Information Protection Technician

Cyberspace Defense Technician (MOS 255S)

By CW5 Todd M. Boudreau

Where We Were

The analogy in this article is like a parable that will help you understand the multidimensional arena into which the Army is deploying expert cyberspace defense technicians.

To fully grasp the analogy you have to understand that our current cyberspace defensive measures are almost entirely reactive in nature.

Most often, adversarial activity is identified by the loss of critical data and/or the malicious manipulation of data elements and devices. After the fact, forensics often discover that such adversarial activity had been going on for quite a significant amount of time before it was discovered. At this point a "signature" is created and placed in devices that are used to look for such adversarial activity. These devices look at current activity and if any matches this "signature" they then alert and activate devices that detect or in some cases prevent further adversarial activity. If placed on a scale in its simplest of forms, it would look something like figure 1 below.

Having established a protected posture, we scan our networks for evidence of adversarial activity by comparing cyberspace activity against our current signatures and various indications and warnings established and in place at the time. Once an adversary has established intent to attack our networks, an operational preparation of the environment sets the way for an attack which then may present a viable avenue to exploit our networks and extract critical information. Once an attack and/or exploit are defeated, we begin the process of remediation to correct any faults, deficiencies, and/or vulnerabilities that created the threat. The defeated adversary then slightly changes the toolset in order to launch a new attack. More sophisticated adversaries create toolsets that automatically morph on their own in order to prevent detection or the capability of the remediation from being successful.

Finally, as the effects of Army transformation and technological advances have caused MOS 254A to shift into a role that mirrors MOS 251A, when both MOS were present in the same organization, the 251A has historically gravitated toward the NetOps elemental gap of Information Assurance and Computer Network Defense (IA and CND respectively). However, few 251A were properly trained and none received any institutional training. Furthermore, few 251A were able to ensure consecutive assignments in such positions making it difficult to impossible to build upon skills and experience.

Where We Are Heading

The current methods are completely inadequate for a variety of reasons. First, we cannot afford to allow adversarial activity to occur unnoticed for any amount of time before we detect and take action. Second, more and more we find our adversaries are using polymorphic malware which means that the adversarial activity continues changing to make it almost impossible to stop with signature-based defensive measures. Instead, we need to begin focusing on

(Continued on page 36)

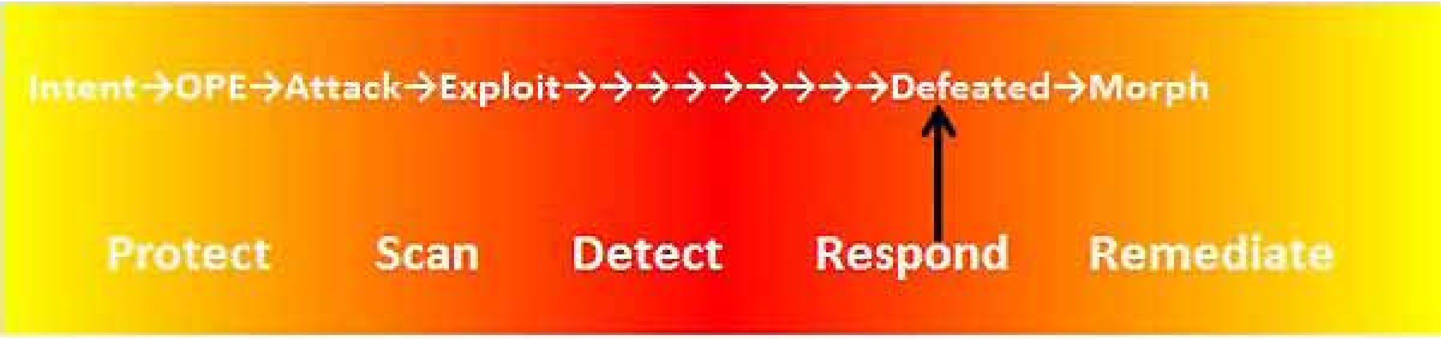

Figure 1 Current Scale Comparing Attack and Defense Cycles

(Continued from page 35)

anomalous activity.

This is not an entirely new concept. Credit and banking systems have been doing this for years. Recently when my credit card had been refused, I immediately contacted my financial institution. They asked me two questions: had I recently charged $1 to a common on-line DVD and Blu-ray disc rental-by-mail and video streaming company and had I recently charged $1 to a not-so-common on-line clothing store. I had done neither. This activity was uncommon to my nominal purchasing history and was viewed as an anomaly. This caused my credit card to be flagged. With a credit card, no funds are immediately transferred. Therefore, they were able to put a hold on my account and eventually disapprove the transactions with no money lost.

I advocate an anomaly based cyberspace defensive posture that moves the "detect and respond" further to the left of the attack cycle as illustrated below in figure 2. However, this calls for some changes in operations. Instead of the adversarial attack or exploit tipping our defensive measures, we must respond to the adversarial OPE. Let me make this clear with the analogy.

Defending a Field

Some have described the nature of cyberspace defense as trying to find a needle in a pile of needles. The point of this illustrative presentation is that there are so many alerts to possible malicious activity on our networks, we are consumed wading through the plethora of false positives (i.e., alerts, indications, and warnings that turn out to be nothing) and/or inconsequential positives (i.e., those that are of little to no concern) that we miss the truly important indications and warnings allowing adversarial activity to continue unchecked for an unacceptable amount of time.

We miss the truly important alarm in the midst of the overwhelming noise of alarms. This needle in a pile of needles illustration accurately presents the issue at hand. Finding the important alert amongst the blaring myriad of alerts is truly like trying to find a special needle in a pile of needles, which also continues to grow in number by the minute. While this illustration has a lot of merit under these circumstances, much more needs to be understood beyond this one critical issue – especially in order to best present the need and capability of the Army's expert cyberspace defense technician.

Imagine a field of grass where each blade is part of an integrated and monitored root system. Any pressure on the field has the ability to trip a sensor and send a warning of a presence upon the field. An adversary wants to step on our field and disrupt, exploit, or destroy those operations which we conduct on and through this field.

However, to step on even a single blade may tip off his presence. So he introduces malicious grass seed into our supply of grass seed. The sheer amount of grass seed sowed into the field makes it impossible to verify every single seed. As the malicious seed begins to grow and take root, it soon provides a patch of grass that allows the adversary a foothold on our field.

Before we get to advancing the "detect and respond" to the left, we must add two exasperating situations. First, the field has also become overgrown with weeds and saplings providing our adversaries cover as they step onto the patch of malicious grass. Secondly, the current field includes friendly plots of sod which are not centrally managed by the larger defender of the field itself.

For unveiling the analogy, let me reveal here that these patches of sod represent the disparate networks that are currently kluged together within the confines of Army cyberspace. And finally the weeds and saplings are the result of poor IA practices. IA practiced upon cyberspace has been likened to preventative maintenance checks and services. Taking a higher view of IA, I include not only patching and IA vulnerability alert response compliance, but also total asset visibility and network transparency.

At the most recent Signal conference at Fort Gordon, MG Rhett Hernandez, Army Cyberspace Command commanding general, mentioned three interrelated aspects of one significant effort that is necessary as part of mak-

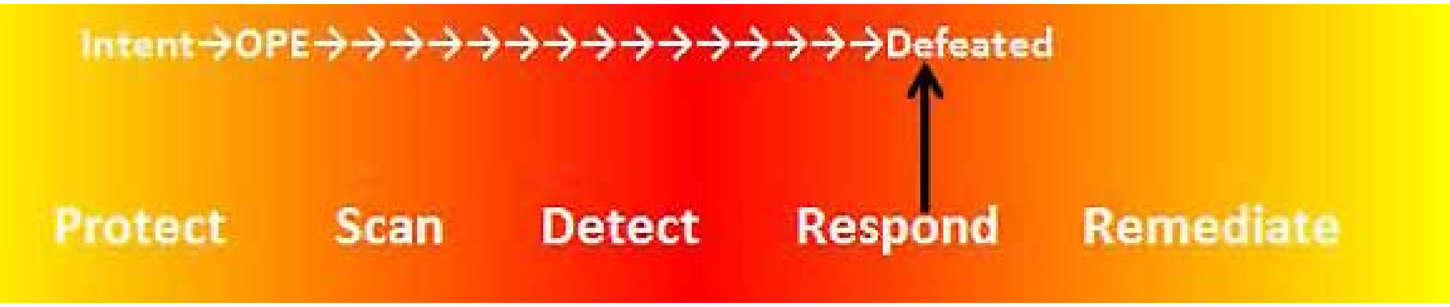

Figure 2 Future Scale Comparing Attack and Defense Cycles

ing cyberspace securely operational. The first two are to know ourselves and to know our enemy. The third is know the terrain one intends to defend. We must first see our cyberspace terrain if we are to effectively defend our cyberspace terrain.

Setting these two immense problems aside (i.e., disparate networks and poor IA), let's revisit that analogy to ensure we are tracking. The seeds represent normal network traffic that is nearly impossible to detect in advance of an attack even if it is malicious. For example, I am not talking about spam or low-tech phishing attacks. I am instead alluding to highly sophisticated attempts to attack our networks through e-mail traffic (for example) that have been crafted by a high-tech peer adversary. Most experts today admit this cannot be stopped. But the e-mail is only carrying a malicious seed that by itself is yet inert. However, as it begins to grow and root, before it has time to become a patch that allows even a toehold, it must be detected and defeated.

In the physical domain of the field of grass in my analogy, the first step is to establish a field-of-fire. Basic warrior tasks and battle drills teach a couple of basic principles in establishing a field-of-fire. First, one must determine how big the field can be and still be scanned effectively against the adversary. Second, one ensures overlapping fields-of-fire to prevent against a seam (at best) or a gap (at worst) which could allow the adversary an avenue of approach through our defenses. If the magnitude of adversarial activity that is to be detected is as small as a blade of grass, the field-of-fire must be small enough to remain manageable.

In the cyberspace domain, we must also default to these basic level cyberspace WT&BD and establish fields-of-fire that are manageable and include overlapping and interlocking fields-of-fire. These malicious e-mails don't plant grass. They plant hooks that provide a point of presence in our networks and data devices. Our cyberspace defenders must be able to scan their sector and detect such malicious PoPs in order to defeat them while the adversary is still in the OPE phase of the attack. Cyberspace defenders must see these hooks as anomalous to their cyberspace fields-of-fire.

One last thought is appropriate before moving on to the practical aspects of discussing MOS 255S. To quickly identify an anomaly, one must be able to quickly discount what is normal. Begging your patience to use another analogy, if someone is going to quickly, efficiently, and effectively defend your office building against a physical attack, such as an explosive device, they best know what normal looks like. Each desk, each box, each copy machine, each piece of furniture or physical structure that could be a fake planted by an enemy and secretly housing an explosive device should be readily identifiable by the defender if one plans to be successful. Similarly, if our cyberspace defenders are not familiar with the network and networked data devices, they are ill prepared to notice an anomaly during the OPE phase of the adversarial attack.

For the best defense posture, cyberspace defenders must live in the space they are assigned to defend. They must sense the anomaly within the normal as early as possible – before the adversary even gets a toehold. Know that we must move forward in this direction immediately. We have no time to wait. We are unquestionably beyond phase zero in cyberspace operations conducted in and through the cyberspace domain today.

Enter the Cyberspace Defense Technicians

The below NetOps construct in figure 3 continues to show its three elements which are also the Regiment's three major core competencies. Previous articles have already addressed MOS 255A (responsible for Cyber Content Management) and MOS 255N (responsible for

(Continued on page 38)

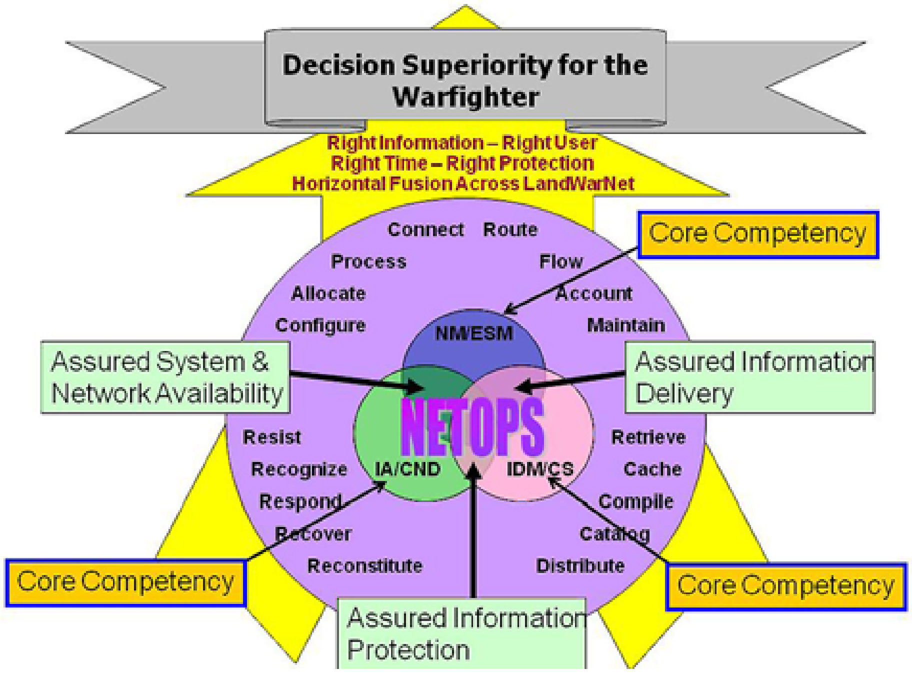
Decision Superiority for the Warfighter
Right Information – Right User
Right Time – Right Protection
Horizontal Fusion Across LandWarNet
Core Competency
Connect
Route
Process
Flow
Allocate
Account
Configure
Maintain
NM/ESM
Assured System & Network Availability
NETOPS
Assured Information Delivery
IA/CND
IDM/CS
Resist
Recognize
Respond
Recover
Reconstitute
Retrieve
Cache
Compile
Catalog
Distribute
Core Competency
Core Competency
Assured Information Protection

Figure 3 Network Operation Construct

(Continued from page 37))

Cyber Network Management); the last article in this particular series will address MOS 255Z (responsible for Cyber NetOps (CyNetOps) in its entirety).

This article now moves to describe MOS 255S (responsible for Cyber Defense) as the newest personnel capability added to the Signal warrant officer cohort.

As we began to look at the capability gap at hand (IA/CND), we made a couple of decisions up front. First, we realized the need to move from a perimeter-positioned and reactionary defensive model to an internally proactive, anomaly based, true defense-in-depth model. Second, knowing the interdependencies of CyD, CyCM and CyD, CyNM, we concluded the need for a more senior and experienced personnel base. Third, we acknowledged the current standard of CyD training to be in the hands of our commercial IT partners. Finally, we recognized the necessity of partnering with our Intelligence Community partners who can provide actionable intelligence relative to our adversaries' intent--their tactics, techniques, and procedures; and any real time feedback on both their current activities as well as their knowledge of ours.

A properly trained and deployed MOS 255S force will be key in meeting the first issue above. In order to move to an internally proactive, anomaly based, true defense-in-depth model, we need an intelligent personnel capability to be a part of the solution set.

To ensure that CyCM and CyNM efforts are not negatively affected, but supported and reinforced, it was decided that MOS 255S would not be an enlisted-level accession MOS. Instead, accessions into MOS 255S will be at the senior W2 grade. This is in line with preferred attendance at the Warrant Officer Advance Course. This ensures newly reclassified 255S have a greater understanding of their actions and the suggestions they make in the CyCM and CyNM areas to better posture for defense. Training will be discussed below. However, the requirement for all 255S to hold a top secret clearance with the ability to be read on to special compartmentalized information is of utmost importance. This allows the IC to feed actionable intelligence into the CyD cell.

Since there are no apprentice cyberspace defense technicians, it is imperative that we get our training right. The transition course from MOS 255S will also serve to give advance course credit (i.e., it will also function as a WOAC).

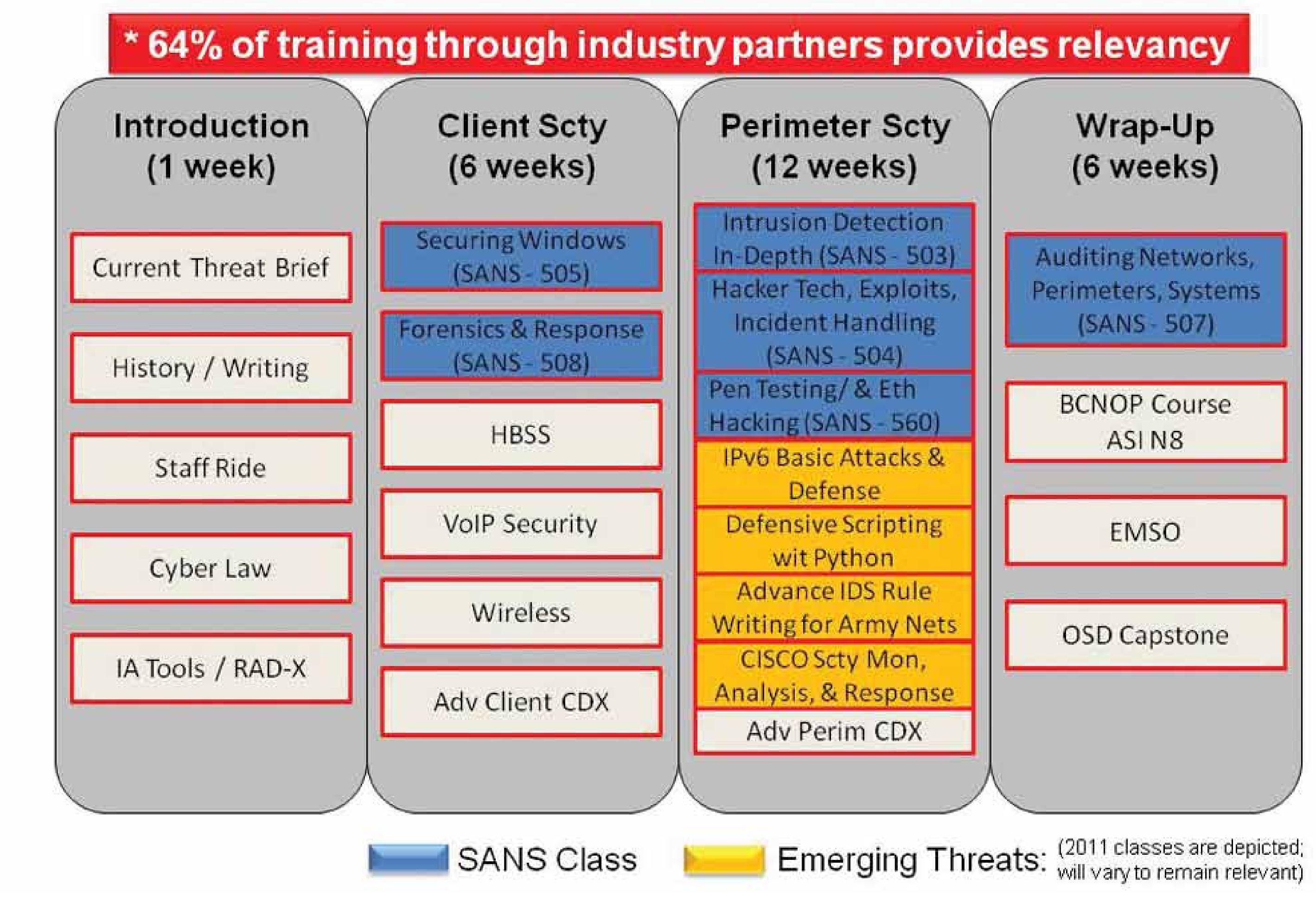
* 64% of training through industry partners provides relevancy
Introduction (1 week)
Current Threat Brief
History / Writing
Staff Ride
Cyber Law
IA Tools / RAD-X
Client Scty (6 weeks)
Securing Windows (SANS - 505)
Forensics & Response (SANS - 508)
HBSS
VoIP Security
Wireless
Adv Client CDX
Perimeter Scty (12 weeks)
Intrusion Detection In-Depth (SANS - 503)
Hacker Tech, Exploits, Incident Handling (SANS - 504)
Pen Testing/ & Eth Hacking (SANS - 560)
IPv6 Basic Attacks & Defense
Defensive Scripting wit Python
Advance IDS Rule Writing for Army Nets
CISCO Scty Mon, Analysis, & Response
Adv Perim CDX
Wrap-Up (6 weeks)
Auditing Networks, Perimeters, Systems (SANS - 507)
BCNOP Course ASI N8
EMSO
OSD Capstone
🟦 SANS Class
🟨 Emerging Threats: (2011 classes are depicted; will vary to remain relevant)

Figure 4. Current 255S Pilot Course Training Course Map

The most credible and holistic CyD training currently resides in the hands of our commercial IT partners. CISCO has a robust perimeter security track of training and the SANS Institute has a number of courses that meet both our client and perimeter training needs as well as a number of other very specific areas to be addressed. Figure 4 below is our current 255S course map.

Journeyman Cyberspace Defense Technicians

MOS 255S are the Army's premier defenders of the Army's portion of the cyberspace domain. They perform computer network defense measures and advise information assurance measures and actions to include the protection, detection, and reaction functions at all levels in support of combat information superiority. Junior 255S (i.e., W1 and W2) do not exist. Instead, junior WOs who may look to access into 255S should focus on acquiring and refining technical and administrative skills within their respective MOS (i.e., 255A or 255N). As they develop these skills and achieve mid-grade CW2 status, should they desire to pursue MOS 255S, they should begin self-study in the cyber defense field, seek to find a senior 255S as a mentor, and look to fill information assurance management positions that will lead them to meeting the 255S prerequisites. IAM positions may be either focused on IA compliance in CyCM or CyNM.

Mid-grade 255S (W3) advise information assurance efforts while focusing on their associated sub-element (i.e., cyber defense) as well as non-lethal electronic protection efforts. They supervise associated personnel and oversee functions within the standards, transport, services, and applications layers of the network in order to achieve confidentiality, integrity, and availability of information, as well as the authentication and non-repudiation of users. They also supervise and/or oversee subordinate sections required to support information protection and network defense such as communications security sections, cryptographic network planning, and electromagnetic spectrum operations to achieve electronic protect, and the implementation and use of electronic keys required supporting communications networks and networked-systems. See figure 5.

It is imperative that commanders and senior leaders understand that MOS 255S will not oversee IA compliancy. MOS 255S are required to know normal and hunt in our portion of cyberspace to identify and defeat adversarial activity. Not all adversarial activity will be defeated. The 255S provides the Signal Regiment a basis to enter into full-spectrum cyberspace operations with our IC partners. The use of deception, cyberspace counter-fire, and adversarial cordoning are just a few of the TTPs a full-spectrum cyberspace operation may use. Therefore, to limit MOS 255S to IA is a colossal waste of talent and completely misses the point of the MOS. Journeymen 255S may advise IA and analyze IA deficiencies to give the "so what" to their respective commanders. They are able to determine the difference between vulnerability and an actual threat and can provide mitigation courses of action.

These journeymen 255S perfect the art of knowing normal by a continued and in-depth analysis of the various feeds received from sensors, data devices, and actionable intelligence received from various IC sources. Unlike the CyCM and the CyNM, it is the journeymen CyD who is nominally assigned to a brigade combat team where he/she has the greatest ability to encounter the widest array of devices and applications found within the breadth of his/her assigned systems. This also makes the 255S the senior Signal warrant officer in most formations. Journeymen 255S also find themselves in theater network operations security centers, regional computer emergency response teams, and a number of similar hands-on organizations to include as high as combat divisions.

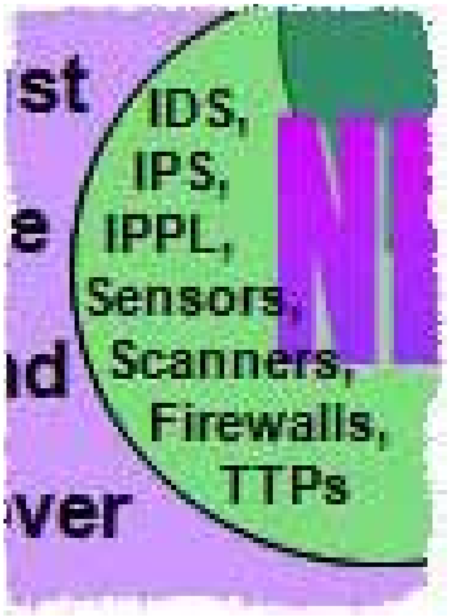

Figure 5

Master Cyberspace Defense Technicians

Senior 255s (i.e., newly promoted W4), quickly master applications, techniques, systems, and CyD attributes which include actions to resist, recognize, respond, recover, and reconstitute. Highly specialized and highly motivated, they quickly inculcate these and move from the outer edges of the CyD circle in this Venn diagram toward the center. They too are now moving from mastery of one element toward the goal of W5--mastery of NetOps.

Master CyDs, as senior-level technical and tactical experts in their chosen field, have also gained familiarity with the other two elements of NetOps (i.e., CyCM and CyNM). As they continue to develop as CW4 255S, they go beyond understanding the basic con

(Continued on page 40)

(Continued from page 39)

cepts of information protection and assured system and network availability and ensure that these attributes of NetOps are obtained. See figure 6. Their prior experience as either 255As or 255Ns is key to their rapid expansion of knowledge.

The master CyD is nominally assigned to a corps, ASCC, and higher level organization where their training and experience has its greatest impact. To prepare the CW4 255S for the duties and responsibilities encountered at these levels of organization, attendance at the Warrant Officer Staff Course is crucial.
The master CyD will be, without argument, today's intellectual capital to ensure the Army not only meets its future demands within and through cyberspace, but that it is secured and defended. While this may not be a new problem-set, its scope has grown significantly. Past generations of Signal equipment were mainly proprietary and circuit-switched. As such, the obstacle between our adversary and our critical systems was quite large and almost insurmountable. Mobile subscriber equipment and TRI-TAC systems were proprietary and not easily reproducible by others. A significant amount of intellectual capital and funding were required to acquire, reverse engineer, fabricate, and reproduce such equipment by our adversaries. Additionally, the circuit-switched nature of MSE and TRI-TAC networks made it very difficult to introduce rogue equipment into our networks with the intent to exploit or disrupt.

Today, these barriers have all but disappeared with our reliance on commercial off-the-shelf equipment. Almost anyone with inclination can find a virtual potpourri of attack toolsets from which to choose. A malicious personality merely chooses from a variety of desired cyberspace effects much like one picks from an assortment of foods at al buffet restaurant. Attribution is made difficult with the virtual, non-contiguous, yet ubiquitous nature in which cyberspace presents itself. One merely needs to walk into a busy hotel and use the hotel's business center as a platform to launch a cheap, unsophisticated, yet often effective attack against our networks.

Presently, even a low-tech attack often overwhelms our primarily reactive defenses inundated with a myriad of false-positives. This creates another source of noise that helps to mask more complicated, high-tech, peer adversarial activity. IA compliance may lower the noise-floor making the former easier to spot, identify, categorize, and remediate. However, more complicated, high-tech, peer adversarial activity requires an expert cyberspace defense technician who is fully equipped, informed and actively hunting anomalies within our complex networks and systems.

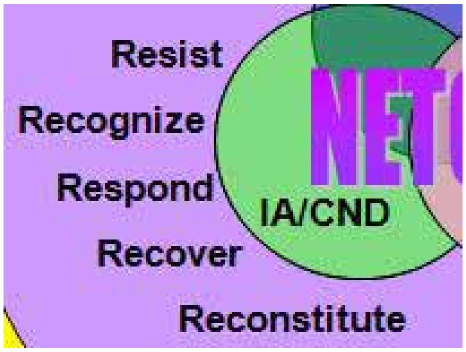

Figure 6

Subsequent to promotion to CW5, the master CyD also becomes part of an ever smaller, elite group of Signal warrant officers, the cyberspace network operations technician, MOS 255Z.

As will be done for all 255Z, senior leadership will be cognizant of their past MOS and as such leverage their knowledge, skills, attributes, and experience for future assignments. For further information on MOS 255Z, an article summarizing their career paths and describing their skills, attributes, duties, and responsibilities is included on page 48 in this edition of the *Army Communicator.*

Join the Discussion
https://signallink.army.mil

ACRONYM QuickScan

ARCYBER – Army Cyberspace Command
ASCC – Army Service Component Command
CND – Computer Network Defense
COMSEC – Communications Security
CyCM – Cyberspace Content Management
CyD – Cyberspace Defense
CyNetOps – Cyberspace Network Operations
CyNM – Cyberspace Network Management
CyNOT – Cyberspace Network Operations Technician
DVD – Digital Versatile Disc
EMSO – Electromagnetic Spectrum Operations
IA – Information Assurance
IAM – Information Assurance Management
IAVA – Information Assurance Vulnerability Alert
IC – Intelligence Community
MOS – Military Occupational Specialty
MSE – Mobile Subscriber Equipment
NetOps – Network operations
OPE – Operational Preparation of the Environment
PMCS – Preventative Maintenance Checks and Services
PoP – Point of Presence
R-CERT – Regional Computer Emergency Response Team
SCI – Special Compartmentalized Information
T-NOSC – Theater Network Operations Security Center
TS – Top Secret
TTP – Tactics, Techniques, Procedures
WOAC – Warrant Officer Advance Course
WOSC – Warrant Officer Staff Course
WOSSC – Warrant Officer Senior Staff Course
WT&BD – Warrior Tasks and Battle Drills