The Library of Sparta

David Raymond, Gregory Conti, and Tom Cross

Abstract

Abstract: On today's increasingly militarized Internet, companies, non-profits, activists, and individual hackers are forced to melee with nation-state class adversaries. Just as one should never bring a knife to a gunfight, a network defender should not rely on tired maxims such as "perimeter defense" and "defense in depth". Today's adversaries are well past that. This paper provides key insights into what we call the Library of Sparta - the collective written expertise codified into military doctrine. Hidden in plain sight, vast free libraries contain the time-tested wisdom of combat at the tactical, operational, and strategic levels. This is the playbook nation-state adversaries are using to target and attack you. We will help you better understand how adversaries will target your organization, and it will help you to employ military processes and strategies in your defensive operations. These techniques scale from the individual and small team level all the way up to online armies. This work isn't a dry index into the library of doctrine, we provide entirely new approaches and examples about how to translate and employ doctrinal concepts in your current operations.

I. Introduction

Whether you like it or not, if you are charged with defending a network, you are facing nation-state adversaries. It is no longer sufficient to be "just a little more secure than the other guy". Our enemies in the digital world will target both of you. And they will probably be successful.

Many people in the computer security community use words like "OPSEC", "Kill Chain" and "intelligence-driven" without fully understanding the underlying concepts. Even worse, many show their ignorance by using military jargon incorrectly, thereby alienating clients, customers, and colleagues. These concepts are powerful and should not be ignored, but they must be well understood before they can be leveraged in your network.

Here we describe resources that you can give you insights into how the enemy uses military strategies to attack your network, and how you can use similar strategies to defend it. Attackers have a clear intelligence advantage over defenders when it comes to vulnerabilities, malware, and open source information. We will help defenders generate the intelligence, information, and disinformation advantage necessary to turn the tables. You will gain an entirely new arsenal of military-grade strategies that will help you advance your work beyond the individual and small team level and will prepare you to take on the most advanced adversaries.

II. Dead White Guys - Foundations of Military Strategy and Doctrine

Much of U.S. military doctrine is based on the writings of a handful of military theorists. Primary among them is Carl Von Clausewitz, a German general and military strategist of the early 19th

century whose book, On War[1], is widely read by military leaders around the world. Clausewitz rightfully saw military action solely as a tool to gain political aims and famously said that "war is the extension of politics by other means." Another early 19th century military theorist was Antoine-Henri (Baron Von) Jomini, whose book The Art of War[2], is another staple among contemporary military leaders . Jomini wrote extensively on the Napoleonic wars and is called by some the "founder of modern strategy."

Much of U.S. Navy doctrine is based on the work of Alfred Thayer Mahan, a 19th century Navy Admiral, historian, and strategist. Mahan's writings shaped U.S. Naval doctrine during the 19th and 20th centuries, leading the U.S. to becoming one of the world's major sea powers.

William "Billy" Mitchell was a pilot in the US Army Air Corps during the first world war, and by the end of the war, was in command of all US air assets. Widely referred to as the "father of the US Air Force", Mitchell's work was the foundation of US Air Force doctrine[3]. A more contemporary air power theorist is Colonel John Boyd, a decorated US Air Force fighter pilot during the Korean and Vietnam wars[4]. One of Col. Boyd's contributions to military thought is the OODA Loop, or Observe, Orient, Decide, Act cycle. According to Boyd, decision making occurs in this recurring cycle and an individual (or organization) that can do this faster than their adversary, or get 'inside their OODA loop', will prevail.

Other historical military theorists of note include Xenophon, a Greek historian, soldier, and strategist and a Student of Socrates, and Sun Tzu, a Chinese general, philosopher, and strategist born in approximately 500 BC. More contemporary examples include Dennis Hart Mahan, a military theorist in the spirit of Jomini and a West Point professor (and father of Alfred Thayer Mahan), J.F.C. Fuller, a British Army officer and theorist of early modern armored warfare, Heinz Guderian, a German field marshal and armored warfare theorist, and B.H. Liddell Hart, a British soldier, military historian, and military theorist. Giulio Douhet was an Italian general and air power theorist of the early 20th century. Mao Zedong[5] was a guerrilla warfare strategist, Vo Nguyen Giap was a North Vietnamese Army general and insurgency strategist and architect of the Tet Offensive, Easter Offensive, and Ho Chi Minh Campaign. Finally, David Kilcullen is a contemporary Australian author, strategist, and counterinsurgency expert.

---

[1] Carl von Clausewitz, *On War*, Originally published: 1832 [Online]. Available: http://www.clausewitz.com/readings/OnWar1873/TOC.htm [Accessed April 2014].

[2] Jomini, Antoine Henri, baron von. *The Art of War*, Originally published: 1862 [Online]. Available: http://www.gutenberg.org/ebooks/13549. [Accessed April 2014]. Jomini's work should not be confused with Sun Tzu's work of the same name. While Sun Tzu is credited with writing a laundry list of platitudes concerning warfare, Jomini's treatment was written in the context of modern warfare and provides deep analysis of conduct thereof.

[3] Mitchell, William. *Winged Defense: The Development and Possibilities of Modern Air Power--Economic and Military*. The University of Alabama Press, Tuscaloosa, AL. 1925.

[4] Coram, Robert. *Boyd: The Fighter Pilot Who Changed the Art of War*. The Little, Brown and Company, May 2004.

[5] Mao Zedong. *On Guerilla Warfare*, [Online]. 1937. Available: http://www.marxists.org/reference/archive/mao/works/1937/guerrilla-warfare/. [Accessed May 2014].

III. "What is this 'doctrine' of which you speak?"

We use the word 'doctrine' as shorthand for 'military doctrine,' which is defined as "fundamental principles by which the military forces or elements thereof guide their actions in support of national objectives. It is authoritative but requires judgment in application."[6] Doctrine helps standardize operations and helps to provide a common frame of reference among military commanders.

In military parlance, the term 'joint' refers to two or more of the armed services working in concert[7]. The canon of U.S. joint doctrine, codified in a series of documents called Joint Publications ('Joint Pubs' or JPs) apply to all of the services. Each service then publishes service-specific doctrinal manuals to interpret and apply joint doctrine to their specific service. Both joint and service-specific doctrinal manuals are numbered using the continental staff numbering system given in the list below[8]. As an example, the "2 series" manuals cover intelligence functions. Army Field Manual (FM) 2-0 is entitled "Intelligence Operations" and gives an overview of how the Army approaches the intelligence function. Other 2-series manuals cover specific aspects of intelligence operations, for example, FM 2-91.4 is entitled "Intelligence Support to Urban Operations."

- 1, manpower or personnel
- 2, intelligence
- 3, operations
- 4, logistics
- 5, plans
- 6, signal (communications or IT)
- 7, training
- 8, finance and contracts
- 9, civil-military operations or civil affairs

A comprehensive offering of U.S. Joint Doctrine can be found on the DOD's Joint Electronic Library website[9]. The authors are most familiar with U.S. Army doctrine and will primarily rely

[6] This definition comes from the United States DOD Dictionary of Military Terms website at http://www.dtic.mil/doctrine/dod_dictionary/. This online dictionary provides a comprehensive, authoritative source of U.S. military definitions.

[7] Interservice cooperation was largely nonexistent previous to the Goldwater-Nichols Act of 1986, which increased the powers of the Chairman of the Joint Chiefs of Staff, streamlined military chains of command to bypass the service chiefs and go directly to combatant commanders, and required senior officers to serve in joint positions as a prerequisite to promotion to senior positions.

[8] Wikipedia.org, "Staff (military)", [Online]. Available: http://en.wikipedia.org/wiki/Staff_(military). [Accessed April 2014]. This wikipedia article provides a good discussion of how military staffs are organized and the responsibilities of each component.

[9] The U.S. Joint Electronic Library is at http://www.dtic.mil/doctrine/.

on such during this discussion. Army publications can be found on the Official Department of the Army Publications and Forms website[10].

IV. Key Principles and How to Apply Them

In the following paragraphs, a handful of doctrinal concepts are introduced, followed by a discussion on how these concepts can be applied to network defense. The intent is to get out of the traditional network defender mindset and think about how military strategies can be leveraged to improve your chances of keeping your data safe from intruders.

Operations Security (OPSEC). There is a short Joint Pub devoted to operations security and it is well worth the read[11]. JP 3-13.3, Operations Security, describes the OPSEC process as "a systematic method used to identify, control, and protect critical information and subsequently analyze friendly actions associated with military operations."

OPSEC is about information. What information is available that an adversary can use against you and how can you limit the availability of that information?

You can consider this question from the perspective of an attacker as well as the perspective of a defender. From the perspective of an attacker, OPSEC can be thought to operate at three levels. Often attackers wish to prevent defenders from discovering an operation, so the first level regards protecting the fact that an operation is occurring. Even if defenders are aware of an operation, attackers may wish to prevent them from learning details of it, so the second level regards protecting information about the operation. Typically, Internet attackers also seek to avoid attribution. If defenders can attribute an attack, they can strike the attacker directly. So the third level has to do with protecting the true identity of the attacker. In some cases, attackers may wish to maintain OPSEC at one of these levels, but not at another. For example, the attacker may wish for the victim to know about an operation, or to know who was responsible, but not how the operation will be carried out.

To maintain OPSEC at the first level, each aspect of an attack should be planned so that defenders do not become aware of it, or if they discover some aspect of it, they misinterpret what they've found. An example might be the use of poorly crafted phishing scams that are broadly targeted against an organization in hopes that if they are detected, they might be dismissed as an insignificant attack, whereas a well crafted phishing email might be more carefully scrutinized by the network defenders if it is discovered.

At the second level, attackers may take steps to prevent defenders from understanding how an operation will unfold, so the defender cannot take steps to prevent it even if they are aware that it is happening. A perfect example of this is the use of Domain Name Generation Algorithms by

[10] The U.S. Official Department of the Army Publications and Forms Website is at http://armypubs.army.mil/doctrine/Active_FM.html.

[11] Department of Defense. *Joint Publicatin 3-13.3, Operations Security,* [Online]. 4 January 2012. Available: https://publicintelligence.net/jcs-opsec/. [Accessed April 2014].

botnet operators, which prevent defenders from knowing exactly where the botnet operator's command and control system will appear.

At the third level, a disciplined attacker considers how every aspect of what they are doing could generate bread crumbs that connect their operation with their true identity, or enable defenders to narrow down their identity. This could include the location from which systems are accessed, cross pollination of usernames, the time of day when operations take place, language settings on computers, the use of particular writing styles or frequent misspellings of words, etc.

From the perspective of a defender, OPSEC can present a significant challenge if your organization is large. There may be many open sources of information that an attacker could use against your organization. In particular, attackers may seek to understand your organizational structure so that they can perform effective spear phishing attacks. They may also seek to learn things about your organization's IT infrastructure and your approach to defending it.

Are executive travel plans posted? Is the corporate directory available externally? Is ALL paper trash shredded or burned? What do employees in your IT department say about their jobs on LinkedIn?

Controlling every piece of information that could potentially be valuable to an adversary is impossible to do within the culture of most civilian organizations. It's therefore important to focus your efforts of the pieces of information that present the greatest risk to your organization. With this in mind, consider the five-step OPSEC process:

1. *Identification of Critical Information.* That is, what are you trying to protect? Be sure to consider this from an offensive perspective! What is important to you isn't necessarily the same as what is important to an adversary.

2. *Analysis of Threats.* Try to be specific. Who might target your organization and why.

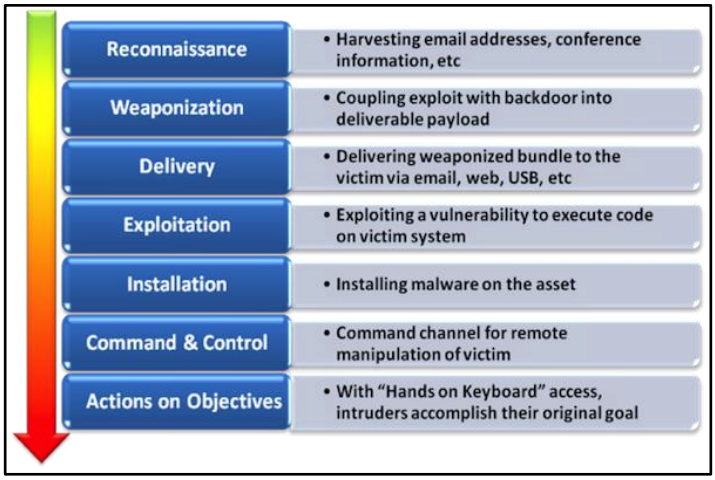
3. *Assessment of Vulnerabilities.* From an OPSEC perspective - where are you leaking critical information of value to an attacker? How valuable is that information?

4. *Assessment of Risk.* Risk = Threat X Vulnerability. There is a range of risks, some acceptable and some not. What risks are you not willing to accept? This leads to the last step.

5. *Application of Appropriate Operations Security Countermeasures.*

Kill Chain. The "kill chain" was described in the online Air Force Magazine in July of 2000[12] and later codified into U.S. Air Force targeting doctrine[13]. The USAF targeting process has six steps: Find, Fix, Track, Target, Engage, Assess (or F2T2EA), a chain of events that has become known within the Air Force as the kill chain. In 2010, a team of researchers at Lockheed Martin took the concept of the kill chain and applied to to the steps that an attacker takes to gain unauthorized access to a network[14]. The insight in this paper is that in order to be successful, an attacker must be successful at each step in the chain. If a defender can successfully prevent intrusion by causing the attacker to fail in one of these steps, thereby breaking the chain.

The kill chain concept has been widely influential in computer security because it uses military doctrine to provide defenders with a new way of thinking about the problem that they are trying to solve. Traditionally, attackers are thought to have an asymmetric advantage in computer security because defenders have to identify and remediate every vulnerability in their infrastructure whereas attackers only have to find one in order to be successful. The kill chain concept flips the asymmetry on it's head, providing a model in which the attacker must be successful at every stage but the defender need only succeed once. This way of thinking highlights the natural advantages that defenders have.

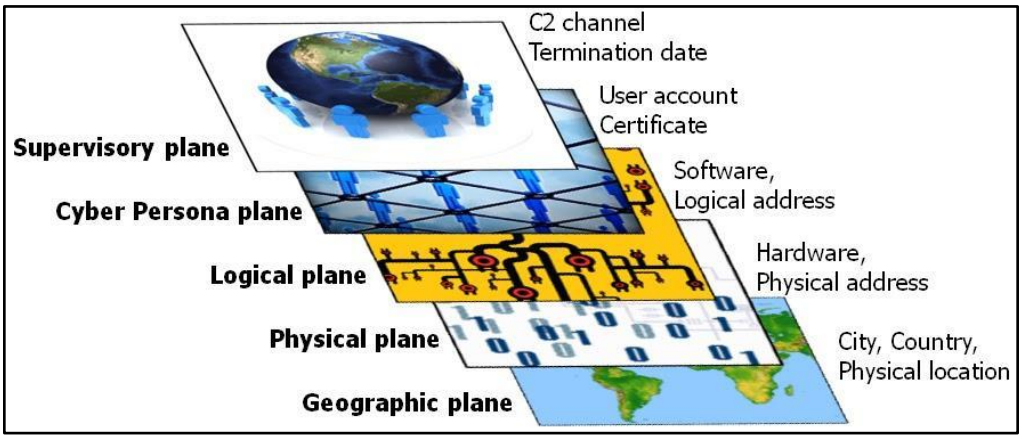


Cyber Kill Chain[15]

Cyber Terrain and the Cyberspace Planes. Cyberspace is thought of as an analog to real space, but one that exists within the environment of our computer networks. There are opportunities to draw parallels between how military doctrine applies to real space and how it

[12] John A. Tirpak. "Find, Fix, Track, Target, Engage, Assess", in *Air Force Magazine*, [Online]. 2 July 2000. Available: http://www.airforcemag.com/magazinearchive/pages/2000/july%202000/0700find.aspx. [Accessed March 2014].
[13] United States Air Force, *Air Force Doctrinal Document 3-60, Targeting (Change 1),* [Online]. 8 June 2006. Available: http://www.fas.org/irp/doddir/usaf/afdd3-60.pdf. [Accessed April 2014].
[14] Hutchins, et. al., Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains," in *6th Annual International Conference on Information Warfare and Security,* [Online]. March 2011. Available: http://www.lockheedmartin.com/. [Accessed April 2014].
[15] Ibid.

applies to cyberspace. In discussing operational concepts such as maneuver and fires in cyberspace, some fall into the trap of defining cyber terrain as the physical devices that make up computer and communications networks. Complicating matters is the fact that the DOD defines cyberspace[16], but does not define cyber terrain. In work published in the 2014 NATO Conference on Cyber Conflict (CyCon), the authors define cyber terrain as "the systems, devices, protocols, data, software, processes, cyber personas, and other networked entities that comprise, supervise, and control cyberspace"[17]. This definition reflects the Cyberspace Planes described in another CyCon paper[18] and depicted in the figure below.



Cyberspace planes[19].

Cyber Terrain Analysis using Cyberspace Planes[20]. Traditional military terrain analysis uses a process represented by the acronym OCOKA, which stands for Observation and Fields of Fire, Cover and Concealment, Obstacles (man-made and natural), Key Terrain, and Avenues of Approach. This terrain analysis process helps one think through the identification of key terrain on a battlefield and how to defend it. Hobbs applies the traditional OCOKA analysis to cyberspace[21] and we expand on his observations below.

1) Observation and Fields of Fire. *Observation* refers to the ability to see enemy forces from a particular vantage point; a *field of fire* combines this ability to observe with the ability to engage

[16] The DOD's Joint Publication 3-1 defines cyberspace as "A global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."
[17] D. Raymond, G. Conti, T. Cross, and M. Nowatkowski, "Cyber Key Terrain: Seeking the High Ground," in *6th International Conference on Cyber Conflict*, Tallinn, Estonia, June 2014.
[18] D. Raymond, G. Conti, R. Fanelli, and T. Cross, "A Framework for Control Measures to Limit Collateral Damage and Propagation of Malicious Software," in *5th International Conference on Cyber Conflict*, Tallinn, Estonia, June 2013.
[19] Ibid.
[20] This discussion of cyber terrain analysis using the cyberspace planes is reproduced and edited from Raymond, Conti, Cross, and Nowatkowski's 2014 CyCon paper on Cyber Key Terrain.
[21] D. Hobbs, "Application of OCOKA to Cyberterrain," White Wolf Security White Paper, Lancaster, PA, June 2007.

enemy targets within the maximum range of your weapon. The idea of observing cyber terrain, while different from physical terrain, is still meaningful. Much like physical terrain, observation is based on vantage point. Someone scanning a network from outside of a firewall will likely get an entirely different result than someone scanning the network from inside.

2) Cover and Concealment. In kinetic terms, *concealment* protects an individual from observation, while *cover* protects one from observation and enemy fire. *Camouflage* is sometimes used to enhance or provide concealment. In cyberspace, as in physical space, a third category exists in which a target can be seen but not engaged and is therefore out of range of an adversary's available weapons.

For the network defender, cover is often provided by firewalls that prevent traffic from reaching specific hosts while also protecting those systems from observation. An intrusion prevention system can be used to place hosts out of range of an attack by blocking malicious network traffic, but they do not provide concealment – the hosts behind an intrusion prevention system can still be observed by the attacker through authorized transactions.

3) Obstacles. In cyberspace, *obstacles* are those technologies or policies that limit freedom of movement within a network. These can include router-based access control lists, air gaps, firewalls, and other devices that are used to restrict the flow of network packets. In cyber terrain, the distinction between obstacles and cover is not always clean. A device installed to limit the enemy's freedom of movement can also provide cover for some network systems. Furthermore, by filtering malicious packets from traffic destined to a system visible on the network, cyberspace obstacles sometimes put target systems out of range of an attackers cyber weapons.

4) Key Terrain. Earlier we defined cyber terrain, here we define cyber *key terrain* as systems, devices, protocols, data, software, processes, cyber personas, or other network entities, the control of which offers a marked advantage to an attacker or defender.

5) Avenues of Approach. Avenues of approach in cyberspace are composed of the various paths that can be traversed to reach a target. The physical pathways that connect systems such as switches, routers, fiber, and Ethernet cable are often less relevant than the logical connections facilitated and limited by these devices since the devices traversed by Internet flows can change over time. An HTTP connection to a web server can be an avenue into a target network. Avenues of approach in cyber operations might also include multi-pronged attacks such as a phishing attack on an employee followed by a logical connection to resources left open by the phishing attack.

A consideration of cyber terrain analysis leads to two key insights. The first is that attackers are often operating with imperfect information about the environments they are targeting, and they have to discover how those environments are laid out through active reconnaissance. All of that reconnaissance involves interacting with computer systems and may be detected by a careful defender. Attackers are also forced to engage in a constant process of

reassessment of key terrain as they progress deeper into a network and develop a more complete picture of how it is constructed. At the outset, attackers may have a hard time understanding the true value of an asset that they discover through reconnaissance, or even whether or not that asset is real.

The second critical insight is that defenders create the environment that attackers are targeting. Terrain may not be what it appears to be. Key Cyber Terrain can be moved, and it can be reorganized in such a way that it ceases to be valuable. A defender could lure an attacker into targeting a piece of key terrain that seems to provide access to a valuable asset, and then change the nature of that terrain once it is compromised. This approach expends attacker resources and forces him or her to reveal capabilities and techniques.

Although honeypots have been a part of defensive approaches to protecting computer networks for a long time, traditional approaches to constructing them have not always kept up with modern attackers and their tactics, and most organizations are not using them as a central part of their operational approach to defending their networks. It is important to design honey pots that are truly attractive to the kinds of adversaries an organization is most concerned with. A good honeypot should appear to be a key piece of terrain in order to attract an attacker's attention.

Deception. Military deception (MILDEC) has myriad applications to the cyber domain. Codified in another short joint publication (19 pages), deception can be a great way to take advantage of your adversaries' initial lack of information about your network[22]. It can be valuable to separately consider moves that deny your adversary access to a piece of information which is true, and moves that deceive your attacker into believing something which is false.

Deception can be used by both attacker and defender. Attackers may wish to deny a defender access to key information (see the previous discussion of OPSEC). They may also wish to present false flags that distract the attacker, mislead them as to the true nature of an operation, or cause them to believe that they have successfully defended the organization and there is nothing more for them to do. Recent public reports have pointed to the use of distributed denial of service attacks on financial institutions as a false flag that distracts defenders away from financially motivated compromises occurring at the same time.

Defenders can use honeynets to draw intruders away from their true network resources and trick them into revealing their presence (see the previous discussion on Terrain). These false resources need not just be systems and services on the network. They could also include phoney database records, files, or other data which wouldn't normally be accessed or used, and they could include phoney employees or user accounts that are sitting ducks for spear phishing attacks. Defenders can also use proxies or network address translation (NAT) to deny their adversary knowledge of their internal network structure, and they can use hidden file systems to prevent intruders from discovering key data.

[22] Department of Defense. *Joint Publication 3-13.4, Military Deception,* [Online]. 26 January 2012. Available: https://publicintelligence.net/jcs-mildec/. [Accessed June 2014].

Consideration of deception and counter-deception, and operationalization of those concepts, could have a significant impact on successful computer network defense. It is often written that the weakest link in computer network defense is the human. In fact, the weakest link in computer network offense may also be the human. What are you doing in your approach to defending your network to exploit the human who is trying to attack you?

Intelligence.

The military's intelligence cycle has be refined over millennia and is currently codified in Joint Doctrine's "2"-series manuals. There is a cottage industry of computer security products and companies that use the term "threat intelligence" in their marketing without understanding or applying the whole process. They might analyze suspicious network traffic or reverse engineer malicious software to produce a list of "evil" IP addresses, domain names, and malware signatures and call this "threat intelligence". Collecting data, however, is only one step in the larger process and a disciplined approach will make better use of scarce resources and will lead to more effective network defense. In practice, intelligence is a thorough analysis and understanding of the threat's capabilities, strategy, and tactics and how they can be used on the cyber terrain comprising your operational environment.

The intelligence process consists of six steps:

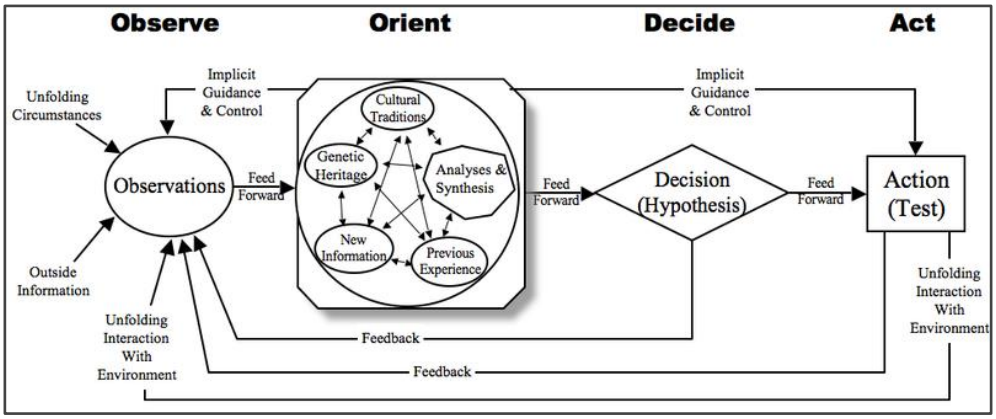
1. Planning and direction. Data is collected for a specific purpose, for example, to identify which avenue of approach an adversary will use. It is usually not necessary to observe the entire battlefield to determine this. Focused collection on a few key areas can answer this question while conserving significant resources that can then be devoted to answering other, similar questions.
2. Collection. This is the process of gathering specific information from a potentially wide array of sources. Step one focuses this effort.
3. Analysis and production. Data from various sources must be analyzed and correlated to turn it into useful information. This is often more important than the collection.
4. Dissemination and integration. Once collected, the intelligence must be disseminated to those that can use it and integrated into the overall operation.
5. Evaluation and feedback. Perhaps the most important step in the process is to evaluate the extent to which planning, collection, analysis, and dissemination increased the success of the overall operation. If significant investment in intelligence collection is providing only mediocre security improvements, it is time to relook your approach.

Tactics, Techniques, and Procedures (TTP). The term TTP is used to refer broadly to actions that one might take in a particular problem domain. It is an umbrella term that captures formal doctrinal standards (procedures) as well as non-prescriptive ways to perform a mission (techniques). There is a whole series of Army Tactics, Techniques, and Procedures (ATTP) manuals covering topics ranging from combined arms in urban terrain to air assault operations

to civilian casualty mitigation[23]. You might also hear the term 'enemy TTPs', referring to the vast collection of tools and techniques your adversary might use against you.

COL John Boyd's OODA Loop. Boyd's previously-mentioned OODA loop (Observe, Orient, Detect, Act) was developed in the context of aerial combat when Boyd was commanding U.S. Air Force units during the Korean War. Boyd was convinced that improved reaction times would give his pilots an advantage. Time required to 'observe' is generally fixed, but Boyd felt that the other components of the cycle could be improved through training. For example, by reducing the number of response choices for a particular stimulus, response times could be improved significantly. Boyd later expanded the model and applied it in broader terms to military strategy[24].

Some misinterpret Boyd's OODA loop and use it to advocate quick decision-making, even in the face of inadequate assumptions and incomplete information, tacking on the tired axiom, "perfect is the enemy of good enough." This misses Boyd's point. His intent was to find ways to improve the speed at which *good* decisions are made and *appropriate* actions are taken through exhaustive training, detailed analysis of the operational environment, and a thorough understanding of potential adversary actions and reactions. It is not designed to be a shortcut, but a guide to the importance of situational understanding and well-designed, exhaustively rehearsed battle drills.



Boyd's OODA Loop[25]

A key insight to draw from the OODA loop is that in a dogfight, every time you change the orientation of your airplane, you change the basic facts that your adversary is contending with. If you can observe your adversary and take action faster than he can, you can disrupt his ability to

[23] Army TTP manuals are available on the Army Publishing Directorate website at http://armypubs.army.mil/doctrine/ATTP_1.html.

[24] Boyd's used aerial combat to explain his OODA loop, but he intended for it to used in a much broader context. A collection of his work can be found in the John Boyd Compendium, http://dnipogo.org/john-r-boyd/, provided by the Project on Government Oversight.

[25] OODA loop image from http://crossvale.com/blog/boiling-ocean-analysis-paralysis-and-ooda-loop.

contend with the situation by changing the factors that he is contending with more rapidly than he can keep up.

The OODA loop comes into play in the process of real time network attack and defense involving sophisticated, adaptive adversaries.[26] How quickly can either party observe the cyberspace environment and with what resolution? How quickly can either party make changes to their orientation within the environment in response to stimuli? As a simple example, if you perform a vulnerability scan once a month and it takes you three months to patch any vulnerabilities that you find, chances are your attacker can find and take advantage of vulnerabilities much faster than that.

As a defender, a key to succeeding is to develop a faster tempo than your attacker. You've got to be able to make high resolution, near real time observations of your environment, and you've got to be able to act quickly based on those observations without compromising accuracy.

Consider this in the context of some of the other recommendations that have been made in this paper. If, as a defender, you identify an attack because of a honeypot - a phoney system that you placed in the environment that looks like a piece of key terrain and that your attacker was foolish enough to try to access - you've got to ask yourself what to do next. You now have an edge on your attacker - his OPSEC has failed, you know that he is present, and he may not yet realize that you are aware of him. However, if you take immediate action to block him, he may come back into your network through a means that you cannot observe.

There is a great deal of value in gaining as complete a picture of the attacker as you can, but that may require allowing the attacker to continue to operate within your network while you collect observations. You have to make a cost-benefit decision regarding how long to allow the attack to continue. There is a constant risk that the attacker may do damage or access a key piece of data that you are trying to defend. If you are able to spin your OODA loop faster than your attacker, that means you can observe his actions and react to them faster than he can make them. If you are in that position, you can confidently observe his actions without fear that the situation will get out of control. However, if your adversary can pivot more rapidly than you can keep up, then the risk of allowing the attack to continue is greater.

How many organizations today view incident response as a real time function in which efficiency - shortening mean time to know - is not just a matter of controlling costs, but a matter of effectiveness against adversaries? This is the sort of operational footing that may be needed to defend organizations against sophisticated, targeted attacks that can bypass perimeter defenses and adapt to the organization's attempts to respond.

[26] This discussion of the OODA Loop in Cyber Security is heavily influenced by: Keanini, T.K. *The OODA Loop: A Holistic Approach to Cyber Security,* [Online]. 27 March 2014. Available: https://www.youtube.com/watch?v=RBv82THpBVA. [Accessed May 2014].

Targeting. Targeting is the process of selecting and prioritizing targets and matching them against the appropriate response to them[27]. A "target" is an entity or object considered for possible engagement or action. The action can be kinetic (bombs and bullets) or non-kinetic (leaflets and press releases). Targeting is very closely tied to the concept of Effects Based Operations (EBO), which recognizes that the purpose of a military operation is to achieve a desired strategic, operational, or tactical effect, such as preventing an enemy attack, but does not always require destruction of the enemy force. For example, destroying a key bridge on the eve of a tactical engagement may prevent ground forces from reaching the battlefield, or a cyber attack against an air defense artillery fire control system may allow friendly air assets to attack unencumbered into enemy territory.

The Army's targeting methodology follows a Decide, Detect, Deliver, and Assess, or D3A, cycle.

- Decide - Determine what effect is desired and what 'targets' might be influenced, either kinetically or non-kinetically, to achieve that effect.
- Detect - Execute an intelligence collection plan to help decide which asset to use against selected targets.
- Deliver - Execute the chosen course of action.
- Assess - Determine whether your delivery was successful or not using battle-damage assessment or some other appropriate tool; if necessary, go back to step 1, Decide.

In U.S. doctrine, cyber effects are among those that commanders can use to influence an adversary. Cyber attack might be used instead of kinetic attack or it might be used along with with kinetic operations. One oft-cited example is Russia's invasion of Georgia in 2008[28].

Adversaries' Approaches to Cyber Warfare.

If you think your network is not being targeted, you are probably wrong. The term "advanced persistent threat" refers to nation-state actors that have the capability and motivation to gain unauthorized access to just about any network. Reasons for gaining access are myriad, from gathering military secrets to scooping up intellectual property. One of the best unclassified analysis of these activities was published by Mandiant in 2013[29].

China. In 1999, two senior Colonels in the Chinese Air Force published a book whose title is translated to "Unrestricted Warfare" that analyzes how technological advances will change the nature of warfare[30]. This work goes beyond military technology and explores new types of warfare, including hacking attacks, trade wars, and finance wars. The book examines

---

[27] Department of Defense. *Joint Publication 3-60 Joint Targeting,* [Online]. 13 April 2007. Available: http://www.dtic.mil/doctrine/new_pubs/jointpub_operations.htm. [Accessed June 2014].
[28] Markoff, John. "Before the Gunfire, Cyberattacks", in The New York Times, [Online]. 12 August 2008. Available: http://www.nytimes.com. [Accessed May 2014].
[29] Mandiant, Inc. "APT1: Exposing one of China's Cyber Espionage Units", [Online]. 2013. Available: http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf. [Accessed June 2014].
[30] Liang, Qiao and Xiangsui, Wang. *Unrestricted Warfare*, [Online]. Available: http://www.fas.org/nuke/guide/china/doctrine/. [Accessed April 2014].

differences in Chinese and American strategic thinking and describes how the Chinese might capitalize on American weaknesses.

Timothy Thomas of the Army's Foreign Military Studies Office at Fort Leavenworth, has extensively studied Chinese Information Warfare doctrine and his trilogy is an excellent source of information[31]. All three works were published by FMSO and are available from Amazon and other booksellers.

Russia. In 2000, Russia published their "Doctrine of Information Security of the Russian Federation"[32] and in 2011, the Russian Military produced "Conceptual Views on the Activity of the Russian Federation Armed Forces in Information Space"[33]. These documents are defensive in nature and describes not only the need to defend military command and control and other information systems against attack, but also "vigorously counteracting the information-and-propaganda and psychological operations of a potential enemy." Perhaps a more realistic view of Russia's cyber doctrine is an analysis provided in the American Foreign Policy Council's Defense Dossier, entitled "How Russia Harnesses Cyberwarfare,"[34] by David J. Smith. This document describes Russia's cyber policy in the context of cyber attacks against Estonia and Georgia in 2007 and 2008. It also discusses Russia's suspected use of organized crime and hacker groups to limit adversaries' ability to attribute cyber incidents to the Russian government.

V. The Future

One excellent source of emerging thought in cyber operations is the Conference on Cyber Conflict (CyCon), hosted annually by the NATO Cooperative Cyber Defence Center of Excellence and now in its Sixth year[35]. Research presented in recent CyCon events include papers on cyber maneuver, cyberspace deterrence, avoiding collateral damage with cyber weapons, cyber key terrain, military deception in cyber operations, and efforts to build a cyber common operational picture, to name just a few. Links to electronic copies of all CyCon proceedings are available on the CCDCOE website at http://www.ccdcoe.org/228.html.

Military operational research that often forms the basis of future doctrine is openly discussed in professional forums such as Military Review (http://usacac.army.mil/CAC2/MilitaryReview/),

---

[31] Thomas, Timothy. *Dragon Bytes* (2003), *Decoding the Virtual Dragon* (2007), *The Dragon's Quantum Leap* (2009). Foreign Military Studies Office, Fort Leavenworth, KS. All books are available at Amazon and other commercial booksellers. US military can get copies free at the FMSO office in Fort Leavenworth.

[32] A translation and analysis of Russia's "Doctrine of Information Security of the Russian Federation" can be found at https://digital.law.washington.edu/dspace-law/handle/1773.1/757.

[33] An unofficial translation of Russia's "Conceptual Views on the Activity of the Russian Federation Armed Forces in Information Space," translated by the NATO Cooperative Cyber Defense Center of Excellence can be found at http://www.ccdcoe.org/strategies/Russian_Federation_unofficial_translation.pdf.

[34] Smith, David J. "How Russia Harnesses Cyberwarfare", in *Defense Dossier,* [Online]. August 2012. Available: http://www.afpc.org/files/august2012.pdf. [Accessed March 2014].

[35] The NATO Cooperative Cyber Defense Center of Excellence (CCDCOE) website is here: https://www.ccdcoe.org/. The CyCon web site is at http://ccdcoe.org/cycon/home.html.

which is published by the U.S. Army's Combined Arms Center at Fort Leavenworth, the online Small Wars Journal (http://smallwarsjournal.com/), and the Center for Army Lessons Learned (http://usacac.army.mil/CAC2/call/). A quick search on the Internet would likely turn up other such doctrinal forums.

VI. Where To Go for More

Unclassified DoD and Military Branch doctrine:

- Intelligence and Security Doctrine (including DoD and all military branches) Federation of American Scientists' Intelligence Resource Program http://www.fas.org/irp/doddir
- DOD Dictionary. http://www.dtic.mil/doctrine/dod_dictionary/
- Joint Doctrine. http://www.dtic.mil/doctrine/doctrine/
- Army Doctrine. http://armypubs.army.mil/doctrine/Active_FM.html
- Air Force Doctrine. http://www.fas.org/man/doctrine.htm#usaf

Periodicals:

- Small Wars Journal: http://smallwarsjournal.com (all online content)
- Military review: http://militaryreview.army.mil (online and print)
- Parameters: http://strategicstudiesinstitute.army.mil/pubs/parameters (online and print). US Army War College quarterly journal.
- Army Branch Magazines (Armor magazine, Infantry magazine, Artillery magazine, ArmyAviation magazine, etc.)
- Combined Arms Research Digital Library: http://cgsc.contentdm.oclc.org
- Military Times: http://www.militarytimes.com

Military Theorists:

- Clausewitz, Carl von. *On War*, [available at www.clausewitz.com], 1832
- Jomini, Antoine Henri. *The Art of War*, [available at www.gutenberg.org], 1862
- Mitchell, William. *Winged Defense: The Development and Possibilities of Modern Air Power--Economic and Military*. The University of Alabama Press, Tuscaloosa, AL. 1925
- Coram, Robert. *Boyd: The Fighter Pilot Who Changed the Art of War*. Little, Brown and Company, 2002
- Mao Zedong. *On Guerilla Warfare*, [Online]. Available at http://www.marxists.org/, 1937
- Mahan, Alfred Thayer. *The Influence of Sea Power Upon History: 1660 - 1783*, Little, Brown and Co. 1890

Conferences:

- NATO Conference on Cyber Conflict (CyCon): http://ccdcoe.org/cycon/home.html
- IEEE/AFCEA Annual Military Communications Conference (MILCON): http://www.milcom.org/

Other:

- Center for Army Lessons Learned: http://usacac.army.mil/CAC2/call/

- School for Advanced Military Studies: http://usacac.army.mil/cac2/cgsc/sams/
- U.S. Army War College: http://www.carlisle.army.mil/

VII. Conclusions

This work only scratches the surface of the vast library of intellectual thought underpinning current military doctrine and tactics. It is intended to provide examples of ways in which elements of this library have been applied to defending networks, and to point readers to where they can do more research. As in warfare, there are few easy answers. New network attack tools make old defensive mechanisms obsolete just like gunpowder led to the demise of the iron-clad knight on horseback. There are many lessons that can be carried over from military doctrine, if one knows where to look.

Authors:

David Raymond is an Associate Professor at West Point where he teaches courses in computer networking and cybersecurity and coaches the West Point CTF Team. He is an Army officer of 25 years with a unique mix of experience in armored maneuver warfare and Army systems automation. He has published over 20 papers and articles on topics including computer architecture, wireless security, online privacy, and cyber warfare and has spoken at several academic and industry conferences.

Greg Conti is an Associate Professor and Director of West Point's Cyber Research Center. He is the author of "Security Data Visualization" (No Starch Press) and "Googling Security" (Addison-Wesley) as well as over 60 articles and papers covering cyber warfare, online privacy, usable security, and security data visualization. He has spoken at numerous security conferences, including Black Hat, DEF CON, CyCon, HOPE, Interz0ne, ShmooCon, and RSA. His work can be found at www.gregconti.com.

Tom Cross is Director of Security Research at Lancope, where he works on advancing the state-of-the-art in network behavioral anomaly detection with netflow. He has over a decade of experience as a computer security researcher and thought leader. He is credited with discovering a number of critical security vulnerabilities in enterprise-class software and has published papers on collateral damage in cyber conflict, vulnerability disclosure ethics, security issues in internet routers, encrypting open wireless networks, and protecting Wikipedia from vandalism. He was previously manager of X-Force Research at IBM Internet Security Systems. He has spoken at numerous security conferences, including Black Hat, DEF CON, CyCon, HOPE, Source Boston, FIRST, and Security B-Sides.