# The Sliding Scale of Cyber Security

The Sliding Scale of Cyber Security is a model for providing a nuanced discussion to the categories of actions and investments that contribute to cyber security.

# The Sliding Scale of Cyber Security

## A SANS Analyst Whitepaper

*Written by:*
*Robert M. Lee*

August 2015

# Executive Summary

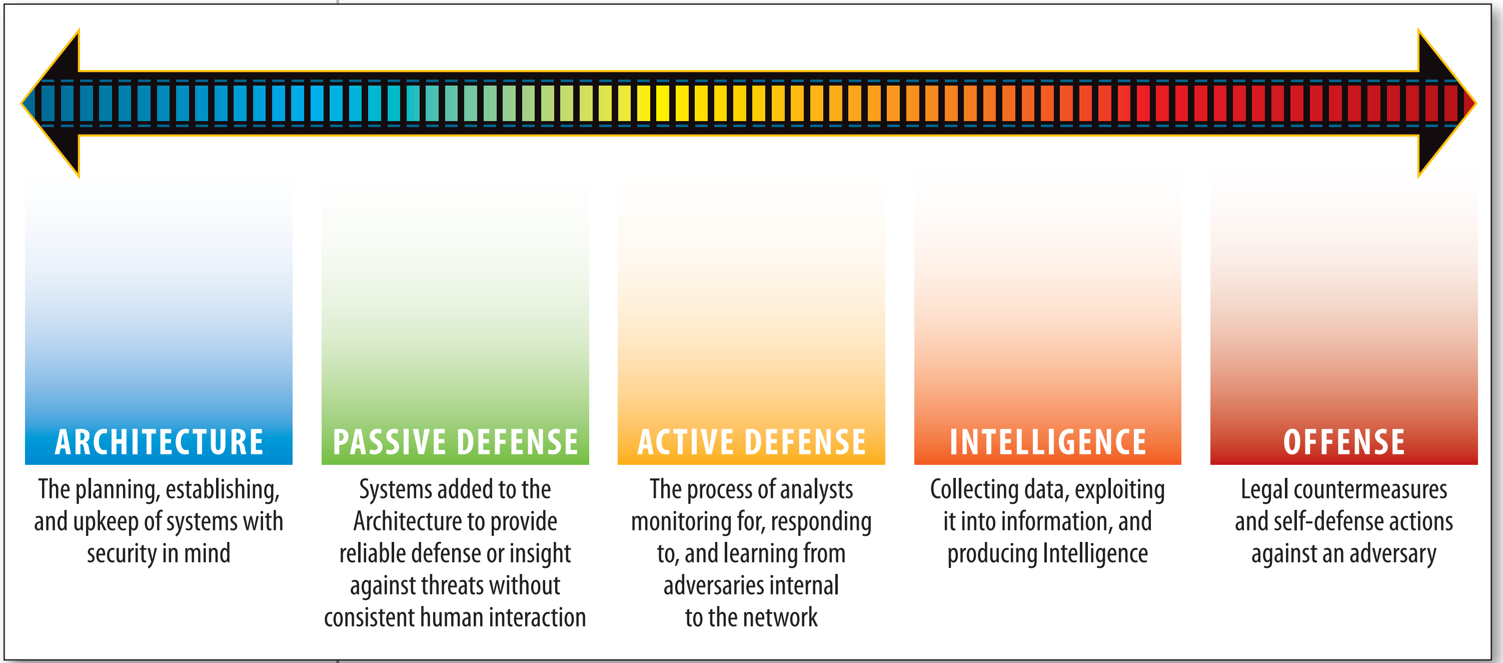
The Sliding Scale of Cyber Security is a model for providing a nuanced discussion to the categories of actions and investments that contribute to cyber security. The five categories in the scale are Architecture, Passive Defense, Active Defense, Intelligence, and Offense. The continuum between the five categories helps visualize that not all actions are static or easily defined. Understanding these interconnected categories that contribute to cyber security helps individuals and organizations better understand the purpose and impacts of their resource investments, establish a maturity model for their security program, and break down cyber attacks to identify root cause analysis in a way that encourages growth by defenders over time. The understanding of each phase helps individuals and organizations understand that categories on the left hand side of the scale build the appropriate foundation that make the other actions of the scale more obtainable, useful, and less resource intensive. The goal should be to invest resources starting on the left hand side of the scale and address those issues to achieve a proper return on investment before allocating significant resources to the other categories. This approach recognizes the increasing cost of success to adversaries facing properly prepared organizations and empowers defenders to engage security in a manner that evolves over time.[1]

[1] The author would like to thank Dr. Thomas Rid, Michael Assante, Lenny Zeltser, and Tim Conway as a few of the individuals that have helped inspire, constructively criticize, and add to the Sliding Scale of Cyber Security and this paper.

# The Sliding Scale of Cyber Security

The Sliding Scale of Cyber Security[2] is a way to add nuance to the discussion of cyber security by categorizing the actions, competencies, and investments of resources that organizations can make to defend against threats. The model serves as a framework for understanding what actions contribute to cyber security. The model's scale is useful in a number of ways, which include explaining technical security matters to non-technical persons, prioritizing and tracking the investment of resources and skillsets, measuring security posture, and confirming accuracy of incidents' root cause analysis.

The model is structured into five categories illustrated in Figure 1: Architecture, Passive Defense, Active Defense, Intelligence, and Offense. These categories will be discussed in this paper to highlight their differences as well as their interconnected nature.



**ARCHITECTURE**
The planning, establishing, and upkeep of systems with security in mind

**PASSIVE DEFENSE**
Systems added to the Architecture to provide reliable defense or insight against threats without consistent human interaction

**ACTIVE DEFENSE**
The process of analysts monitoring for, responding to, and learning from adversaries internal to the network

**INTELLIGENCE**
Collecting data, exploiting it into information, and producing Intelligence

**OFFENSE**
Legal countermeasures and self-defense actions against an adversary

*Figure 1. The Sliding Scale of Cyber Security*

[2] The Sliding Scale of Cyber Security is based on currently unpublished research by the author for his PhD thesis. However, due to its inclusion in multiple SANS Institute classes it is worthwhile to write a whitepaper here discussing it. This should not be seen as an academic level defense of the model but instead as a practical guide.

# Non-Static and Non-Equally Important Categories

The Sliding Scale of Cyber Security provides a framework for individuals and organizations to take part in a discussion on the types of resource and skill investment that contribute to cyber security. The five categories of Architecture, Passive Defense, Active Defense, Intelligence, and Offense work together to enhance cyber security, but they are not static or equally weighted.

The sliding scale aspect of the model illustrates that some actions in each category can be closely related to adjacent categories. For example, patching vulnerabilities in software would be in the Architecture category, but patching is farther right on the scale, still in Architecture but closer to the Passive Defense category, than engineering the system. Yet, no action in Architecture could reasonably be seen as an Active Defense, Intelligence, or Offense based activity. Another example would be that of Intelligence operations. An Intelligence operation that is conducted in the adversary network would be closer to an Offense action, and more quickly converted to one, than collecting and analyzing open source information. Likewise, collecting, analyzing, and producing Intelligence off of incident response data in the form of Threat Intelligence is closer to Active Defense, where analysts would consume the Intelligence for the purpose of defense.

*All the categories of the sliding scale are important, but the expected return on investment should guide how organizations implement security and when they focus on another category.*

The weight of each category is not equal in its contributions towards security. The clearest example of this is the discussion of Architecture compared to Offense. Actions taken to engineer and implement systems with security in mind will drastically increase the defensive posture of those systems. The return on investment through those actions would be significantly higher than conducting Offense for the same purposes of security. A sufficiently advanced and determined adversary will always find a means to bypass a well-established Architecture. Thus, the focus of investments cannot be on the Architecture alone. All the categories of the sliding scale are important, but the expected return on investment should guide how organizations implement security and when they focus on another category. As an example, an organization that has a poorly maintained Architecture and Passive Defenses would find less value out of Active Defenses and should not pursue Intelligence or Offense without remedying the fundamental issues first.

The goal of achieving cyber security should be obtained through establishing a foundation and culture for security that expands over time. This allows defenders to better themselves and their defense posture in the face of threats and challenges. This reveals another potential use for the scale: a model for the progression of security maturity in an organization. Organizations should focus on achieving the appropriate foundation from the categories on the left hand side of the scale before investing in the ones further to the right. Investing in Architecture appropriately builds the foundation for effectively applying Passive Defenses on top of the Architecture and achieve more benefit out of those investments. Likewise, Active Defense is more achievable and efficient when done in an environment with proper Architecture and Passive Defenses. Conducting Active Defense actions, such as network security monitoring or incident response, is more difficult and costly without that foundation. The aspect of cost highlights the return on investment of the categories as well as illustrated in Figure 2. As an example, executing Offense based actions in an effective way requires, at a minimum, the use of Intelligence which ultimately stems from understanding and appreciating the organization's Active Defense, Passive Defense, and Architecture actions well enough to truly know and target the threat. Yet, Offense based actions return a significantly lower value to security than properly structuring and implementing the Architecture. Thus it is highly encouraged for organizations to focus primarily on the left hand side of the scale starting with Architecture.

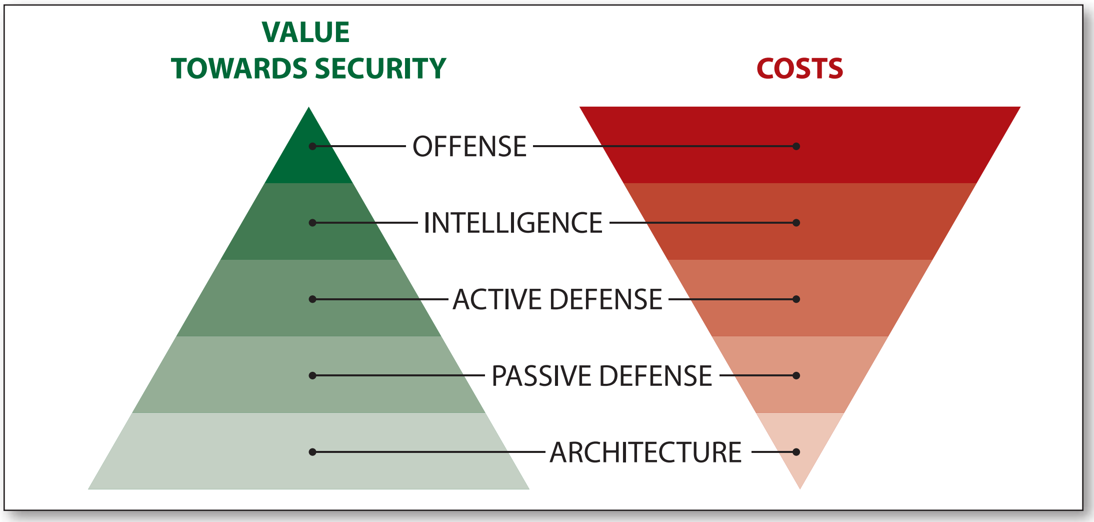


*Figure 2. Value Towards Security (Left) vs. Cost (Right)*

# Architecture

Arguably, one of the most important aspects of security is ensuring the proper architecture of the systems, which includes the mapping to the organization's mission, funding, and manning.[3] Architecture refers to ***the planning, establishing, and upkeep of systems with security in mind.*** Ensuring that security is designed into the system provides a foundation upon which all other aspects of cyber security can build. Additionally, the establishment of a proper Architecture aligned with the organization's needs causes the other categories to become more effective and less costly. For example, a network that is not properly segmented and maintained with software patches is wrought with more issues than the defenders can reasonably handle. Real threats that defenders should identify, such as adversaries inside the network, are lost in the noise of security issues, incidental malware, and network configuration problems that come with poorly implemented Architecture.

The starting point for Architecture is generally the planning, engineering, and design of the system to support the organization's needs. To accomplish this, the organization should first identify the business objectives supported by its IT systems, which might be different across companies and industries. Security of the systems should support these goals. Rather than aiming to defend against an adversary, the Architecture should accommodate normal operating conditions and emergency operating circumstances. This could include accidental malware infections, peaks in network traffic from misconfigured systems, and systems that cause disruption to each other simply by being placed within the same network. All of these conditions and more are typical of normal environments in today's networked infrastructure. Designing systems with these scenarios in mind helps maintain the confidentiality, availability, and integrity of the system in support of the organization's business needs.

ARCHITECTURE:

*the planning, establishing, and upkeep of systems with security in mind*

A secure production, acquisition, and implementation of the system is another key component to the Architecture category. It is important to secure each element in this chain to help ensure quality controls are put into place. In combination with maintaining the system, such as applying security patches, these actions make it easier to defend the system. The applications of software and hardware patches are sometimes mistaken as an action of defense; instead, they are steps that contribute to security but are not themselves defensive actions.[4] These actions and others associated with good Architecture also reduce the attack surface, to minimizing the opportunities adversaries have to gain access to a system and restricting their actions once access is gained.

[3] It is important to note that "systems" does not just refer to individual systems. Systems in this paper also refer to the system of systems whether they are networks or individual hardware or software components. This includes software such as applications and all the individual components of the broader system.

[4] The United States Department of Defense military services' have on multiple occasions referred to the architecting and patching of systems as a defensive role. This has often been referred to as Defense Cyber Operations (DCO). However, the architecting and patching of systems is required as a basic aspect of security; the action contributes to the ability to be able to defend the system but its purpose is the maintenance and operation of the system besides just adversary-based scenarios.

Through the course of this paper, sample models will be presented that can be used as a reference to implement the practices relevant to the category being discussed.

## Sample Architecture Models

- National Institute of Science and Technology (NIST) 800 Series
    - The NIST 800 series of special publications lay out numerous guidelines for securely acquiring, designing, implementing, and hardening systems.[5] The architecture of systems is driven by the desired outcome and need from the system however these publications give good guidance. Noteworthy is the 800-137 "Information Security Continuous Monitoring for Federal Information Systems and Organizations" which outlines that organizations should continuously and proactively monitor their networks for security violations and vulnerabilities to remedy them before they can be taken advantage of by an adversary.
- Purdue Enterprise Reference Architecture
    - The Purdue model is a good example of a high level architecture model for industrial control system networks.[6] The purpose is to show separation and segmentation that is needed amongst network segments by their function. Proper segmentation in networks can drastically increase the ability to secure them.
- Payment Card Industry Data Security Standard (PCI DSS)
    - PCI DSS is an information security standard for those organizations that handle specific types of credit cards and the data associated with them. Some of the standards relate to Passive Defenses, such as the implementation of a Firewall, but most of the standards relate to Architecture. As an example, the requirements to develop and maintain secure systems, encrypt data, restrict access to cardholder data, and to not use vendor-supplied default passwords are all actions that contribute to a proper Architecture.

[5] *NIST Special Publications 800 Series*

[6] Purdue Research Foundation, *A Reference Model for Computer Integrated Manufacturing (CIM)*. Purdue Research Foundation, 1989.

# Passive Defense

Once an organization has established the proper foundation for security through the investment in the Architecture category of this model it is then necessary to invest in Passive Defenses. Passive Defenses are added on top of a good Architecture to secure systems in the presence of an adversary. Adversaries, or threats, that have the opportunity, intent, and capability to do harm will eventually bypass a good Architecture – Passive Defenses are required.[7] Before discussing the definition of a Passive Defense it is important to realize the history of the term.

Traditionally there have been two forms of defense: passive and active. Many of the debates between the definitions of these two terms took place from the 1930's to the 1980's, well before the advent of the term "cyber."[8] The United States (U.S.) Department of Defense settled upon a definition for passive defense as: "measures taken to reduce the probability of and to minimize the effects of damage caused by hostile action without the intention of taking the initiative."[9] The translation of this to the field of cyber security has been a contention point for some academics, security practitioners, and military professionals. Although the definition itself may seem easy to understand the application to the normal operating environment of the cyber landscape requires more than a literal translation.

Understanding the intention, and not just the literal definition, helps the transition of the terms. First, the intent of passive defenses in the original debates was to provide a level of defense against an adversary without requiring the interaction of the military services themselves. An example would be the hardening of a bunker for protection against the dropping of a bomb. Although this may seem similar to applying a software patch to a system it is more akin to hardening the structure than defending against an adversary. It is not an aspect of defense but just an understanding of the typical environments systems find their selves in – patching is a maintenance action. Similarly, constructing barriers against the elements around a military conference room would not be considered "passive defenses against the wind" but instead just a normal required action for the environment. Likewise, it would be the strengthening of those barriers, the addition of decoys, camouflage, or other secondary aspects added on to the building that would constitute passive defenses. Lastly, the physical world suffers from attrition. Adversaries deplete their resources, such as one less bomb after one is dropped. In the digital world adversaries do not deplete resources in the same way; once a piece of malware is used if it is not detected and countered it can be re-used in a number of other campaigns. What adversaries do deplete though is time and the resources associated with it and their personnel. Depleting an adversary's resources, including their time to plan and achieve their objectives, is of critical importance to a defender. Passive Defenses help achieve this.

[7] Adversaries that have the opportunity, intent, and capability to do harm are known as threats. Reference:

[8] A major reason for these debates was the advent of long range bombers and intercontinental ballistic missiles. The RAND institute as well as early Air Force and Army publications and field manuals present a good look at this debate.

[9] *Joint Publication (JP) 1-02 Dictionary of Military and Associated Terms.* U.S. Department of Defense, March 2015.

In examining the history of passive defense terminology, it is possible to derive that there is a concept of add-ons to structures for the purpose of their protection. This concept of protection against an adversary and not necessarily enhancing the purpose of the system itself helps derive a definition for a passive defense. Passive defenses in the physical world also do not require constant interaction from personnel. Therefore the definition of a passive defense is: ***systems added to the architecture to provide consistent protection against or insight into threats without constant human interaction.*** Sample systems that get added to the architecture to add protection to assets, stop or limit well known security gaps, reduce the probability of interaction with a threat, or give insight into encounters with threats would be firewalls, anti-malware systems, intrusion prevention systems, anti-virus, intrusion detection systems, and similar traditional security systems. These systems require maintenance, turning, and care over time but not constant human interaction to make the systems work. They are consistent but not necessarily always effective. There are already a number of models in existence as well which give recommendations for the deployment of these systems.

PASSIVE DEFENSE:

*systems added to the architecture to provide consistent protection against or insight into threats without constant human interaction*

## Recommended Passive Defense Model

- Defense in Depth
    - One of the foundational concepts for applying passive defenses on top of the architecture of systems is the Defense-in-Depth model.[10] The model is a high level approach to ensuring passive defense systems are included throughout a network. It also ties directly into the concept of adversary attrition by layering defense in a way that adds to the time and effort adversaries must use to achieve their goals. However, this requires that the defense that is layered is not simply the same technique or circumvented in the same way which in return does not deplete an adversary's time.
- National Institute of Science and Technology (NIST) 800 Series
    - The NIST 800 Series supplies a number of documents that are useful for implementing passive defenses.[11] The 800-41, 800-83, and 800-94 publications are worth special attention for the discussion of firewalls, anti-malware systems, and intrusion prevention systems.
- NIST Cybersecurity Framework
    - The NIST Cybersecurity Framework puts forth a roadmap to help organizations defend themselves against threats.[12] It encompasses aspects of architecture, passive defense, and active defense but its main contributions are those recommendations for implementing and using passive defenses correctly. It is an outstanding reference model to help guide organizations.

[10] *Defense in Depth.* U.S. Department of Defense, n.d.

[11] *NIST Special Publications Series 800*

[12] *NIST Cybersecurity Framework*, Feb 2013

# Active Defense

Passive Defense mechanisms will eventually fail in the face of determined and well-resourced adversaries. Countering advanced and determined adversaries requires an active approach to security built on the premise that highly trained security personnel are needed to neutralize highly trained adversaries. It is vital to empower these trained security personnel and to have them operate within a good Architecture secured and monitored with well-placed Passive Defenses. However, Active Defense tends to be the subject of fierce debate and misuse in media and news outlets when discussed in the context of cyber security. Due to some of the misuse of the terminology it is important to cover the historical context of the term with some depth.

In the 1970s the term active defense was also heavily debated when used in context of land warfare by the U.S. Army. Army General William E. DePuy, the first commander of the Army Training and Doctrine Command, used the term in a 1974 paper discussing the 1973 Arab/Israeli war. In this context he was discussing the ability for the defending forces to be able to move instead of fighting in a static position: "What that means is that the defending force must possess the ability to move. It must engage in an active defense of the sector."[13] He later expanded upon his use of the term when he wrote: "The concept of active defense is to wear down the attacker by confronting him successively and continuously with strong combined arms teams and task forces fighting from mutually supported battle positions in depth throughout the battle area."[14] He placed the term in the 1976 Field Manual 100-5 "Operations." General DePuy noted later that the term "active defense" came under heavy criticism due to misunderstanding of the term in the Field Manual despite the fact that the document was credited with beginning a revolution of Army doctrine post-Vietnam. He stated "the term 'active defense' is mentioned only in passing in 100-5 as an adjective and seldom in 71-2. However in 71-1 'active defense' becomes the official descriptor of the defensive doctrine set forth in this family of manuals, although, as we shall see later, there is no consensus on the meaning of that term."[15]

[13] General William E. DePuy, *Implications of the Middle East War on U.S. Army Tactics, Doctrine and Systems.* 1974

[14] Ibid

[15] General William E. DePuy, *FM 100-5 Revisited.* November 1980

Despite the heavy debates around the term, which mimic present day debate of the terms use in cyber security, there was an official definition adopted by the U.S. military for the purposes of military action not in the context of cyber security.[16] The definition, relating to traditional warfare, is: "the employment of limited offensive action and counterattacks to deny a contested area or position to the enemy." The use of counterattack here has been misused as a literal translation into cyber security for "hack-back." Unfortunately this understanding does not accurately reflect the intention of the term. As it turns out, simply copying terms from physical domains of warfare into cyber security do not accurately portray the meaning of the terms. The meaning of the term active defense was always centered on maneuverability, the ability to incorporate military intelligence and indicators to identify an attack, respond to the attack or against the capability within the defensive zone or contested area, and the ability to learn from the encounter. This was highlighted within a RAND study from 1965 and the discussion of using integrated air defenses to track and destroy intercontinental ballistic missiles (ICBM) before they struck their target.[17] It is important to note for the discussion of cyber security that the focus of the "counterattack" was only inside the defended area and against the capability, not the adversary. I.e. a counterattack in cyber security would be more properly reflected in the concept of incident response where personnel "counterattack" by containing and remediating a threat. The incident responders or other personnel do not go on the offensive against adversaries in their networks or systems just as the ICBM active defense mechanisms of integrated air defenses destroyed missiles – not people or their cities.

ACTIVE DEFENSE:

*the process of analysts monitoring for, responding to, learning from, and applying their knowledge to threats internal to the network*

From this background and understanding of active defense a definition can be constructed for cyber security: ***the process of analysts monitoring for, responding to, learning from, and applying their knowledge to threats internal to the network.*** It is important to add the ending piece of "internal to the network" to further discourage misrepresentation of the definition into the idea of a hack-back strategy. Analysts that can fall into this category include incident responders, malware reverse engineers, threat analysts, network security monitoring analysts, and other security personnel who utilize their environment to hunt for the adversary and respond to them.

[16] *Joint Publication (JP) 1-02 Dictionary of Military and Associated Terms.* U.S. Department of Defense, March 2015.

[17] A. L. Latter and E. A. Martinelli, *Active and Passive Defense.* RAND Corporation, August 1965

The focus on analysts instead of tools brings about a proactive approach to security that highlights the intention of the original strategy: maneuverability and adaptability. Systems themselves cannot provide an active defense; systems can only serve as tools to the active defender. Likewise, simply sitting in front of a tool such as a system information and event manager does not make an analyst an active defender – it is as much about the actions and process as it is about the placement of the person and their training. What makes advanced threats persistent and dangerous is the adaptive and intelligent adversary behind the keyboard. Countering these adversaries requires equally flexible and intelligent defenders.

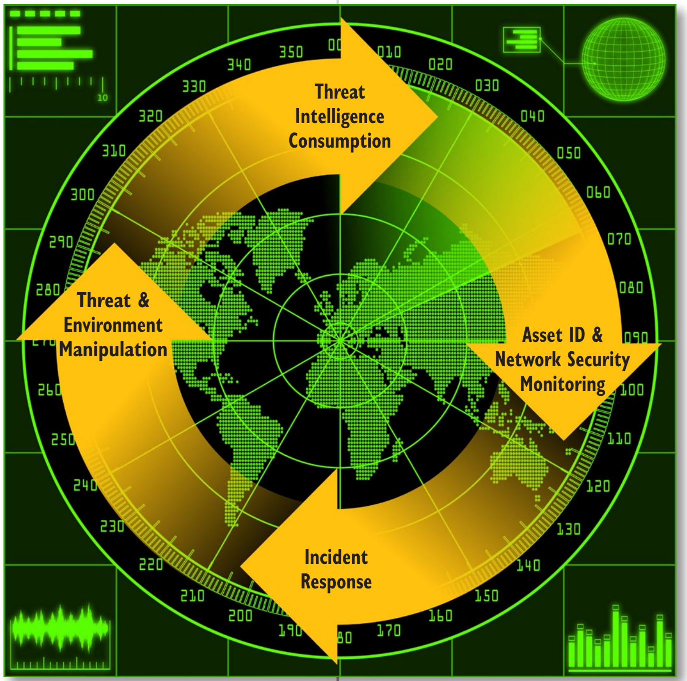

Threat Intelligence Consumption
Asset ID & Network Security Monitoring
Incident Response
Threat & Environment Manipulation

*Figure 3. The Active Cyber Defense Cycle*

**Recommended Active Defense Model:**

- The Active Cyber Defense Cycle
  - The Active Cyber Defense Cycle is a model created by the author of this paper and is the subject of the SANS ICS515 – Active Defense and Incident Response course. It is the continual process of four phases of actions that defenders can take to actively monitor for, respond to, and learn from adversaries. The four phases are: threat intelligence consumption, asset identification and network security monitoring, incident response, and threat and environment manipulation as illustrated in Figure 3.[18]
- Network Security Monitoring
  - Network Security Monitoring (NSM) was formalized as a set of actions in the 1980's by Todd Heberlein with his development of the Network Security Monitor, a system for detecting network intrusions.[19] NSM was then popularized and expanded by other analysts; notably, the works of Richard Bejtlich has extended the field and brought it widespread attention with his writings which include the book *The Tao of Network Security Monitoring*. While NSM is a component of the Active Cyber Defense Cycle it is its own model and in of itself represents an approach to an active defense. This approach stresses the value of analysts attempting to detect an adversary internal to their environment. It helps drive incident response actions to adversary campaigns instead of singular intrusions.

[18] The Active Cyber Defense Cycle was first publicly presented at BSides Huntsville 2015 and a recording can be found here: www.irongeek.com/i.php?page=videos/bsideshuntsville2015/active-cyber-defense-cycle-robert-m-lee additionally the "Implementing an ICS Active Defense Strategy" SANS webcast covered the topic here: www.sans.org/webcasts/implementing-ics-active-defense-strategy-100072 and the SANS ICS515 – Active Defense and Incident Response class covering the model can be found here: www.sans.org/course/industrial-control-system-active-defense-and-incident-response

[19] Richard Bejtlich, *Network Security Monitoring History*. TaoSecurity, 11 April 2007

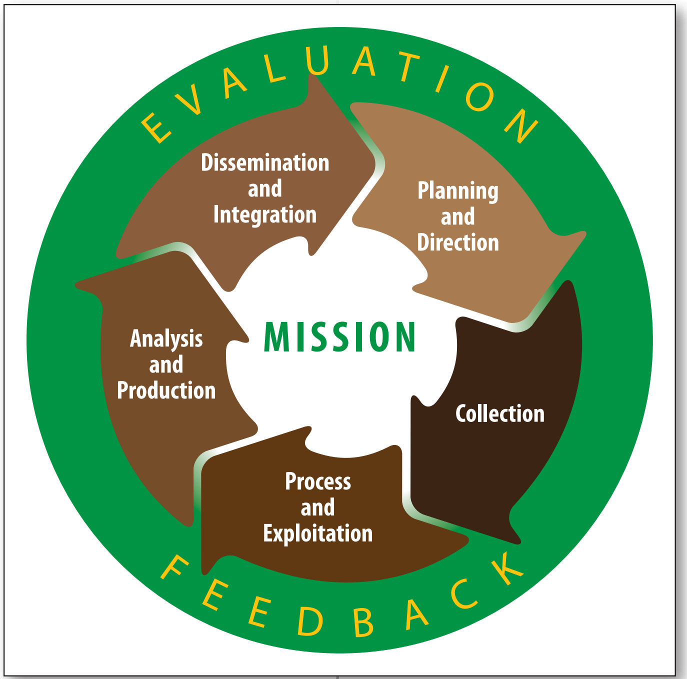


*Figure 4. The Intelligence Process*[22]

One of the keys to effective Active Defense is the ability to consume intelligence about the adversary and have it drive security changes, processes, and actions in the environment. Consuming intelligence is part of an Active Defense but generating intelligence falls within the Intelligence category. It is within this phase that analysts produce data, information, and intelligence about the adversary from a variety of sources and methods.

Intelligence is a commonly used word yet often misunderstood concept. In the U.S. Department of Defense's definition of terms the word appears 998 times.[20] Military intelligence has made up the bulk of the field of study and contributed largely to the understanding in the field of cyber security. The U.S. military definition of intelligence is: "the product resulting from the collection, processing, integration, evaluation, analysis, and interpretation of available information concerning foreign nationals, hostiles or potentially hostile forces or elements, or areas of actual or potential operations. The term is also applied to the activity which results in the product and to the organizations engaged in such activity."[21] In short, intelligence is defined as both a product and process. It is defined here, for the purposes of cyber security, as: ***the process of collecting data, exploiting it into information, and producing an assessment that satisfies a previously identified knowledge gap.*** The intelligence process, seen in Figure 4, has been documented thoroughly and is often presented as a continual cycle of collecting data, processing and exploiting that data into information, and analyzing and producing information from various sources to produce Intelligence.

INTELLIGENCE:

*the process of collecting data, exploiting it into information, and producing an assessment that satisfies a previously identified knowledge gap*

[20] *JP 1-02*, March 2015

[21] Ibid.

[22] Ibid.

The understanding of the relationship of data, information, and Intelligence is where some of the abuses of the word Intelligence stem from in cyber security.[23] A visual understanding of this process can be seen in Figure 5. Numerous security vendors have touted tools that produce intelligence. This has also led to the often-abused term of "actionable intelligence." Tools do not create Intelligence. Only analysts can create Intelligence. Tools and systems are useful for collecting data from the operational environment, whether they be an organization's networks or the adversary's systems. Tools and other systems created for the purpose of processing and exploitation of data into useful information is also a worthwhile investment. However, the analysis and production of that information, other sources of information, and executing needed processes such as the analysis of competing hypotheses are only possible by human analysts. These human analysts understand the internal decisions or actions that need made and analyze various sources of information to generate intelligence assessments. These assessments are needed to develop recommendations for internal decisions and courses of action. Tools alone cannot accomplish that process.

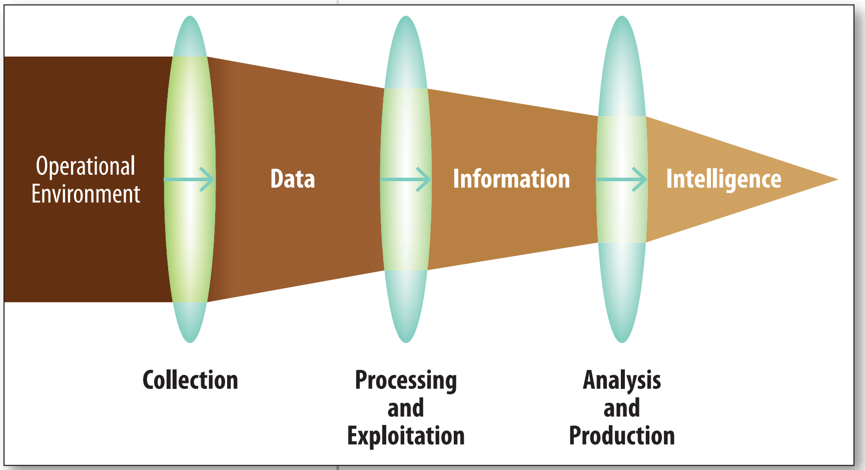


*Figure 5 – The Relationship of Data, Information, and Intelligence*[24]

Intelligence in the field of cyber security can fall into a range of activities. For example, a group of persons accessing an adversary network to collect and analyze information would be conducting a cyber intelligence operation. Another example would be documents that call home after being stolen by an adversary. These documents are inside the adversary's network and are transmitting back information to the defenders about the true location of the adversary's environment. The information gathered would be useful intelligence for national policy makers, the military, or others to know about the research, development, and plans to use adversary capabilities. Likewise, researchers standing up honeypots to analyze attacks against it are gathering information and analyzing it to create intelligence about adversaries without engaging in an operation against the adversaries. Finally, another good example would be analysts collecting data and information from systems that have been compromised by adversaries in their networks or other networks to derive intelligence about threats they are facing. This last example has been identified as Threat Intelligence in the cyber security community.

[23] For a discussion on the difference between data, information, and intelligence and how it is used in the security market today see: https://digital-forensics.sans.org/blog/2015/07/09/your-threat-feed-is-not-threat-intelligence

[24] Ibid.

Threat Intelligence is a specific type of Intelligence that seeks to give defenders knowledge of the adversary, their actions within the defender's environment, and their capabilities as well as their tactics, techniques, and procedures.[25] The goal is to learn from the adversary with the intent of better identifying and responding to them. Threat Intelligence is extremely useful but due to a lack of understanding in the field of intelligence many organizations have not taken full advantage of it which leads to cynicism regarding the term. Properly taking advantage of Threat Intelligence requires at least three things:

1. Defenders must know what qualifies as their threats (only those adversaries that have the opportunity, capability, and intent to do them harm)
2. Defenders must be able to use intelligence to drive actions in their environments
3. Defenders must understand the difference between generating intelligence and consuming it

Currently, most organizations do not accurately understand their threat landscape. That is to mean that they cannot properly determine what adversaries and capabilities actually constitute a threat to them and which ones do not. For example, without a firm understanding of the Architecture and Passive Defenses in an organization it is not feasible to identify if an identified vulnerability exists within an organization's systems or if the vulnerabilities can be or have been fixed; thusly there also cannot be an accurate representation of risk. If defenders do not know their business processes, security status, network topologies, and Architecture it is impossible to effectively use Threat Intelligence. Likewise, many defenders do not have the internal organizational knowledge or empowerment from decision makers to take the actions required to protect their environment. There cannot be a failure of intelligence if the intelligence cannot be used anyway. Lastly, there is a significant difference in the analysts, processes, and tools required to generate intelligence and those required to consume it. Generating intelligence often requires significant investment of resources, a wide availability of data collection opportunities, and a singular focus of learning all there is to know about the target. Intelligence consumption though requires analysts be familiar with the environment that the Threat Intelligence is meant for, understand the business operations and technology that can be impacted by it, and be able to put the intelligence into a usable form by the defenders. Generating intelligence is an action of Intelligence whereas consuming it is a role for Active Defense.

[25] To learn more about Cyber Threat Intelligence consider taking SANS FOR578 – Cyber Threat Intelligence for a deep dive into the material by Mike Cloppert, Chris Sperry, and the author of this paper www.sans.org/course/cyber-threat-intelligence

Stated simply, organizations must understand themselves, understand the threats, and empower personnel to use that information for defense to properly use Threat Intelligence. This basic concept is more difficult than it appears as it must build upon all the other categories presented so far in the Sliding Scale of Cyber Security. It is this core foundation that makes Threat Intelligence extremely valuable to defenders and without it drastically reduces any value that can be obtained from intelligence.

### Recommended Intelligence Models

- The Cyber Kill Chain™
  - The Cyber Kill Chain™ was first made available in an unclassified form in the paper "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains."[26] It was authored by Eric M. Hutchins, Michael J. Cloppert, and Rohan M. Amin, Ph.D. It is an effective model to describe adversary actions against defender systems and breaks those actions into easily identifiable phases. This model can extract indicators and information from interactions with the adversary that can be used in combination with other models such as the Diamond Model to help produce Threat Intelligence.
- The Diamond Model of Intrusion Analysis
  - The Diamond Model was first made available in an unclassified form in the paper "The Diamond Model of Intrusion Analysis."[27] The paper was authored by Sergio Caltagirone, Andrew Pendergast, and Christopher Betz based on their experiences analyzing adversary campaigns within the U.S. Department of Defense. The model helps articulate and analyze the four key points of any event: adversary, infrastructure, capability, and victim. Understanding these four points of the model, discovering the information related to each, and understanding where in the adversary's kill chain the event occurred significantly contributes to understanding an adversary and likewise producing Threat Intelligence.
- Intelligence Life Cycle
  - The Intelligence Life Cycle, or Intelligence Process, presented previously in this paper is the classic approach to producing Intelligence. Doing this in the field of cyber security with a focus on threats is a tested method for producing Threat Intelligence. Using existing models to support this process such as the Cyber Kill Chain and the Diamond Model positions defenders well to respond to their threats.

[26] Eric M. Hutchins, Michael J. Cloppert, and Rohan M. Amin, Ph.D., *Intelligence-Driven Computer Network Defense Informed* by Analysis of Adversary Campaigns and Intrusion Kill Chains. Proceedings of the 6th International Conference on Information Warfare and Security, 2011

[27] Sergio Caltagirone, Andrew Pendergast, and Christopher Betz, *The Diamond Model of Intrusion Analysis*. Active Response, July 2013.

# Offense

With the proper foundations represented so far within the Sliding Scale of Cyber Security, including a heavy investment into Intelligence, Offense can contribute to cyber security. Offense is the final phase of the sliding scale and represents direct action taken against the adversary outside friendly networks. Those practicing offensive operations require the understanding and skillsets found in the other phases and often times requires actions from those categories. For example, identifying a threat in the environment is often done in the Active Defense phase. To perform Active Defense correctly requires the foundation that Passive Defense and Architecture establishes. Then, identifying information about the adversary, building the required knowledge to conduct an operation, and establishing markers for success are achieved in the Intelligence phase. Offense is costly when considering the single action but with the appreciation of the foundation required to be successful reveals itself to be the most costly actions organizations can take.

The word offense was chosen for the Sliding Scale of Cyber Security over the terminology of a cyber attack due to the wide set of actions often covered by it. Often times, organizations and news media describe cyber attacks with a variety of definitions including those actions of network breaches and espionage that would be better described as an adversary Intelligence operation. The U.S. Department of Defense's joint publication for the definition of terms does not contain a definition for offensive cyber operations, however the publication discusses offensive cyber operations in the following way "to project power by the application of force in or through cyberspace."[28] It is important to note here that the use of the word "force" aligns with the international use of the term which is used to describe a set of unlawful actions outside of war. The U.S. military has unofficially and commonly used the actions of "deny, disrupt, deceive, degrade, and destroy" to describe a cyber attack.[29]

A distinction needs to be made between the projection of power upon states by states and those actions organizations can take to increase their cyber security. Offensive actions must be discussed as an option that can increase cyber security but the legality of these options for civilian organizations is highly contested. Offensive actions by states that would be deemed legal under international law is also highly debated and the most complete document to address the debate to date is the Tallinn Manual.[30] There have been interesting case-studies for this debate to arise recently including the alleged North Korean attack on the civilian company Sony. Even without firm attribution the United States likely had reason and legal impunity to apply countermeasures in the form of a cyber attack.[31] This discussion is outside the scope of this paper though.

[28] *Joint Publication (JP) 3-12 Cyberspace Operations.* U.S. Department of Defense, 5 Feb 2013

[29] *Air Force Cyber Command Strategic Vision.* U.S. Air Force, 2008

[30] Professor Michael N. Schmitt, *The Tallinn Manual.* NATO Cooperative Cyber Defence Centre of Excellence, 2009

[31] The discussion of this case-study is outside the scope of this paper but can be found by Professor Michael Schmitt on the Just Security blog here: http://justsecurity.org/18460/international-humanitarian-law-cyber-attacks-sony-v-north-korea/

Whatever the national and international laws evolve to, the actions by organizations, civilian or national, on the offensive must be legal in nature to be deemed an act of cyber security and not an act of an aggressor. Offense can be done for purposes other than cyber security such as national policy or conflict. However, to contribute to cyber security the definition for these offensive actions is defined here as: legal countermeasures and counterstrike actions taken against an adversary outside of friendly systems for the purpose of self-defense. It is in the opinion of the author that civilian organizations cannot currently participate in such actions and remain within the spirit of the law. While loopholes may be found it is due to the law's inability to keep up with technical actions and not due to informed debate and discourse that would allow such actions. Additionally, with appreciation of the return on investment for Offense based actions it should be easily determined that organizations should have already achieved a hypothetical maximum return on investment from the other categories before seeing any value towards security from Offense. Reasons based on vengeance or retaliation are both illegal under international law and never seen as acts of self-defense.

### Recommended Models for Offense

- None; the subject of which has been highlighted in the web comic Little Bobby as seen in Figure 6

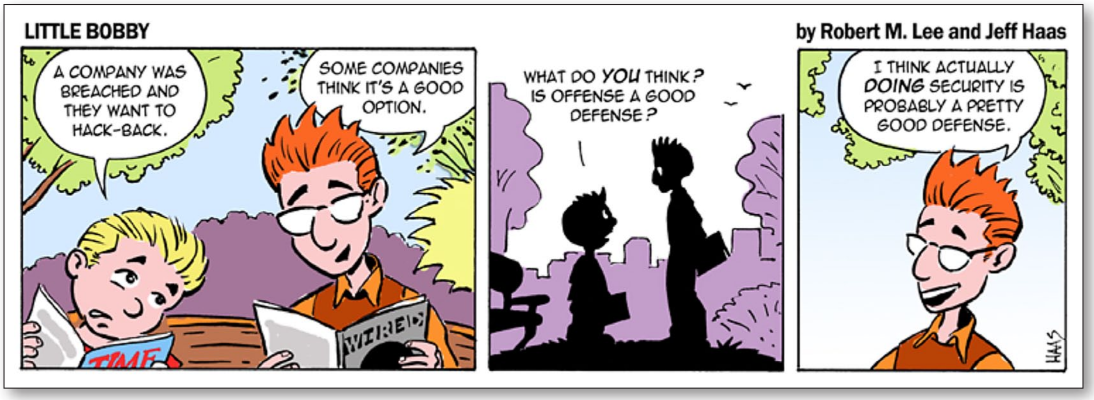

LITTLE BOBBY
by Robert M. Lee and Jeff Haas
A COMPANY WAS BREACHED AND THEY WANT TO HACK-BACK.
SOME COMPANIES THINK IT'S A GOOD OPTION.
TIME
WIRED
WHAT DO YOU THINK? IS OFFENSE A GOOD DEFENSE?
I THINK ACTUALLY DOING SECURITY IS PROBABLY A PRETTY GOOD DEFENSE.
HAAS

*Figure 6: Little Bobby – Week Three*[32]

[32] www.LittleBobbyComic.com

# About the Author

**Robert M. Lee** is a SANS Certified Instructor and the course author of SANS ICS515: Active Defense and Incident Response and the co-author of SANS FOR578: Cyber Threat Intelligence. He is also the CEO, co-founder of Dragos Security LLC where he has a passion for control system traffic analysis, incident response, and threat intelligence research.  He is a passionate educator and is a frequent speaker at conferences around the world. Robert obtained his start in cyber security in the U.S. Intelligence Community where he served as an Air Force Cyber Warfare Operations Officer. He has performed defense, intelligence, and attack missions in various government organizations and established a first-of-its-kind ICS/SCADA cyber threat intelligence and intrusion analysis mission. Robert also routinely writes articles and journals in publications such as Control Engineering, Wired, and the Christian Science Monitor's Passcode. He is currently a non-resident National Cyber Security Fellow at the New America think tank and is pursuing his PhD at Kings College London with research into the cyber security of control systems. Lastly, Robert is the author of the book *SCADA and Me* and the weekly web-comic www.LittleBobbyComic.com. He may be found on Twitter @RobertMLee

Last Updated: September 19th, 2015

# Upcoming SANS Training

**Click Here for a full list of all Upcoming SANS Events by Location**

| | | | |
|---|---|---|---|
| **SANS Perth 2015** | **Perth, AU** | **Sep 21, 2015 - Sep 26, 2015** | **Live Event** |
| **SANS Baltimore 2015** | **Baltimore, MDUS** | **Sep 21, 2015 - Sep 26, 2015** | **Live Event** |
| **SANS Tallinn 2015** | **Tallinn, EE** | **Sep 21, 2015 - Sep 26, 2015** | **Live Event** |
| **SANS ICS Amsterdam 2015** | **Amsterdam, NL** | **Sep 22, 2015 - Sep 28, 2015** | **Live Event** |
| **SANS Bangalore 2015** | **Bangalore, IN** | **Sep 28, 2015 - Oct 17, 2015** | **Live Event** |
| **SANS Seattle 2015** | **Seattle, WAUS** | **Oct 05, 2015 - Oct 10, 2015** | **Live Event** |
| **SANS DFIR Prague 2015** | **Prague, CZ** | **Oct 05, 2015 - Oct 17, 2015** | **Live Event** |
| **SOS: SANS October Singapore 2015** | **Singapore, SG** | **Oct 12, 2015 - Oct 24, 2015** | **Live Event** |
| **SANS Tysons Corner 2015** | **Tysons Corner, VAUS** | **Oct 12, 2015 - Oct 17, 2015** | **Live Event** |
| **SANS Gulf Region 2015** | **Dubai, AE** | **Oct 17, 2015 - Oct 29, 2015** | **Live Event** |
| **SANS Tokyo Autumn 2015** | **Tokyo, JP** | **Oct 19, 2015 - Oct 31, 2015** | **Live Event** |
| **SANS Cyber Defense San Diego 2015** | **San Diego, CAUS** | **Oct 19, 2015 - Oct 24, 2015** | **Live Event** |
| **SANS South Florida 2015** | **Fort Lauderdale, FLUS** | **Nov 09, 2015 - Nov 14, 2015** | **Live Event** |
| **SANS Sydney 2015** | **Sydney, AU** | **Nov 09, 2015 - Nov 21, 2015** | **Live Event** |
| **SANS London 2015** | **London, GB** | **Nov 14, 2015 - Nov 23, 2015** | **Live Event** |
| **Pen Test Hackfest Summit & Training** | **Alexandria, VAUS** | **Nov 16, 2015 - Nov 23, 2015** | **Live Event** |
| **SANS Hyderabad 2015** | **Hyderabad, IN** | **Nov 24, 2015 - Dec 04, 2015** | **Live Event** |
| **SANS Cape Town 2015** | **Cape Town, ZA** | **Nov 30, 2015 - Dec 05, 2015** | **Live Event** |
| **SANS San Francisco 2015** | **San Francisco, CAUS** | **Nov 30, 2015 - Dec 05, 2015** | **Live Event** |
| **Security Leadership Summit & Training** | **Dallas, TXUS** | **Dec 03, 2015 - Dec 10, 2015** | **Live Event** |
| **SANS Cyber Defense Initiative 2015** | **Washington, DCUS** | **Dec 12, 2015 - Dec 19, 2015** | **Live Event** |
| **Data Breach Investigation Summit & Training** | **OnlineTXUS** | **Sep 21, 2015 - Sep 26, 2015** | **Live Event** |
| **SANS OnDemand** | **Books & MP3s OnlyUS** | **Anytime** | **Self Paced** |