SMALL WARS JOURNAL

WHY YOUR INTUITION ABOUT CYBER WARFARE IS PROBABLY WRONG

Articles

Thu, 11/29/2012 - 9:29pm

Since the dawn of time, when one caveman first struck another, humans have relied on a natural understanding of their physical environment to conduct warfare. We have an inborn ability to understand the laws of the physical world. In order to shoot an artillery round farther, just add more powder; to provide cover for protection against bullets, hide behind a rock. A private might accidentally shoot the wrong target, but the potential damage is limited by the maximum range of his or her rifle. The laws of physics, however, are counterintuitive in cyberspace. In cyberspace, our understanding of the "laws of physics" is turned on its head. Weapons can be reproduced instantly, "bullets" travel at near the speed of light, destroyed targets can be brought back from the dead, and a seventeen year old can command an army. As human beings we are at a distinct disadvantage when thinking intuitively about cyber warfare. In this article we study where our intuition fails us in cyber warfare and suggest alternate ways to think about the conduct of cyber war that account for the vast differences between the kinetic and the non-kinetic fight. A correct understanding and appreciation of these differences and common misconceptions is absolutely necessary to conduct cyber warfare and to integrate cyber effects into the kinetic battlefield. To ground this work we need to define the term "cyber." There is significant and evolving debate regarding the precise definition of cyber. For purposes of this article we define cyber as a spectrum of cyberspace operations including Computer Network Attack (CNA), Computer Network Exploitation (CNE), and Computer Network Defense (CND).

The Attacker has the Advantage over the Defender

In classic military doctrine, the defender has a distinct advantage (http://www.globalsecurity.org/military/library/policy/army/fm/3-90-2/chap12.htm#12-17) over the attacker. In today's model of cyber security, defenders build layers of defenses to protect the confidentiality, integrity, and availability of critical assets. Security professionals pour millions of dollars into such defenses, but with only limited success. A Maginot Line (http://en.wikipedia.org/wiki/Maginot_Line) strategy rarely works in cyberspace because attackers need only find a single flaw to launch a successful attack. Perfect defense is impossible; the astronomic complexity of the software and hardware woven into our information systems and networks is beyond human comprehension. As an example, the Windows XP operating system alone has more than 45 million lines (http://www.facebook.com/windows/posts/155741344475532) of computer code, creating an immense attack surface (http://en.wikipedia.org/wiki/Attack_surface). Many aspects of computer security cannot be solved (http://en.wikipedia.org/wiki/Undecidable_problem) by computers, such as determining the exact operation of a piece of untrusted software. Attackers however, can probe (http://en.wikipedia.org/wiki/Fuzz_testing) these complex systems to find a flaw and are frequently successful (http://www.securityfocus.com/archive/1). Hardware and software monocultures (http://en.wikipedia.org/wiki/Monoculture_%28computer_science%29), such as widespread use of a single operating system or web browser, amplify the impact of these discoveries by facilitating widespread compromise. Against a determined adversary, many security experts believe we cannot keep our computers secure, compromise is simply a function of time and dedicated resources. Common defenses, such as antivirus systems are reaching the end of their usefulness (http://www.pcworld.com/businesscenter/article/145148/security_vendors_slam_defcon_virus_contest.html) and cannot be relied upon (http://www.wired.com/threatlevel/2012/06/internet-security-fail/) for effective defense. Even air-gapped networks (http://en.wikipedia.org/wiki/Air_gap_%28networking%29), not directly connected to the Internet, have proven vulnerable to mobile malicious code (http://smallwarsjournal.com/jrnl/art/stuxnet-cyberwar-revolution-in-military-affairs). Recent research indicates that defenders must field 1,000 times the resources (http://www.youtube.com/watch?v=IWGjWYIToFU) (money, people, time, compute power, etc.) to reach parity with attackers in cyberspace; this is not a winning proposition for the defender.

Figure 1: In cyber warfare, adversary tactics evolve on a daily basis, unlike the notional Krasnovian Army formerly used in training exercises. (Image Source: Krasnovia.com (http://www.krasnovia.com/krasnovia.jpg))

We aren't Fighting the Krasnovian Army (http://www.globalsecurity.org/military/ops/ctc-ntc-scenario.htm)

During the Cold War, military planners could rely upon relatively fixed threat doctrine, see Figure 1. We knew the capabilities of threat units and could plan accordingly. In the cyber domain, threat Tactics, Techniques and Procedures (TTPs) are constantly changing. One day we may have a distributed denial of service attack (http://searchsecurity.techtarget.com/definition/distributed-denial-of-service-attack), the next day a phishing (http://www.microsoft.com/security/online-privacy/phishing-symptoms.aspx) attempt. We could also have a drive-by download (http://www.cio.com/article/699970/6_Ways_to_Defend_Against_Drive_by_Downloads), a USB stick dropped in a parking lot (http://www.schneier.com/blog/archives/2012/07/dropped_usb_sti.html) or something else entirely new. The list goes on and on because new capabilities and TTPs are developed on a daily basis. Adversaries include well-resourced nation states and large online criminal organizations; however, even small groups and individuals can join the fray (http://www.sans.org/reading_room/whitepapers/attacking/jester-dynamic-lesson-asymmetric-unmanaged-cyber-warfare_33889) and have a tremendous (http://en.wikipedia.org/wiki/Operation_Payback) impact (http://arstechnica.com/tech-policy/2011/02/anonymous-speaks-the-inside-story-of-the-hbgary-hack/). In some ways we are already at war. We have much to learn by studying insurgency (http://www.amazon.com/Learning-Eat-Soup-Knife-Counterinsurgency/dp/0226567702) and applying those lessons in cyberspace.

Reserve Forces may be more Capable than Active Duty Troops

In kinetic operations, reserve forces have always been at a distinct disadvantage, often equipped with older equipment and less frequent training opportunities. However, reserve personnel are at their best when their civilian careers match their military roles. Truck drivers are a textbook example. Great opportunity lies for the military to recruit Reserve and National Guard personnel who are experts in cyber security; and we need to. The high churn of active duty forces between assignments inside and outside cyber continually degrade their skills. Embracing the value of reserve cyber experts, and civilian cyber experts, bears great promise for the future cyber workforce.

A Computer Can Be Turned into a Brick

Cyber Attacks can have devastating real world effects. We tend to think in terms of lost or corrupted data as a result of an attack, however computer hardware can be destroyed, or "bricked (http://en.wikipedia.org/wiki/Brick_%28electronics%29)," by corrupting its internal firmware (http://en.wikipedia.org/wiki/Firmware) and other means. This happens fairly rarely today because many malicious applications are tied to online crime and avoid harming their host. However, we should assume that our adversaries in a time of war will not be reluctant to destroy our information systems, weapon systems, and our Nation's critical infrastructure, including financial systems. Beyond just disabling or destroying computer hardware, software, and data, malicious software can also cause significant physical damage. Experts have warned of vulnerabilities in the SCADA systems which control water, power, communication, transport, and manufacturing systems. Stuxnet provided a very clear example of such capabilities by reportedly destroying centrifuges used to enrich uranium. We shouldn't forget that our weapon systems are heavily reliant on computer technology and may be vulnerable. The recent virus found in a military drone command center (http://www.wired.com/dangerroom/2011/10/virus-

hits-drone-fleet/) may be a warning of things to come. Our military depends on its technical advantage. If we lose our communication and information processing systems we will be severely degraded as a military and possibly rendered combat ineffective.

Cyber Terrain is more like a Parallel Dimension than Physical Space

We have been navigating physical terrain since birth, but networks aren't physical space. Cyberspace crosscuts the physical domains of air, land, sea, and space, and touches at myriad points. Networks aren't physical battlefields. Attacks can transit the globe at near the speed of light. Battles can be won or lost in milliseconds. In this virtual world, distance approaches zero. Enemies can teleport, appearing from numerous locations around the globe in the blink of an eye. Cyberspace is a man-made domain, it is constantly shifting as new nodes are added and others disappear. Grid squares (http://en.wikipedia.org/wiki/Military_grid_reference_system) can move (by changing a network address) or lie (spoofing a network address). Laws and military doctrine were written with physical boundaries in mind, but national borders in cyberspace are intertwined in complex ways unanticipated by the law. Unit boundaries, measured in kilometers of dirt are frequently meaningless. A cyberspace attacker may instantly appear in a brigade operations center in Afghanistan or a game console in New Jersey.

Adversaries Can Easily Camouflage, Deceive or Disappear

Deception is easy on the Internet. Identities can be spoofed (http://www.darkreading.com/security/news/225702468/robin-sage-profile-duped-military-intelligence-it-security-pros.html) or stolen (http://www.wired.com/gadgetlab/2012/08/apple-amazon-mat-honan-hacking/all/). Age, date of birth, gender, appearance, and marital status are all malleable. Adversaries can operate invisibly or leave little trace behind by cleaning logs. Attackers may disappear and reappear instantly on the other side of the world, by simply changing network connections or paths.. History itself may even be rewritten by altering system log files or other data. The nature of the Internet allows many people to share the same identity (by sharing the same authentication credentials) and one person to appear as many (by creating numerous user accounts). Trust is often misplaced. The end result is that is that things aren't necessarily what they might appear to be in cyberspace.

The Law of War and Cyber Policy Cannot Keep up with Technology

The law of war is well understood around the world and briefed to every service member. The law of *cyber* war is unsettled. Most legal professionals and judges have limited understanding of technology. One leading cyber warfare legal expert describes the situation in stark terms – explain technology to lawyers at the third grade level (http://www.blackhat.com/presentations/bh-usa-07/Clark/Presentation/bh-usa-07-clark.pdf) and to judges and juries at a first grade level (http://video.google.com/videoplay?docid=-7193032412048967982) (Clark's Law). Of course, technically savvy legal experts and policy makers exist, but the rapid advance of technology guarantees law and policy will lag years, if not decades, behind what is technically feasible today. For the foreseeable future, military leaders will be constantly challenged with navigating this legal and policy morass and petitioning policy makers (http://www.usnews.com/news/blogs/dotmil/2012/07/09/nsa-general-on-cyberattacks-probability-for-a-crisis-is-mounting) for updated laws.

Your Weapon Systems May Work Once, Twice, or Not at All

If you've seen Star Trek, you are probably familiar with the Borg (http://www.youtube.com/watch?v=Ybw2AkJ7kYc). In numerous episodes the Enterprise crew attempts to defeat borg drones by calibrating their phasers. However, the Borg quickly adapt and the phasers are no longer effective. The same holds true for cyber weaponry.

We see this cycle repeated on a daily basis. New vulnerabilities and exploits (http://en.wikipedia.org/wiki/0day) are discovered and weaponized (http://www.metasploit.com/), but once used or disclosed vendors will patch systems, antivirus companies will issue new signatures, and security professionals will develop countermeasures (http://en.wikipedia.org/wiki/Low_Orbit_Ion_Cannon). Unlike our M16's, we cannot be assured that cyber capabilities will work after first use, if at all. The result is an ongoing cyber arms race (http://www.businessweek.com/magazine/cyber-weapons-the-new-arms-race-07212011.html) and a burgeoning malware economy (http://www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits/) to acquire newer and better techniques.

Any Sufficiently Advanced Technology is Indistinguishable from Magic (http://en.wikipedia.org/wiki/Clarke%27s_three_laws)

Without an understanding of technology and networks, computers are just magic black boxes that sit on our desks. In the kinetic realm, warfighting leaders are developed over decades of developmental assignments, operational experiences, and training programs that are among the best in the world. While work is ongoing to develop cyber career paths, we are in the early stages. At the same time, there is a common misconception that "leaders are leaders" and that anyone can effectively lead cyber warfare units. Cyberspace is a new operational domain, and as we have tried to illustrate in this article, many of our instincts are wrong. The generalist leader model, where everyone is replaceable, may work *within* an operational domain (Air, Land, Sea, Space, Cyberspace), but leaders forced into other domains are at a distinct disadvantage, at best. There is a reason why we don't place Army officers in charge of aircraft carriers. That being said you go to war with the Army you have, not the Army you wish you had (http://www.washingtonpost.com/wp-dyn/articles/A132-2004Dec14.html). We need to fight to understand the domain (http://smallwarsjournal.com/jrnl/art/self-development-for-cyber-warriors) of cyberspace and learn to effectively lead (http://smallwarsjournal.com/jrnl/art/leadership-of-cyber-warriors-enduring-principles-and-new-directions) cyber warriors.

A Seventeen Year Old can Command an Army

Adversary leaders in cyberspace need not be seasoned fifty year old General Officers, and unless they are part of a traditional nation-state military organization, they almost certainly will not. Adversary leaders will likely emerge based on merit and possess significant experience online. Some will possess traditional schooling, but others will be self-taught and may have tapped the exceptional free resources available online from organizations including Wikipedia (http://en.wikipedia.org/wiki/Main_Page) and Khan Academy (http://www.khanacademy.org/), even MIT (http://ocw.mit.edu/index.htm) or Stanford (http://news.stanford.edu/news/2012/march/online-courses-mitchell-030612.html). Some will have experience in leading distributed teams, possibly Clan Armies (http://runescapeclans.wikia.com/wiki/List_of_Clans) in online games and virtual worlds. Their weapon systems can be actively controlled (http://www.eecs.umich.edu/fjgroup/botnets/) or passively controlled via pre-programmed logic. Lawyers won't be involved (a major agility advantage), and organizational structures will be more like a fluid New Model Army (http://www.amazon.com/New-Model-Army-Adam-

Roberts/dp/0575083611) than a rigid hierarchical organization. As a result, adversaries will be very agile. The command post, where a commander monitors maps and receives briefings from their staff to make decisions often has little utility when fighting in the cyber domain. The speed of decision making required is beyond human capacity. In an era where a network packet can travel around the globe in milliseconds carrying an attack payload (http://www.aspeninstitute.org/about/blog/general-keith-alexander-protecting-homeland-cyber-attacks), by necessity, algorithms will increasingly do much of the fighting. Future cyber warfare will be far more like high-speed trading on Wall Street than briefing the commander on potential courses of action.

You Can't Fire Cannons at the Internet (http://news.bbc.co.uk/2/hi/4897786.stm)

The infrastructure of the Internet is remarkably resilient. The ability to route around physical destruction is built into the Internet's design. There is no Internet kill switch, but there are certainly weaknesses (http://www.computerworld.com/s/article/75454/Net_s_Vulnerability_Exposed) that could be exploited by a determined adversary to disrupt its proper function. When we move above the physical and logical infrastructure planes which comprise the Internet, we should think in terms of specific end users and computing systems. Spear phishing (http://en.wikipedia.org/wiki/Phishing) via email accounts has long proven to provide precise means of targeting end users. Drive by downloads (http://en.wikipedia.org/wiki/Drive-by_download) of malicious software hosted on compromised websites is another well known way to target users. Social networking sites are yet another means of spreading malicious software (http://blogs.wsj.com/digits/2011/03/29/app-watch-the-deadly-sins-of-facebook-malware/) and targeting users. Attackers can destroy companies (http://servicesangle.com/blog/2012/05/14/online-threat-growing-rapidly-can-destroy-companies-says-fbi-cyber-security-head/) overnight by humiliating leaders or stealing intellectual property. However, as we've discussed elsewhere in this article, false identities can be easily created, complicating targeting. Attacks also bring the real possibility of collateral damage and limited effectiveness. For example, data can be replicated on multiple servers in various locations around the world, so even a successful attack may be quickly negated as a mirror (http://en.wikipedia.org/wiki/Mirror_%28computing%29)-image of the server is brought online.

Figure 2: Any networked device, including consumer electronics such as the digital picture frame, is a potential enemy combatant. (photo source: Wikimedia Commons (http://upload.wikimedia.org/wikipedia/commons/thumb/9/9c/Digital_photo_frame_with_picture.jpg/640px-Digital_photo_frame_with_picture.jpg))

An Enemy Combatant can be the Digital Picture Frame (http://www.securityfocus.com/news/11499) at Grandma's House

In cyberspace virtually any computing device is a potential threat or ally. The rise of the Internet of Things (http://en.wikipedia.org/wiki/Internet_of_Things), where many physical items will include computer processors and network connectivity, means we will face many potential combatants in cyberspace, see Figure 2. These devices may be compromised during design, manufacture, or anytime thereafter. Imagine if attackers discovered a flaw that allowed successful compromise of a common gaming console. We could be fighting an Army of tens of millions of PlayStations. This scenario isn't out of the realm of the possibility (http://www.pcworld.com/article/226128/sony_makes_it_official_playstation_network_hacked.html); botnets (http://en.wikipedia.org/wiki/Botnet) of more than one million hosts exist today (http://www.networkworld.com/news/2009/072209-botnets.html). Research indicates that bot armies can be rented for as little as nine dollars an hour (http://www.zdnet.com/blog/security/study-finds-the-average-price-for-renting-a-botnet/6528). Your next combat kill may be a robot or a refrigerator (http://en.wikipedia.org/wiki/Internet_refrigerator).

You Probably Won't Know Who is Shooting at You

In Internet combat you likely won't know who is shooting at you. Anonymity was built into the design of the Internet. Network traffic is comprised of packets that need only a source address and a destination address. Theoretically, the source address would be that of the attacker and the destination address would be the target. In reality, the source address can be easily spoofed and set to *any* network device anywhere in the world. To blindly return fire, you could, and most likely will, hit an innocent. Even if the source address is accurate, the attacker could have routed the attack through numerous intermediary nodes, some of which are in the United States, in allied countries, or in countries with no desire to help the US military. In most cases, attribution requires tedious step-by-step analysis—walking back node-by-node to the attacker—and patience to cope with legal and bureaucratic barriers at every turn. There are even anonymity networks that are designed to protect against such attribution attempts that are remarkably resistant to analysis. Note that these anonymity networks (https://www.torproject.org/), and the design of the larger Internet, were designed to allow open sharing of information, not to facilitate cyber warfare attribution. As a result, accurately identifying aggressors may take weeks, months, or even prove impossible (http://en.wikipedia.org/wiki/2007_cyberattacks_on_Estonia).

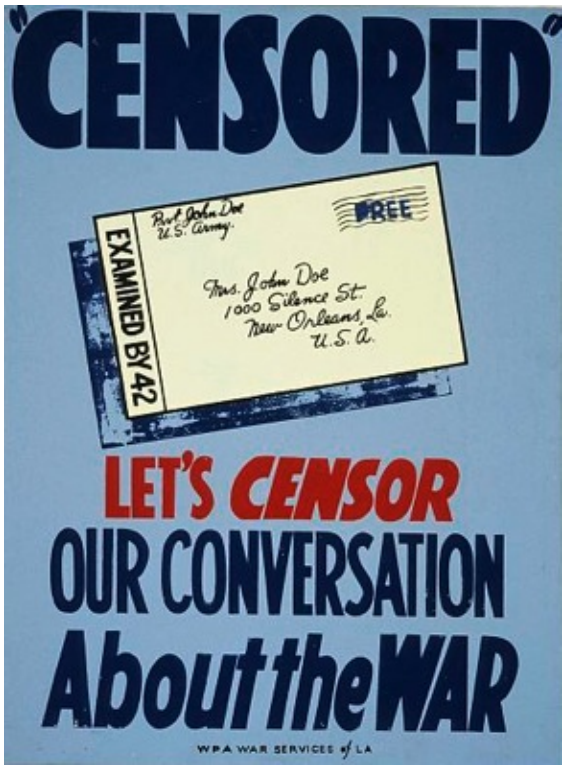

Figure 3: WWII-era censorship poster from the U.S. Library of Congress. Censorship in the digital age is far less simple.

Information Wants to be Free (http://en.wikipedia.org/wiki/Information_wants_to_be_free)

Digital information is slippery. Even the most aggressive attempts at limiting disclosure are not foolproof. Previous attempts at censoring communications, see Figure 3 (http://www.loc.gov/pictures/item/98518277/), look quaint in an era where an easily concealed 20 dollar thumb drive can hold 21 million pages of text (http://www.lexisnexis.com/applieddiscovery/lawlibrary/whitePapers/ADI_FS_PagesInAGigabyte.pdf). Encryption provides an all but impenetrable layer to mask malicious activity. Military censorship is an uphill battle that will only catch a few honest (http://www.wired.com/threatlevel/2011/10/diplomat-loses-security-clearance/) or inept people; true threats will likely take much longer or may never be detected. Censorship attempts also have a counterintuitive secondary effect—they often make the information more available. Coined the Streisand effect (http://en.wikipedia.org/wiki/Streisand_effect), attempts to remove information from the Internet tends to increase proliferation. For example, attempts to prevent dissemination (http://www.huffingtonpost.com/2010/08/05/us-military-banned-from-v_n_671967.html) of Wikileaks data (that was widely available online) only drew additional attention to the disclosure and prevented law-abiding Department of Defense personnel from studying the documents. To compound the problem of information disclosure, social networking sites entice disclosure (http://gcn.com/articles/2011/05/04/dodiis-social-media-creates-new-security-challenges.aspx) of sensitive personal information from government employees and service members, opening the door to misuse (http://gcn.com/articles/2012/05/23/military-dating-hack-government-social-media-risks.aspx).

Calling for “Cyber Support” is not the same as “Calling for Fire (http://www.globalsecurity.org/military/library/policy/army/fm/6-30/f630_5.htm)”

There is a trend now to consider cyber operations as being analogous to artillery fire missions. Fire missions are straightforward: get on the radio, pass along target grid coordinates, and moments later artillery rounds come raining in. The same isn't true for cyber operations. As we've discussed earlier, cyber weapons aren't guaranteed to work and even if they do their controllers may be reluctant to expend them against many objectives. Targeting is difficult and may span multiple countries, far beyond the sector of a tactical unit. Even a single bit (http://en.wikipedia.org/wiki/Bit) in error could result in collateral damage. While details of government cyber operations are not publicly available, civilian red team and penetration testing (http://en.wikipedia.org/wiki/Penetration_test) operations require extensive, time consuming planning. The murky law of cyber warfare compounds the problem, whereas the law of kinetic warfare is largely settled. Lawyers will be involved in cyber warfare, and you can be certain the timelines of many cyber operations will rarely approach the responsiveness of simple artillery fire for the foreseeable future.

Like it or not, Geeks are Warfighters

Cyberspace is the domain of technical experts, in some ways a hybrid of traditional Signals Intelligence and Communications domains, but in other ways altogether different. This cultural shift is uncomfortable for many (http://smallwarsjournal.com/jrnl/art/recruiting-development-and-retention-of-cyber-warriors-despite-an-inhospitable-culture). Technologists have historically not fared well (http://tech.slashdot.org/story/09/03/13/1336206/how-do-militaries-treat-their-nerds) in the military. Those with technical expertise may be reluctant to lead, lest their skills atrophy, and those without technical skills may not like the shift in power and status to the technologists. Human resources processes are a significant part of the problem. Military human resource systems were designed for interchangeable personnel in well defined specialties. Current guidelines in the Army require frequent moves and check-the-block career progression. Manning documents are based on outdated and slow-to-evolve specialty codes. Given the critical shortage (http://www.reuters.com/article/2012/06/12/us-media-tech-summit-symantec-idUSBRE85B1E220120612) of cyber security professionals, restrictive manning documents artificially constrain available positions to only a small, and often ill prepared, percentage of the force. One potential solution is the creation of a Special Forces-like model where candidates can be rigorously assessed and the best can be selected from across the force.

Conclusions

Cyber operations, alone or in concert with traditional kinetic operations, are intrinsic part of all future warfare. This article was designed to highlight how our physical world instincts often fail us when thinking about cyberspace. Cyberspace operations present both a critical national threat and a significant advantage to the defense of our country. By better understanding cyberspace and its laws of physics we will be better prepared for both.

The views expressed in this article are those of the authors and do not reflect the official policy or position of West Point, the Department of the Army, Army Cyber Command, US Cyber Command, or the United States Government.

Categories: cyberwarfare (/taxonomy/term/834) - cyberwar (/taxonomy/term/865) - cyber (/taxonomy/term/369) - asymmetric threats (/taxonomy/term/1095)

About the Author(s)

Matthew Miller (/author/matthew-miller)

Major Matthew Miller is a Signal Corps Officer and an Assistant Professor in West Point's Electrical Engineering and Computer Science department. He holds an M.S. from the Georgia Institute of Technology and a B.S. from West Point. He has served as a Brigade and Battalion Signal Officer as well as Company Commander in 1st Cavalry Division, in support of Operation Iraqi Freedom.

Jon Brickey (/author/jon-brickey-0)

Lieutenant Colonel Jon Brickey is an Information Systems Officer and the Army Cyber Command Fellow at the Combating Terrorism Center, West Point. He holds a B.S. from West Point, an M.S. from the Naval Postgraduate School, and a Ph.D. from the University of Colorado Denver. He has held leadership positions in cyber-related programs at the National Security Agency, USNORTHCOM, and USARCENT.

Gregory Conti (/author/gregory-conti)

Colonel Gregory Conti is a Military Intelligence Officer and Director of West Point's Cyber Research Center. He holds a Ph.D. from the Georgia Institute of Technology, an M.S. from Johns Hopkins University and B.S. from West Point. He has served as an advisor in US Cyber Command Commander's Action Group (CAG), as Officer in Charge of US Cyber Command's Expeditionary Cyber Support Element in support of Operation Iraqi Freedom, and co-developed US Cyber Command's Joint Advanced Cyber Warfare Course.