their investments in building a DoD cyber red team capability.

4. Conclusion

Chronic deficiencies with DoD cyber red teams are a result of DoD's failure to define, design, develop, and sustain the capability through a sound systems engineering process. The deficiencies produce a severely limited essential capability and result in unsuitable mission risk for DoD when operating in a contested cyber environment. Currently, red team mission and requirements are not defined. Without them, DoD

continues to spend millions of dollars without a plan detailing how to build the capability. Following a systems engineering process would force DoD to identify red team requirements while designing a capability which is feasible, capable, and sustainable.

Cyber security experts both inside and outside of DoD have noted the severe limitations of red teams and their effect on DoD's ability to defend itself against advanced persistent cyber attacks for years. DoD leadership often cites a lack of resources (funding to hire and train additional workforce) as the cause of the deficiencies and requests additional funding to fix them. However, a monetary based solution is not feasible nor scalable as the demand for red team capacity and capability continue to grow.

The current DoD Red Team capability is ad-hoc, being built in pieces when DOD identifies a critical need and funding. The lack of a structured approach results in many inefficiencies which magnify the deficiencies. The ad-hoc process is unable to meet DoD's needs and is becoming a financial drain as leadership attempts to throw more money towards patching holes in an overall failing dam.

The absence of a sound engineering approach towards building the red team capability becomes apparent as each identified deficiency is analyzed. By treating red team capability as a complex system and implementing a systems engineering approach to the design and management of this system, DoD can make substantial progress towards reducing the red team deficiencies they are currently facing. The most efficient way of tackling the deficiencies is to start back at the beginning and use the systems engineering process to define the requirements of the red team capability. Requirement definition which DoD never completed is the first and most critical step toward building an efficient and effective solution. Without a structured approach to solving this problem, the current ad-hoc method which demands unrealistic amounts of resources will continue to result in red team deficiencies and unacceptable risk to our national security.

5. References

Board, D. o. (2017, February). *Task Force On Cyber Deterrence.* Retrieved from Office of the Under Secretary of Defense for Acquisition, Technology and Logistics: http://www.acq.osd.mil/dsb/reports/2010s/DSB-CyberDeterrenceReport_02-28-17_Final.pdf

Buchanan, C. S. (2010, January 5). *Cyber Space Security: dispelling the myth of Computer Network Defense by true Red Teaming the Marine Corps and Navy.* Retrieved from Defense Technical Information Center: http://www.dtic.mil/dtic/tr/fulltext/u2/a536674.pdf

Chabrow, E. (2009, May 28). *A Red Team Primer.* Retrieved from Gov Info Security: http://www.govinfosecurity.com/interviews/red-team-primer-i-244

Clotier, D. R. (2016, July 25). *Is a Baseball Team a System?* Retrieved from University of South Alabama: http://www.southalabama.edu/colleges/engineering/dsc-se/blog/16.0725se_baseball.html

College, D. o. (2001). *Systems Engineering Fundamentals.* Fort Belvoir: Defense Acquisition University Press.

Congress, U. S. (2016). *National Defense Authorization Act for Fiscal Year 2016.* Retrieved from U.S. Government Publishing Office: https://www.gpo.gov/fdsys/pkg/BILLS-114s1356enr/pdf/BILLS-114s1356enr.pdf

Cordell, C. (2016, December 1). *OPM lays out pay scale, incentives for federal cyber pros.* Retrieved from Federaltimes: http://www.federaltimes.com/articles/gsa-finalizes-value-driven-human-capital-hr-systems-contracts

Defense Acquisition University. (2017, March 1). *Systems Engineering Process*. Retrieved from Defense Acquisition University ACQuipedia: https://dap.dau.mil/acquipedia/Pages/ArticleDetails.aspx?aid=9c591ad6-8f69-49dd-a61d-4096e7b3086c

Derene, G. (2008, June 29). *Inside NSA Red Team Secret Ops With Government's Top Hackers.* Retrieved from Popular Mechanics: http://www.popularmechanics.com/technology/security/how-to/a3342/4270420/

Director, O. T. (2009, January). *Procedures for Operational Test and Evaluation of Information Assurance in Acquisition Programs.* Retrieved from Defense Acquisition University (DAU): https://acc.dau.mil/adl/en-US/649704/file/71936/DOTE%20Procedure%20for%20OTE%20of%20IA_21Jan09.pdf

Director, O. T. (2010, November). *Clarification of Procedures for Operational Test and Evaluation of Information Assurance in Acquisition Programs.* Retrieved from http://www.dote.osd.mil/pub/policies/2010/20101104Clarification_ofProcedures_forOTE_ofIA_inAcqProgs.pdf

Director, O. T. (2013, February). *Test and Evaluation of Information Assurance in Acquisition Programs.* Retrieved from http://www.dote.osd.mil/pub/policies/2013/2013-02-01_TE_of_IA_in_Acq_Programs(6079).pdf

Director, O. T. (2014, August). *Procedures for Operational Test and Evaluation of Cybersecurity in Acquisition Programs.* Retrieved from The Office of the Director, Operational Test and Evaluation: http://www.dote.osd.mil/pub/policies/2014/8-1-14_Procs_for_OTE_of_Cybersec_in_Acq_Progs(7994).pdf

Director, O. T. (2016, December). *2016 Cybersecurity Annual Report.* Retrieved from The Office of the Director, Operational Test and Evaluation: http://www.dote.osd.mil/pub/reports/FY2016/pdf/other/2016cybersecurity.pdf

Director, O. T. (2016, November). *Department of Defense (DoD) Cyber Red Teams Deficiencies.* Retrieved from Office of the Director, Operational Test & Evaluation.

Goldenson, J. P. (2012, November). *The Business Case for Systems Engineering Study: Results of the Systems Engineering Effectiveness Survey.* Retrieved from Software Engineering Institute Carnegie Mellon University: http://resources.sei.cmu.edu/asset_files/SpecialReport/2012_003_001_34067.pdf

Guide to the Systems Engineering Body of Knowledge. (2015, June 29). *Stakeholder Needs and Requirements*. Retrieved from Guide to the Systems Engineering Body of Knowledge: http://sebokwiki.org/wiki/Stakeholder_Needs_and_Requirements

Harold F. Tipton, M. K. (2010). *Information Security Management Handbook.* Boca Raton: Auerback Publications.

Harris, S. (2015, December 16). *Pentagon Memo: U.S. Weapons Open to Cyberattacks.* Retrieved from the Daily Beast: http://www.thedailybeast.com/articles/2015/12/16/pentagon-memo-u-s-weapons-open-to-cyber-attacks.html

Haughey, D. (n.d.). *Requirements Gathering 101*. Retrieved from Project Smart: https://www.projectsmart.co.uk/requirements-gathering.php

Iannone, A. M. (2014). *A Systems Engineering Approach to the Challenges of Sports Business.* Retrieved from UK Chapter International Council on Systems Engineering: https://incoseonline.org.uk/Documents/Research/Alessandro_posterV1.pdf

Joseph P. Elm, D. D. (2013). *Quantifying the Effectiveness of Systems Engineering.* Retrieved from Defense Technical Information Center: http://www.dtic.mil/ndia/2013/system/W131023_ELM.pdf

Matthews, W. (2016, July 13). *Unpacking DoD's Cyber Strategy and $6.7B Spending Plan.* Retrieved from Govtech Works: https://www.govtechworks.com/unpacking-dods-cyber-strategy-and-6-7b-spending-plan/#gs.COd4EXM

Maunual, C. o. (2013, February 28). *Department of Defense Cyber Red Team Certification and Accreditation.* Retrieved from Joint Chiefs of Staff: http://www.jcs.mil/Portals/36/Documents/Library/Manuals/m651003.pdf?ver=2016-02-05-175711-083

McCain, S. J. (2014, April 9). *Remarks By Senator John McCain On The Navy's Troubled Littoral Combat Ship Program*. Retrieved from Senator John McCain: https://www.mccain.senate.gov/public/index.cfm/floor-statements?ID=5DD94059-3E13-400E-ACF9-06632038F9E9

MITRE. (1997). *Systems Engineering Guide*. Retrieved from Eliciting, Collecting, and Developing Requirements: https://www.mitre.org/publications/systems-engineering-guide/se-lifecycle-building-blocks/requirements-engineering/eliciting-collecting-and-developing-requirements

MITRE. (1997). *Systems Engineering Guide*. Retrieved from Analyzing and Defining Requirements: https://www.mitre.org/publications/systems-engineering-guide/se-lifecycle-building-blocks/requirements-engineering/analyzing-and-defining-requirements

ODASD(SE) Organization. (2016, August 25). Retrieved from Office of the Deputy Assistant Secretary of Defense (ODASD) Systems Engineering: http://www.acq.osd.mil/se/org.html

Officer, A. S. (2015, November 10). *DoD 8570.01-M Information Assurance Workforce Improvement Program - Incorporating Change 4.* Retrieved from Defense Technical Information Center: http://www.dtic.mil/whs/directives/corres/pdf/857001m.pdf

Officer, O. o. (2016, February). *United States Department of Defense Fiscal Year 2017 Budget Request.* Retrieved from Department of Defense: http://comptroller.defense.gov/Portals/45/Documents/defbudget/fy2017/FY2017_Budget_Request_Overview_Book.pdf

Pascal Brangetto, E. C. (2015). *Cyber Red Teaming.* Tallinn: NATO Cooperative Cyber Defense Centre of Excellence.

Representatives, C. o. (2014, December). *Carl Levin and Howard P. "Buck" Mckeon National Defense Authorization Act For Fiscal Year 2015.* Retrieved from U.S. Government Publishing Office: https://www.gpo.gov/fdsys/pkg/CPRT-113HPRT92738/pdf/CPRT-113HPRT92738.pdf

Serbu, J. (2016, February 2). *Pentagon report says most military exercises don't account for cyber threats.* Retrieved from Federal News Radio: https://federalnewsradio.com/defense/2016/02/pentagon-report-says-military-exercises-dont-account-cyber-threats/

Sternstein, A. (2016, March 16). *The Military's Cybersecurity Budget in 4 Charts.* Retrieved from Defense One: http://www.defenseone.com/business/2015/03/militarys-cybersecurity-budget-4-charts/107679/

Stevbros Training and Consultancy. (2017). *80% New Products Fail, 70% Of Software Projects Fail Due To Poor Requirements*. Retrieved from Stevbros Training and Consultancy: http://stevbros.com/blog/80-new-products-fail-70-of-software-projects-fail-due-to-poor-requirements.html

Takala, R. (2015, December 17). *Pentagon's cyberwarriors aren't 'keeping pace' with adversaries.* Retrieved from Washington Examiner: http://www.washingtonexaminer.com/pentagons-cyberwarriors-arent-keeping-pace-with-adversaries/article/2578619

Thales Group. (n.d.). *Link 16 Operational Overview*. Retrieved from Thales Group: https://www.thalesgroup.com/sites/default/files/asset/document/White%20Paper%20-%20Link%2016%20Overview.pdf

Valerdi, C. B. (2008). *Measuring Systems Engineering Success: Insights from Baseball.* Retrieved from Massachusetts Institute of Technolgy: https://dspace.mit.edu/bitstream/handle/1721.1/84544/CP_080615_BlackburnValerdi_INCOSE08_P372.pdf?sequence=1

What is Systems Engineering? (n.d.). Retrieved from International Council on Systems Engineering Website: http://www.incose.org/AboutSE/WhatIsSE