18th ICCRTS

Implementing an Integrated Network Defense Construct

Topics: Data, Information, and Knowledge; Collaboration, Shared Awareness, and Decision Making; Networks and Networking; Cyberspace Management

Authors
Ronald J. Clark, Major, US Air Force (STUDENT)
Jonathan W. Butts, Major, USAF, PhD
Robert F. Mills, PhD

Air Force Institute of Technology
Wright-Patterson AFT OH

Point of Contact
Jonathan W. Butts, Major, USAF, PhD
Chief, Computer Science and Engineering Division
Air Force Institute of Technology
2950 Hobson Way
Wright-Patterson AFB OH 45433-7765
937-255-3636 x4332
FAX 937-656-4055
Email: jonathan.butts@afit.edu

Abstract

Traditional network architectures rely on boundary protection mechanisms to prevent malicious actors from gaining access to systems that host sensitive or mission critical data. Historical examples, however, demonstrate that a determined adversary with sufficient resources can establish footholds internal to the network. Leveraging these footholds, the adversary may maneuver within the network with impunity; largely due to the lack of network monitoring and alert correlation. To combat this threat, capability gaps must be addressed that provide enhanced situational awareness and allow evaluation of system security from the inside-out, as opposed to traditional penetration testing which uses outside-in techniques. Furthermore, advances in network defense must be integrated in a fashion that is complementary versus competitive in nature. Comparing network defense with a proven system that utilizes the attributes of collaboration and integration in a seamless manner provides valuable insight into addressing these deficiencies. This research examines the integrated air defense system construct and applies the command and control characteristics to network defense. Findings demonstrate the improvements will provide unprecedented situational awareness and help mitigate an adversary's ability to maneuver throughout enterprise networks.

1. Introduction

On September 11, 2001, the United States awoke to a catastrophic reality. The Cold War-era air defense model of looking outward for an external, known enemy led to disastrous effects when terrorists took advantage of the soft interworkings of the national air transportation system. The lack of the ability to track internal traffic, and consequently threats, by air defense sectors, and the inability to seamlessly coordinate the use of surveillance equipment facilitated the ease of the attack.

Analysis of the construct determined that the perimeter-based model of defense was inadequate to actively detect and respond to threats (Davis et al., 2007). Modern enterprise network defense models share many similarities to the pre 9/11 air defense posture. While the risk to life in telecommunication network defense pales in comparison to that experienced in the attacks against the World Trade Center and Pentagon, cyber-based attacks against the nation's critical infrastructure could wield devastating results.

This paper examines the construct of an integrated air defense system (IADS) and the feasibility of applying its attributes to large enterprise networks. Section two identifies background on the need to move to a collaborative construct in network defense. Section three describes the fundamental components of IADS and how they evolved into the modern-day system. Section four introduces an integrated network defense model incorporating key characteristics from the IADS construct and Section five concludes the paper.

2. Background

The principle of a layered defense has existed for millennia. The premise is to devise a defensive structure that causes an attacker to needlessly expend resources with little chance of success. In early warfare, commanders used terrain or built walls to create an easily defendable avenue for ingress and egress. In medieval times, castles leveraged this principle. If an attacker was brazen enough to attempt to capture the fortification, defensive mechanisms slowed the impending charge and placed the attacker at a marked disadvantage. Indeed, the defender had the upper ground, visibility of the attack and the ability to respond with force. They could meet the attacker head-on if they had equal or greater capabilities, or they could wait out the opponent and fight from an entrenched position if outmatched.

The physical protection model has evolved from defending castles to modern physical security systems; network security naturally followed this precedent. Just as terrain and manmade obstacles were engineered to create defensible structures, network architects sought to build impenetrable virtual bastions with routers, firewalls and switches. The model incorporated controls presented in overlapping succession to preserve confidentiality, integrity, and availability of system resources (Brancik, 2008). The devices are certainly part of a defensive network strategy; however, they are not sufficient to achieve a defensible network infrastructure. Accordingly, many security experts feel that the layered construct alone does not fulfill the requirements of an encompassing defensive structure for network security (Small, 2012).

2.1. The Cyber Defense Dilemma

While the philosophy of network defense mirrors that of the physical world, its application has some significant drawbacks. Whereas the medieval castle defenders had the high ground and clear visibility of attacks, in the networking environment, the defender has to discover the attacker's presence in order to respond and defend its resources. In the physical realm, it is possible to enumerate likely avenues of approach and pre-plan response actions to attacks when they occur. In cyber, the rapid pace of tool development and methods to infiltrate a system often play to the adversaries' advantage (i.e. it is difficult to pre-plan responses to unknown exploitation methods).

In the current environment, adversaries on the network have myriad capabilities at their disposal, ranging from unpatched systems with known vulnerabilities to misconfigurations of network infrastructures. Moreover, sophisticated attackers develop custom exploits unknown to the system owner or application developer. An attacker need only gain one entry point to secure access to numerous network resources. For example, Lockheed Martin documented three intrusion attempts, over a three-week period, linked to a single actor using escalating exploitation capabilities to gain corporate network access (Hutchins, Cloppert & Amin, 2011). Understanding that determined actors have and will continue to develop means to gain access to enterprise systems is a fundamental prerequisite in identifying their presence on corporate networks.

The state of the art in network defense cannot keep pace with the agile tactics, techniques and procedures of offensive actors. Today, defensive techniques work against indiscriminate attacks, but these strategies alone are not sufficient against targeted attacks (Arnold *et al.*, 2012). The challenges culminate in a defensive dilemma; the network defender must be ever vigilant, block all intrusion attempts from all directions while the offense only has to achieve one successful exploit to declare victory. To remedy this imbalance, Mike McConnell, the former United States Director of National Intelligence, identified a need for an early-warning system to monitor cyberspace, identify intrusions and locate the source of attacks with a trail of evidence that can support diplomatic, military and legal options (McConnell, 2010).

2.2. Areas for Improvement

The challenges associated with the defense of large networks can be divided to five main areas. First, current intrusion detection and protection mechanisms are largely signature based,

requiring prior knowledge of a threat. Second, enterprise-class network defense devices handle incredibly high speeds and large amounts of data, making data aggregation and anomaly detection difficult. Third, an outward-facing perimeter defense posture lacks the ability to observe inter-network interactions at the host level. Fourth, the typical centralized analysis and defense of the network isolates network defenders from the mission owners which leads to disconnects in developing situational awareness and formulating response options. Finally, distributed network defense postures lack an agile command structure that cohesively ties geographically separated network enclaves into one common framework.

To tackle these five areas of improvement, this research recommends using an integrated air defense system (IADS) as a template for an integrated network defense system (INDS) for large networks servicing distributed operation centers. Individual components of IADS provide formidable protection against an airborne attack, but when properly implemented, the integration of the individual elements creates a synergistic effect for the defenses. Logically an INDS can and should follow the same premise.

3. Integrated Air Defense

To model an INDS after an IADS, it is necessary to understand the development of the IADS architecture and the evolution into the collaborative system it is today. Furthermore, it is important to examine the components of an IADS and how they contribute to the overall architecture. This section explores the concepts, components and functions that comprise an IADS.

3.1. Evolution of IADS

Ever since the first use of aircraft in military applications, nations have invested in technology to counter the air threat. Early adaptions included guns simply aimed at aircraft. Over the years, the evolution of anti-air capabilities consisted of variances in ammunition and fusing options, fire-control, and applying the use of interceptor aircraft (Deeney, 2012; Gleick, 2011). Advances in research led to mechanical prediction computers and incorporation of optical and acoustic devices to augment visual observation ("Huge "Ear" Locates Planes and Tells Their Speed" 1930). By the late 1930s, command and control (C2) of air defense systems were “integrated” into a single hierarchical structure under the Air Defence of Great Britain initiative (Checkland and Holwell, 1998). This implementation was the earliest concept of a command structure that integrated defensive air capabilities.

After the Second World War, research surrounding IADS began to gain momentum. Indeed, the beginning of the Cold War motivated an arms race, propelling the need to defend sovereign airspace. To meet this need, the Soviet Union sought to create economical, mobile equipment consisting of sensors, weapons, and C2 nodes that are easily moved and linked together (Deeney, 2012). Defending airspace had moved beyond a series of autonomous units. Fire control systems became directly linked with command channels enabling communications from decision makers to the firing units. The simplicity and cost-effectiveness of the Soviet design was not only attractive for the USSR, but to other nations with aspirations of power and the need to defend sovereign airspace. To date, the inexpensive modular platforms have become popular exports to

countries wishing to employ a robust air defense system. In the years following the Cold War, many improvements were made to anti-air platforms and IADS. Missile technology, radar-directed fire control, and further sensor advances including optronics focused on more lethal equipment bolstering the construct.

On September 11, 2001, great catastrophe brought about much change and new innovations to integrated air defense in the United States. In response to the attacks on New York and the Pentagon, significant deficiencies were identified in the ability to detect, respond and defend against internal threats from commercial aircraft. To resolve these deficiencies, monumental changes for homeland defense were instituted under Operation Noble Eagle (Air Force Historical Studies Office 2012; Davis et al. 2007). During the discovery process, it was determined that even with sophisticated systems supporting the air defense of the United States, the lack of integration failed to provide a common air picture. Additionally, existing sensors were insufficient for target identification (Davis et al. 2007). Improvements were necessary to give military and civilian decision makers the ability to rapidly detect, identify, and coordinate response actions to atypical aircraft attacks (Davis et al. 2007).

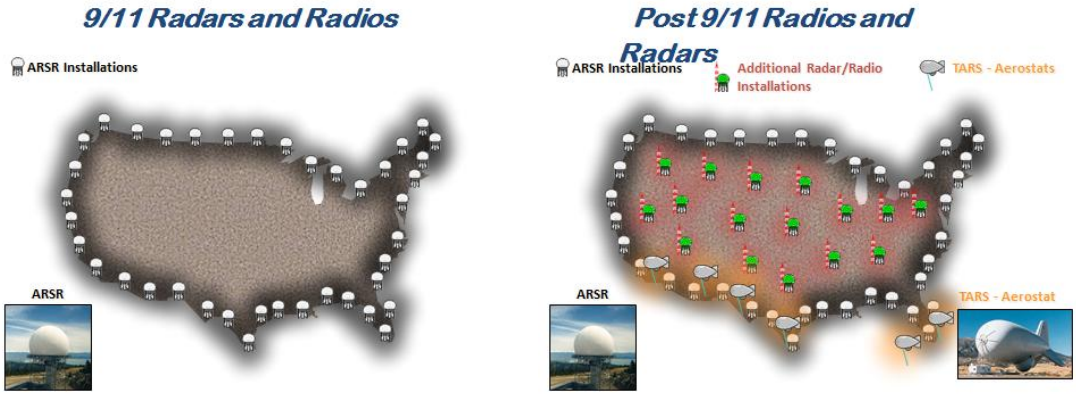

Figure 1. Air Defense Coverage Pre and Post September 11, 2001.

As identified in Figure 1, prior to 9/11 the North American Aerospace Defense Command (NORAD) focused on outward detection of Soviet bombers, not on the identification of an aircraft launching an attack from within the United States (Davis et al., 2007). In a post 9/11 environment, the air defense posture was forced to make tremendous leaps in capability and capacity. In response, NORAD, with support from the Federal Aviation Administration (FAA), duplicated feeds from field sites around the nation and combined them to form one common air picture that included outward and inward facing sensors. This summarily eliminated the perimeter only defense posture for airborne attacks. The initiative created the ability to narrow the focus to the regional level while still providing national-level situational awareness to decision makers. The distributed system provided NORAD the necessary air picture and collaborative environment to facilitate real-time responses to immediate threats.

3.2. Structure

In order to relate the air defense structure to network defense, it is necessary to examine the major components that comprise a modern IADS. An IADS is comprised of: sensors, weapons, command, control, communications, computers, and intelligence systems, and personnel (AFTTP 3-2.31, 2009). Organizationally, the IADS structure overlays physical and logical connections with a C2 architecture that allows for seamless communication and collaboration. The structure focuses on defeating a threat by finding and identifying targets, controlling sensors and weapons, and engaging the target (Macfadzean, 1992). To facilitate a systematic engagement methodology, IADS are divided into geographic areas or sectors. Each sector connects to a neighboring sector, a regional headquarters and further on to national level headquarters.

3.2.1. Command and Control

The nature of an IADS is successful due to the integration and federation of all its components into a seamless C2 structure. The architecture enables tasking, collaboration and response actions by numerous entities across many areas of responsibility, covering great distances. Multi-service tactics, techniques, and procedures state that there are seven principles of an IADS: centralized planning and direction; decentralized execution; planned responses; effective and efficient communications; layered defense; 360-degree coverage; early detection; discrimination; classification; and identification (AFTTP 3-2.31, 2009). Indeed, employing these principles in such a complex system requires a robust C2 architecture.

Alberts *et al*. evaluated C2 constructs of highly complex operations where numerous entities from disparate command chains worked together for a common goal under the North Atlantic Treaty Organization (NATO) Network Enabled Capability (NNEC) Maturity Model (N2C2M2) (2010). A system as diverse as the IADS necessitates a robust C2 structure to achieve a functional capability level. The N2C2M2 study examined the NNEC capability levels of disjointed operations, de-conflicted operations, coordinated operations, integrated operations, and transformed operations and correlated each with a corresponding C2 maturity level (1-5 respectfully) (Alberts *et al*., 2010). Due to the nature of C2 integration in an IADS, a mature C2 level, consistent with integrated operations (Level 4) is necessary, requiring what Alberts *et al*. referred to as an Edge C2 approach. Edge C2 incorporates a self-synchronizing collaboration model that provides members of the collective system "a high degree of shared awareness, widespread access to information, and unconstrained interactions" (Alberts *et al*., 2010). The Edge C2 approach provides the agility necessary to react to dynamic situations, while coordinating actions with numerous entities.

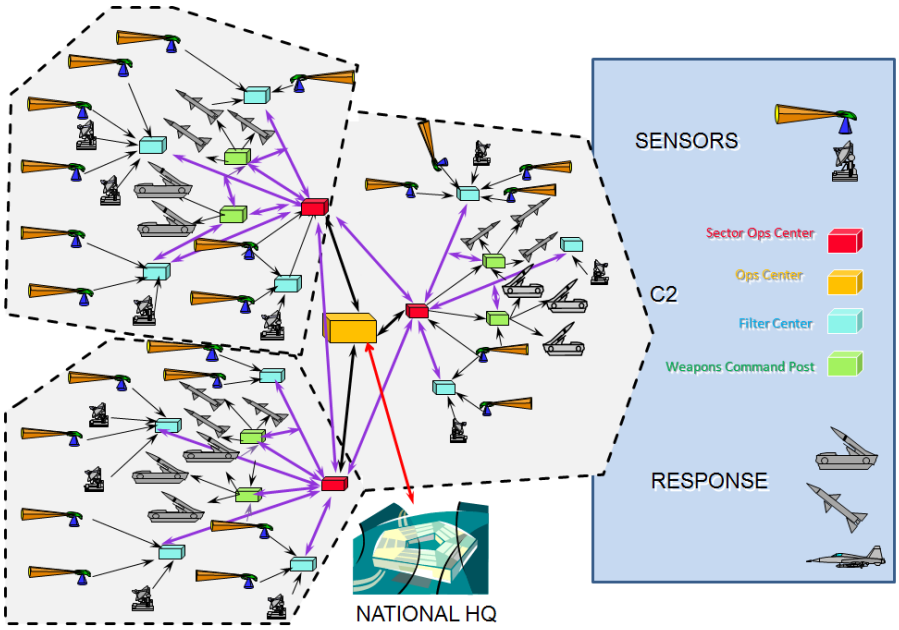

Figure 2. Notional IADS Construct.

Information flow in IADS C2 uses a swarming method of information transfer beginning with assorted sensors identifying potential threats. The data from these devices are aggregated at filtering centers and sent to a Sector Operations Center (SOC). SOCs are accountable for a geographic area of responsibility, but serve the overall system by relaying threat information to other SOCs, operational control centers, weapons command posts and national headquarters. Figure 2 identifies a notional IADS command and control construct. The lines indicate communication flow within the sector, where operational information is verified, vetted and consolidated using collaborative analysis. This intelligence is shared with the entire collective construct. The model is an efficient method of sharing threat information across different areas of responsibility under a single C2 structure.

3.2.2. Threat Identification

Threat identification consists of four processes: (i) search; (ii) detect; (iii) non-precision track; and (iv) identify association (Macfadzean, 1992). The process begins once a target is detected in the search area of interest. Targets entering the air space are typically evaluated via identify friend or foe (IFF) transponders to determine if they are hostile or friendly. Target identification is conducted using a wide variety of sensing devices including radar, acoustic, optronics, electronic emanations, communications/signals intelligence and visual observation. Each of these sensors produces information using its own protocol and reporting mechanism, and is fed into the filter centers, SOCs, and on to the collective system.

Targets identified as hostile are labeled threats. From the initial moment a threat is identified, other sectors and decision makers are notified of its presence and apprised of its movements.

Each of the SOCs manage track information and use specialized metadata that depicts the nature of the target and its determined intent. The swarm model of communication used in this exchange ensures all necessary entities are up-to-date with the best information. The structure alerts neighboring areas so they may react or provide forces to assist in response.

3.2.3. Battle Management Controlling

After a target is identified and validated as a hostile threat via IFF determination, it is necessary to begin the response process. Controllers continuously monitor the threat, conferring with numerous data sources to ascertain its origin, purpose and assessed intentions. Threats are continuously monitored. As more detailed information returns from sensors, it is added to the collection system, enriching the intelligence available on the threat. As with threat identification, information obtained in the battle management phase, details are fed immediately to decision makers. This enables the transfer of firing unit control directly to air battle managers (ABMs) who are charged with controlling, and ultimately eliminating, the threat.

3.2.4. Engagement

Depending on rules of engagement and decisions directed from higher echelons, weapons control maneuvers to engage the threat. Responding forces are armed with capabilities to include surface to air missiles, radar-guided anti-aircraft ammunition, or intercept aircraft. Based on the attributes of the threat, range, and the available weapon systems, controllers restrict, redirect, or destroy the threat. During this critical time, adjacent SOCs ready forces to engage if the threat deviates into their area of responsibility.

Table 1 summarizes the functionality of each of the components of an IADS as well as resources required to accomplish the mission. Note that the complementary nature of the construct facilitates collaboration and situational awareness at each level.

Table 1. IADS Primary Attributes

Function	Primary Attribute	Utilizes
Command and Control	Information Sharing, Reporting, Centralized Planning and Direction	Various Communication Channels; Effective and Efficient Communications
Threat Identification	Detect, Acquire Target; Layered Defense; 360-Degree Coverage; Early Detection	Sensors; Effective and Efficient Communications
Battle Management	Decentralized Execution; Discrimination; Classification Track/Control Target	Common Operating Picture; Effective and Efficient Communications
Engagement	Execute Planned Responses; Eliminate Target	CAP, Air Defense Artillery, Missile Defenses; Effective and Efficient Communications

4. An Integrated Network Defense

Conceptually, air defense and network defense share many commonalities. Both sprang from numerous independent systems that gather and inform using differing protocols, reporting mechanisms and formats. Integrating the data from these disparate systems capitalizes on the strengths in individual components and overcomes the shortfalls in others. Additionally, to be effective, both air and network defense require agile C2 architectures that require situational awareness and collaboration at each level up and down the echelon. However, when comparing organizational models, it is easy to note differences between IADS and network defense. IADS employ a mesh architecture to disseminate and distribute information. Network defense uses a hierarchical model that requires information transfer both up and down echelons to distribute information to peer organizations. By adapting efficiencies incorporated in the IADS model, an INDS could enhance threat identification. This section explores the primary attributes of an IADS as applied in an INDS construct.

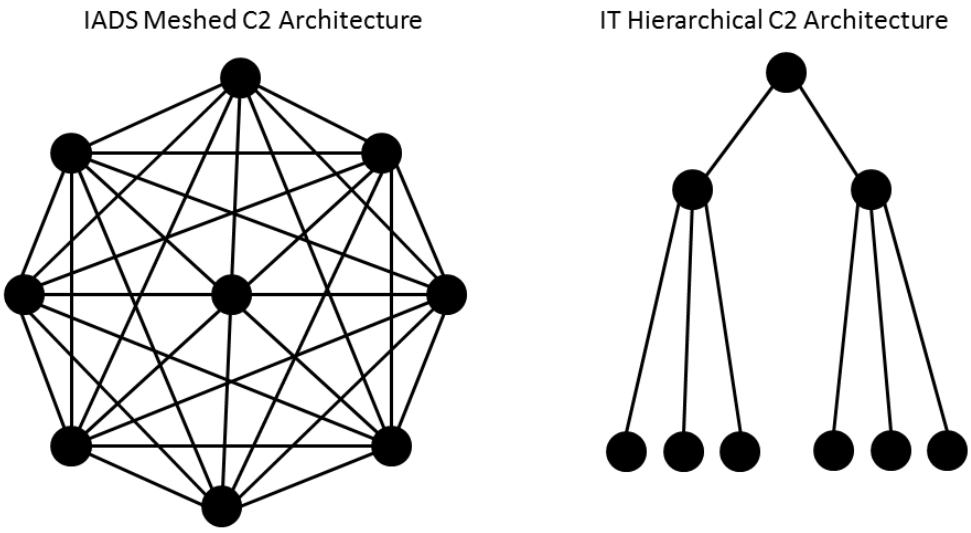

Figure 3. IADS and Network Defense Organizational Diagrams.

4.1. Command and Control

Effective C2 is the first requirement that an enterprise network defense construct and IADS share. Large enterprise networks have Network Operations Centers (NOC) that delegate to local information technology (IT) departments at operational locations for response actions, sometimes called "touch maintenance." When a compromise occurs, the local IT staff incident response team executes response actions on the operation center's behalf in order to remove infections. This construct roughly parallels the IADS SOC model. Both structures execute actions based on delegated authority and rely on coordination to accomplish their mission.

Aside from the similarities in organization, key differences in IADS and network defense are notable. There is significant confusion and blurring-of-the-lines between enterprise services and network defense. Depending on the situation, it is often difficult to determine who is responsible for taking action and which reporting chain should be used. Exacerbating the issue is the fracture between the operational chain and the administrative chain that often inhibits rapid defensive responses. The NOCs have the charge of directing local IT staff to remediate defensive deficiencies, but they have no means of administrative enforcement (Bishop, 2011). Furthermore, mission owners who rely on cyber services have no real-time visibility of their networks or the associated threats. Consequently, IT staffs often serve two masters, which delays response times and defeats effective collaboration. Due to the high volume of response actions that must be performed on enterprise-class networks, very little analysis is applied to the correlation of the attack to the mission at hand or attack vector. Additionally, organizations with similar missions are rarely alerted to determine if they have fallen victim to comparable attacks. By contrast, under the IADS model, the free flow of information up and down echelon coupled with streamlined C2 remove ambiguity of responsibilities and enables ABMs across the system to readily access the information that is important for defending assigned areas.

The current C2 maturity level of network defense operations approximates to the de-conflicted operational NNEC capability level, with a C2 maturity level of 2. The structure focuses on "avoidance of adverse cross-impacts between and among the participants by partitioning the problem space" (Alberts *et al.*, 2010). Operating at a low level of C2 maturity, there is no clear collective objective, limiting information sharing and interactions. To remedy the fractured command structure, the mission owner needs dedicated network analysts with the situational awareness necessary to adequately defend their area of responsibility. These personnel belong and report to the mission owner, but ultimately operate as a liaison under the authority (with appropriate privileges) to the NOC. Having ties to the local mission provides the context necessary to more effectively identify anomalous behavior and determine priority for assets under attack.

Using this structure, overall network defense more closely resembles an IADS collaborative construct, providing the mission owner near instantaneous appraisal of intrusions. This situational awareness and response capability alleviates the need for intervention with the intermediate and higher level echelons of the NOCs, allowing the delegation of decisions to the lowest possible level. The INDS model also makes situational awareness available to the operational and strategic echelons, providing oversight to the incident from all levels.

4.2. Threat Identification

A significant technical challenge in implementing an INDS is to identify adversaries that gain access to a network and are operating in a traditionally unobservable way, moving laterally from host to host. Typical network traffic sensing devices examine traffic only at perimeter gateways. Some enterprise antivirus solutions provide protection at the host level, but fail to allow network defenders the ability to observe interactions at the physical layer of communications. To counter this problem, the focus has to turn to identifying movements throughout the network.

Once an attacker gains access, they will attempt to gather more information about the network and enumerate other vulnerable computers in the enterprise. As described previously, the traditional boundary defense's outward looking approach is insufficient to ascertain threats as they traverse across the internal network since the sensors are only monitoring traffic entering and

exiting the network. In order to effectively carry out this mission, the network needs to be instrumented to identify and track the adversary as it is moves through the internal network. Only then will network defenders gain an understanding of the adversary's exploitation vector, methods of persistence, and intentions.

A mesh of networked sensors (devices placed to adequately observe low-level communications between nodes) is necessary to actively monitor an adversary's movements within the boundaries of the perimeter defense. Just as connecting the radar systems from field sites provides a consolidated air picture, these sensors enable the illumination of previously unobservable traffic. The sensor arrays consist of a combination of active and passive devices placed at operational locations to provide maximum visibility of all the hosts on the network. Under an INDS, these devices fall under the control of the resident network analysts, but are redirected to higher echelon organizations based on priority. Furthermore, when engagement is deemed appropriate, the sensors are able to facilitate reaction operations.

Through application of rule sets based on analysis from network controllers and automated trigger events, anomalous behavior can initiate automated response actions, such as full packet captures and alert analysts of irregularities. The automated response provides detailed information that increases the effectiveness of the network analysts by allowing an educated decision to be made at the lowest level.

The addition of sensors adds strength to the defensive structure by providing analysts the upper hand in investigations and response actions. The passive sensors enable a more tailored view of infected hosts without tipping off attackers that they are being monitored. Having more comprehensive information on attacks assists in root-cause analysis, identifying a possible motive for the exploit, attributing the event to an actor, and leads to a better understanding of adversary capabilities. Additionally, having a large array of sensors throughout the enterprise allows NOCs to sample a wider range of hosts to enable a more comprehensive search area during security audits.

One of the more impressive aspects of the IADS construct is the ability to take data from numerous sources, fuse it into one common platform, and enrich it with analysis to build the common air picture. There are a number of data sources available to assist in identifying exploitation attempts on a network that function in a similar manner to IADS sensors. Intrusion detection/prevention devices, firewalls, routers, switches, proxies, and hosts all produce logs that hold evidence detailing successful and unsuccessful intrusion attempts. Intrusion attempts always leave some trail of evidence; the challenge is deriving the exact trace information necessary to identify anomalous activity in the enormous amount of data from disparate sources. Most network defense appliances (e.g., firewalls, proxies and IDS/IPS) have management interfaces that analysts use to identify malicious activity. However, there is no integration between the systems; each looks at a separate aspect of the network, making correlation of incidents extremely difficult. Some commercial products such as ArcSight and Splunk attempt to bridge this gap, but there is no current way to share the information with the distributed enterprise without incurring significant licensing costs, making them suboptimal in the collaborative model. The security information and event management (SIEM) framework also attempts to create a common picture (Praste 2012). However, existing SIEM products today lack the breadth necessary to encompass the entire IADS cycle of identification to destruction.

In order to truly create a collaborative network defense environment, a paradigm shift must occur. The IT business model of large enterprise networks needs to transition into an intelligence collection model to assist in identifying adversaries as they traverse their corporate network. To stop the loss of intellectual property, the organization has to obtain information on those who wish to gather intelligence or steal from their organization. To do so, all of the data sources have

to be consolidated, parsed, scrubbed, normalized and placed in a real-time data repository to enrich analysis. In essence, this system needs to be an intelligence collection platform that gathers information about the network, correlating events from hosts and segments. Having this information allows for the creation of prediction models and enables proactive and automated response actions. The summation of the information gathered in data aggregation and processing will create a common network picture that every echelon of the INDS will utilize to facilitate collaboration and seamless response actions.

4.3. Battle Management

A major benefit from the IADS for the United States air defense mission is the collaborative work environment. The cohesive structure enables the monitoring of feeds from numerous entities and the remediation of threats through multiple agencies and authorities. To bridge this concept to network defense, analysis and decision support is necessary to accurately quantify the threat of an intrusion. Each level in the defensive construct is distinct in focus and information need, but all of the information necessary for each level is derivable using the same data. Using common data with tailored views at the tactical, operational and strategic levels ensures the most accurate data is available across the enterprise. The distributed model shares the burden on analytical resources and aids in identification of threats. Shared threat analysis and a situational awareness framework institute the collective INDS workforce against a common foe.

Once all the data is collected and fused for threat identification, network analysts throughout the enterprise are granted access to perform research based on their individual work roles. At the lowest level, the addition of a centrally managed network knowledge repository will allow mission owners to have insight to their area of responsibility. Managers are able to assign a local priority to each resource based on mission assurance criteria, allowing better response actions when necessary. The use of a common, centrally managed system will provide better oversight at the operational level, allowing for NOC, Computer Emergency Response Team (CERT), and location views for quality assurance roles and overall situational awareness. Contrary to most additional network defense capabilities, the use of a distributed active defense knowledge base will actually decrease the workload on the severely overtasked defenders at the NOC and CERT levels. Under this construct, nodal analysis and response actions are pushed down to the mission owners. This philosophy places more eyes on the targets, frees higher echelons to correlate events at different locations and generates an overall threat picture to enable sharing of information across the organization as required. Information sharing leads to a better understanding of the attacks which aids in identification of the perpetrator (Rashid, 2012).

At the strategic level, the common picture facilitates situational awareness via real-time decision support for events needing elevation or coordination with external entities. It also provides an overall threat picture of networks under their control in order to dispatch additional resources to areas with immediate needs. The seamless nature of cyber enables analysts and operators to focus on remote remediation of threats at other locations. The common platform facilitates a streamlined tasking mechanism down to the incident responders, reducing crucial time.

4.4. Engagement

When response actions are necessary to protect vital national interests for an IADS, units enable missile systems or scramble intercept aircraft to engage the threat. In the same manner, incident response teams track and seek to eradicate network-based threats. Response actions beyond the gateway are highly controversial, bringing in many ethical and legal concerns (Small, 2012). However, response actions within the boundaries of the corporate network are within the authority of network defenders.

Traditional incident response procedures focus on removing the intruder from the network and disrupting their means of ingress. For a determined adversary, this approach serves merely as a hurdle to their operations. Once identified, it is best to characterize the enemy to determine their infection vector, persistence mechanisms, and intentions before removing their access. The computer security firm Mandiant used this technique while investigating breeches in computer networks of The New York Times (Perlroth, 2013). Security investigators monitored attackers as they moved around the newspaper's systems, correlating known tactics with suspected compromised hosts and established operating times. The Times' security team watched the hackers for four months, identifying every back door and compromised computer before taking action. Having an increased understanding of the attack and attackers assisted Mandiant in attributing the actor as well as formulating a plan to eradicate all infections.

With the use of the collaborative INDS, it is possible to discover information about adversarial operations on the network through kill chain analysis. Lockheed Martin identified seven phases characterizing advanced persistent threats (APTs) in a network: reconnaissance, weaponization, delivery, exploitation, installation, C2, and actions or objectives. The computer security industry has largely adapted this model as the "cyber kill chain" (Croom, 2010; Hutchins, Cloppert & Amin, 2011). The goal of the defender is to break the chain and stop the attacker. If one link in the chain is removed, each subsequent link is affected or negated. To assist in obfuscating adversarial operations, each phase of the chain can occur at various locations across the network. When applied to a large enterprise, APTs are able to avoid multiple layers of security by performing small actions (such as sending only a few packets) over a large temporal period. During this period, the APT can target separate phases in the kill chain on numerous hosts across large distances without being detected. This level of stealth makes identifying an APT at one location difficult. However, with the use of an enterprise-wide collaborative system, it is possible to identify commonalities and overlapping indicators through dimensional correlation of intrusions (Hutchins, Cloppert & Amin, 2011).

Once an APT is discovered, this information is instantly pushed to the operational and strategic levels for decision support. The root-cause approach lends to a more survivable defensive posture and a better understanding of the adversary's capabilities. Outfitted with the right sensing and operational capabilities, coupled with decision support mechanisms, incident response teams are able to actively monitor an intruder from a distance in order to learn intentions, tactics, techniques and procedures. Based on rules of engagement and tasking from higher echelons, the response team can now actively control the threat. Options to eliminate, redirect, or continue to monitor the adversary are then able to be executed.

Table 2. INDS Application of IADS Construct

Function	Primary Attribute	Utilizes
Command and Control	Information Sharing, Tasking, Reporting	Various Communication Channels, Collaborative Tools
Threat Identification	Detect, acquire target, attribute actor, determine intentions/infection vector	Shared Threat Information, Firewalls, Proxies, IDS/IPS, Host-Based IDS, Advanced Sensors
Battle Management	Track/control target; monitor movements, gain understanding of capabilities	Common Network Picture, Collaborative Tools Automated Decision Matrixes
Engagement	Eliminate, redirect target	Incident Responders

Table 2 applies the key attributes of IADS to an INDS. Using this construct, it is possible to leverage efficiencies and lessons-learned from air defense. C2 channels take further advantage of collaborative tools across the enterprise to provide timely tasking and reporting mechanisms. Threat identification is bolstered through a common knowledgebase that leverages internet protocol address reputation, capability use, as well as signatures to understand adversarial means and methods. Battle management correlates historical threat information with active monitoring, enabling faster, and more accurate tracking of lateral movements throughout the network until the decision is made to engage the target. Together, these attributes form a cohesive system that enables threat identification and elimination across large networks.

5. Conclusions

Despite the continued advances in perimeter defense, enterprise networks are still vulnerable to infiltration by persistent adversaries. Current network configurations lack the ability to provide defenders true visibility down to the host level. If network defenders do not have discernibility on the wire at all levels, they do not have insight to all possible intrusion attempts and attack vectors. Furthermore, without a collaborative system to facilitate defensive actions, network defenders and mission owners do not communicate vital information to the end mission.

This paper presented how attributes of an IADS are applicable to the active network defense of large, distributed enterprise networks. The characteristics of C2, threat identification, battle management, and engagement each have comparisons in network defense. Integrating these characteristics across echelons and geographically separated locations lessens the adversary's advantage through correlation of threat indicators.

Developing an integrated network defense system will create a cyber environment with increased situational awareness and shared knowledge. Through the use of collaborative, agile C2, and improvements to collection mechanisms, a common network picture is formulated to provide seamless situational awareness from the tactical level to the strategic level. This cognizance facilitates the ability to actively monitor, control and eliminate adversarial actions on enterprise networks.

NOTE: The views expressed in this paper are those of the authors and do not reflect the official policy or position of the United States Air Force, the Department of Defense, or the United States Government.

6. BIBLIOGRAPHY

Alberts, David S., Reiner Huber, James Moffat. DoD Command and Control Research Program. SAS-065. NATO NEC Command and Control Maturity Model. February 2010. Accessed April 14, 2013. http://www.dodccrp.org/files/N2C2M2_web_optimized.pdf

Arnold, Chad, Jonathan Butts, Krishnaprasad Thirunarayan. Strategies for Combating Sophisticated Attacks.

Bishop, Benjamin W. An Assessment of Napoleonic Command and Control Principles in Air Force Network Defense Operations. Air Force Institute of Technology Graduate Research Project. Wright-Patterson Air Force Base, Ohio, June 2011.

Brancik, Kenneth. Insider Computer Fraud: An In-depth Framework for Detecting and Defending against Insider IT Attacks. Auerbach Publications. 2008.

Checkland, Peter and Holwell, Sue. "Information, Systems and Information Systems–making sense of the field". Chichester: Wiley, 1998.

Croom, Charles. (2010). The Cyber Kill Chain: A Foundation for a New Cyber Security Strategy. *High Frontier: The Journal for Space and Cyberspace Professionals* , *6*(4), Retrieved from http://www.afspc.af.mil/shared/media/document/AFD-101019-079.pdf

Davis III, Curtis W., James M. Flavin, Robert E. Boisvert, Kyle D. Cochran, Kevin P. Cohen, Timothy D. Hall, Louis M. Hebert, and Ann-Marie T. Lind. "Enhanced Regional Situation Awareness." Lincoln Laboratory Journal. 16. no. 2 (2007): 355-380.

Deeney IV, John J. "FINDING, FIXING, AND FINISHING THE GUIDELINE: The Development of the United States Air Force Surface-to-Air Missile Suppression Force During Operation Rolling Thunder." All World Wars. . http://www.allworldwars.com/Finding-Fixing-Finishing-Guideline.html (accessed January 4, 2013).

Rashid, Fahmida Y. "Cyber revenge is a dish best served by sharing threat data." SC Magazine, June 21, 2012. http://www.scmagazine.com/cyber-revenge-is-a-dish-best-served-by-sharing-threat-data/article/246820/ (accessed September 23, 2012).

Gleick, James. The Information: A History, A Theory, A Flood. New York: Vintage Books, 2011.

Hutchins, E., Cloppert, M., & Amin, R. (2011, March). In Julie Ryan (Chair). *Intelligence-Driven Computer Network Defense Informed By Analysis Of Adversary Campaigns And Intrusion Kill Chains*. Presentation Delivered at 6th international conference on information warfare and security, The George Washington University, Washington, DC, USA. Retrieved from http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf

"Huge "Ear" Locates Planes and Tells Their Speed." Popular Mechanics, December 1930.

Kadrich, Mark. "High-speed IDS: The search for the Holy Grail...." July 26, 2000. September 23, 2012. https://www.blackhat.com/html/bh-usa-00/bh-usa-00-speakers.html

Lin, Da and Stamp, Mark. Hunting for undetectable metamorphic viruses. Journal in Computer Virology, Volume 7, Number 3 (2011), 201-214. 2011.

Macfadzean, Robert. Surfaced-Based Air Defense System Analysis. Boston: Artech House, 1992.

McConnell, Mike. "Mike McConnell on how to win the cyber-war we're losing." *Washington Post*, wshingtonpost.com edition, sec. Outlook & Opinions, February 08, 2010. http://www.washingtonpost.com/wp-dyn/content/article/2010/02/25/AR2010022502493.html (accessed October 31, 2012).

National Security Agency, "Defense in Depth: A practical strategy for achieving Information Assurance in today's highly networked environments. ." Accessed September 23, 2012. http://www.nsa.gov/ia/_files/support/defenseindepth.pdf.

Oquendo, J. "Why Defense in Depth Will Never Be Sufficient." *Infosecisland* (blog), March 31, 2011. http://infosecisland.com/blogview/12742-Why-Defense-in-Depth-Will-Never-Be-Sufficient.html (accessed September 23, 2012).

Perlroth, Nicole. "Hackers in China Attacked The Times for Last 4 Months." The New York Times, , sec. A1, Janurary 31, 2013. http://www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html?pagewanted=all (accessed February 1, 2013).

Praste , Omprakash Singh. "What is SIEM?." OMWINDOWS (blog), http://ankomwindows.cfsites.org/custom.php?pageid=43560 (accessed September 23, 2012).

Small, Prescott E. "Defense in Depth: An Impractical Strategy for a Cyber World." SANS Institute InfoSec Reading Room. (2012).

U.S. Department of the Air Force. Multi-Service Tactics, Techniques ,and Procedures For an Integrated Air Defense System (AFTTP 3-2.31; FM 3-01.15; MCRP 3-25; ENTTP 3-01.8). Washington, May 2009. http://www.scribd.com/doc/36514061/46/Figure-13-NCR-IADS-Command-Relationships