SMALL WARS JOURNAL

smallwarsjournal.com

Leadership of Cyber Warriors: Enduring Principles and New Directions

by Gregory Conti and David Raymond

Leadership is a core competency of the officers, warrant officers, and non-commissioned officers across the military services. A principle tenant of leadership is competence in the domain of operations. However, until recently, the defense of computer networks and the conduct of network warfare were treated as ancillary functions by the military services. The increasing cyber warfare threat against the United States, the creation of United States Cyber Command and the designation of cyberspace as a warfighting domain now necessitate study of the attributes of successful cyber warfare leaders and the leadership techniques required to successfully lead cyber warriors. In particular, we must develop an understanding of where traditional kinetic leadership paradigms succeed, where they fail, and where new techniques must be adopted.

Leadership is not a one size fits all endeavor. The capabilities and characteristics of the leader and the led and the missions proposed, combined with the impact of the operational environment, all merge to create a complex dynamic where capable leaders will adapt and succeed and less capable leaders will fail. *We argue that successfully leading cyber warriors takes a different type of leader, one who is comfortable in the inherently technical cyber domain, appreciates technical expertise, and understands the personality types, creativity, culture, motivations, and intellectual capability of cyber warriors.*

The emergence of a new warfighting paradigm and the need to adapt is not unique to the cyber domain. Leaders are products of their development processes, which sometimes becomes out of date. Colonels and General Officers of today's Army came through the ranks facing a Cold War threat. Even today, almost ten years into the Global War on Terrorism (GWOT), it is not uncommon to find senior officers who flounder in the counterinsurgency domain because it is an entirely different threat model than these officers faced earlier in their careers. At the same time there are junior officers who, with multiple GWOT tours under their belts, excel in conducting counterinsurgency operations but have little experience with large-scale combined arms warfare. These differences are to be expected. Leaders are the result of their experiences, training, education, and interaction with colleagues, but adaptation to new threats is paramount.

One could argue that the current developmental process of the military services, the promotion structure, personnel evaluation models, training programs, and awards systems are focused on combat arms development and, in their current form, are ill prepared to generate cyber warfare leaders. Cyber warfare is an entirely different, non-kinetic problem set compared to traditional warfare. As a result, qualified cyber leaders are rare and a mature, career long,

tailored development process is non-existent [1]. We argue that the "biggest caveman in the tribe" model (e.g. leaders who are adept at carrying heavy things up hills, surviving on one meal a day, and enduring sleep deprivation) should be replaced with a different model for cyber warfare leaders – one where the most innovative, most skilled in the cyber domain, and most effective technical problem solvers rise to the top. This is not to say that all facets of existing leadership should be discarded, the underlying principles of leadership remain the same, but these principles must be adapted with the cyber warfare mission, environment, and warrior in mind. Some tried and true leadership practices are likely to result in failure, and some principles, such as maintaining technical and tactical proficiency take on an entirely new meaning.

Figure 1: Special Forces candidates are weeded out in the "log pit," where they roll back and forth for long periods of time (left). A candidate becomes physically ill during the process and is hazed by the instructor (right). While these assessment techniques may have proven effective for selecting Green Berets, this approach would fail when selecting the most capable cyber warriors [2].

Differences Between Kinetic and Cyber Domains and Warriors

"I'm an artillery officer, and I can't fire cannons at the internet. Our future posture is still being worked out." -- Brigadier General Mark Kimmitt [3]

The difference in desirable leadership techniques and leader development stem from the people and skills required to conduct cyber warfare operations. These differences represent challenging requirements for change amidst a kinetic warfighting culture. Figure 1 depicts images from the United States Special Forces Assessment and Selection (SFAS) program. Early in SFAS, Special Forces candidates are forced to roll back and forth in a vertigo inducing "Log Pit" to weed out potential Green Berets. Clearly this is an extreme example, but it indicative of the larger kinetic warfighting culture that places the ability to endure physical hardship over intellectual capability.

1 Gregory Conti and John "Buck" Surdu. "Army, Navy, Air Force, Cyber: Is it Time for a Cyberwarfare Branch of the Military;" Information Assurance Newsletter, Vol. 12, No. 1, Spring 2009, pp. 14-18.
2 "Surviving the Cut." Discovery Channel Documentary, 17 December 2009. Available online at http://dsc.discovery.com/videos/two-weeks-in-hell-only-the-first-day.html
3 James Westhead. "Planning the US 'Long War' on Terror." BBC News, 10 April 2006. Available online at http://news.bbc.co.uk/2/hi/americas/4897786.stm

The Cyber Battlefield and the Physical Battlefield

One of the best descriptions of the difference between the cyber battlefield and the kinetic battlefield was given by Brigadier General Mark Kimmitt, who concisely illustrated the ephemeral nature of cyberspace and the near irrelevance of conventional weapons in working against it. These characteristics are the reality of war in cyberspace. The Internet is resistant to even nuclear attack because it routes around physical destruction.[4] In this environment, attempts at censorship or to prevent the dissemination of undesirable information have proved to be impractical. Distance and national borders are irrelevant in many instances. Information flows at nearly the speed of light, but attacks are difficult to trace back to the source. Anonymity is built into the design of the Internet and definitive attribution of real world attackers is an ongoing challenge. One individual may possess dozens of dramatically different online personas. New weapons can be coded by a couple of teenagers over a weekend. Law and policy lag, often a long way, behind technological advancement leaving vast areas of conflicting legal and ethical uncertainty [5]. On the other hand, after centuries of practice, traditional kinetic warfare is far more mature. Training programs are highly refined to produce line troops and special operations units. The law of land warfare defines the commonly accepted legal and ethical boundaries of the conduct of kinetic war.

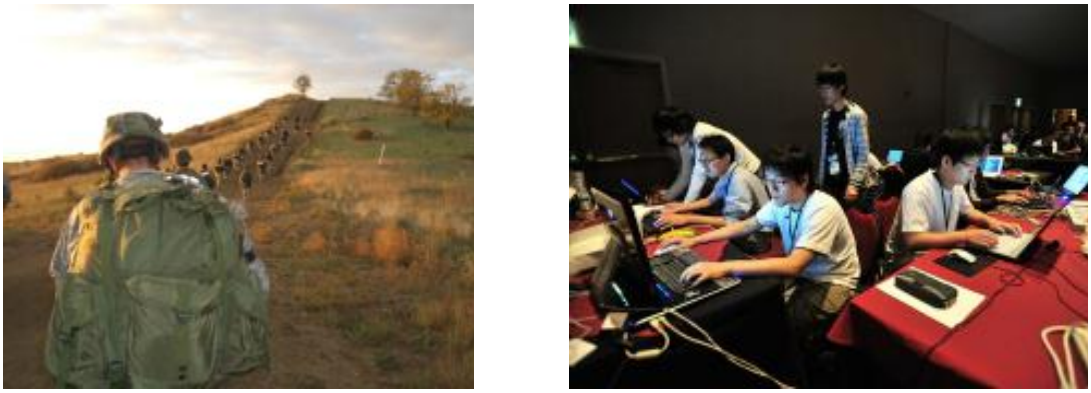

Figure 2: The warfighting environment and combat missions of a cyber warrior are vastly different than in kinetic warfare. We need to move beyond leaders comfortable carrying heavy things up hills (left) toward leaders adept at leading teams of technologists across networks (right) [6,7].

Differences Between Cyber and Kinetic Warriors

There are similarities between cyber warriors and kinetic warriors as well as stark differences. The ideal cyber warrior will possess high technical aptitude, be a creative problem solver, and possess a hacker mindset that enjoys manipulating complex systems and pushing technology in ways unintended by its designers. One downside of the hacking ethos is the siren

[4] This isn't to say that kinetic effects cannot be carefully employed to shape cyber infrastructure.
5 Gina Cairns-McFeeters, John Shapiro, Steve Nettleton, Sonya Finely and Daryk Zirkle. "Winning the Ground Battles but Losing the Information War." Small Wars Journal, 21 January 2010.
6 Image source: http://commons.wikimedia.org/wiki/File:DEF_CON_17_CTF_competition.jpg
7 Image source: http://www.carson.army.mil/units/4eng/images/photos/62nd/061001_full.jpg

song of conducting unethical or illegal activities, particularly as one's skills advance. A key leadership challenge may be to ensure fundamental values of integrity, loyalty and duty are internalized by the cyber warrior and the unit. Where a kinetic warrior may own a Beretta 9mm pistol, a cyber warrior may have their own malware analysis lab tucked away in their basement. From our experience, cyber warriors are often independent and expect that their leaders are at least as bright and technically skilled as they. Many will have college degrees and professional certifications and take part in alternative hobbies and lifestyles. Contrast this with the physical prowess-centric kinetic warfare environment, where being the biggest caveman in the tribe is often enough to earn the respect of the led. Hackers and cyber warriors have a RTFM (Read The Manual) culture, which expects individuals to make every effort to answer their own question before asking an expert. In the intellect-centric environment of cyber warriors, general leadership and management skills alone, without intelligence and technical competence, will not carry the day. Because of their independent streak and desire for intellectual peers (or betters) for leaders, building teams of cyber warriors is a non-trivial leadership challenge for the uninitiated [8]. Different incentive structures may be necessary, for example pinning an achievement medal on a cyber warrior may not be valued as much as an opportunity for access to a new piece of technology or an advanced malware analysis course.

The best leaders will adapt to the characteristics and needs of their people. The cyber warrior is a different animal than the kinetic warrior. In the next section we've outlined leadership principles, both old and new, for taking these differences into account.

Applying Traditional Leadership Principles to the Cyber Warrior

Do you know what TOR is? If not, go find out.

- Anonymous US Cyber Command Leader to his Subordinates

In this section we present leadership principles tailored to leading the cyber warrior. We've included some of the 11 time-tested leadership principles from the Army's classic field manuals on military leadership and augmented them with additional principles based on our long-term experiences leading cyber warriors and military technologists [9]. While the 11 Principles of Leadership are no longer part of Army doctrine (FM 6-22, Army Leadership, replaced the Army's FM 22-100 in October 2006 and no longer lists the Principles of Leadership), these principles have become an integral part of the Army leadership lexicon. We've deliberately excluded some of these principles, not because they aren't applicable to sound leadership, but because we believe they do not require additional explanation in the context of cyber warriors and this article.

Know Yourself and Seek Self-improvement

Each leader must continually assess their strengths and weaknesses and seek self-improvement to augment nascent military training programs. Whereas mature professional development programs exist across the Army and other services for kinetic warfighting, cyber warfare education programs are just emerging. At some point in the future enlisted, warrant

8 TJ O'Connor and Joseph Doty. "We Need Teams of Cyber Warriors." Army Magazine, Vol. 60, No. 1, January 2010. Available online at http://www.ausa.org/publications/armymagazine/archive/january2010/Pages/BuildingTeamsofCyberWarriors.aspx.
9 FM 22-100. Military Leadership. United States Army, 31 October 1983.

officer, and officer cyber warriors will be able to lean heavily on service programs for career-long professional development, but we aren't there yet. Even when these programs exist, the rapid rate of change in technology and cyber warfare tactics will necessitate that every leader maintain and extend their skills through civilian education, professional reading, guest speaker programs, research, writing, conference attendance, and industry certifications and training, among numerous other techniques. As the above quote implies, cyber leaders must be capable of teaching themselves unfamiliar technology, such as the TOR anonymization network which helps attackers (and law abiding citizens) operate anonymously on the Internet. The full range of topics a cyber warrior must understand is beyond the scope of a single article, but examples include: how a webserver works, how domain names (e.g. www.us.army.mil) are converted into IP addresses (143.69.251.36) by the Domain Name System (DNS), the basics of a buffer overflow, and how passwords may be cracked through brute force techniques. Cyber leaders must also understand bigger picture concepts such as security through obscurity, security theater, that cryptography won't solve every problem, and the implications of a major breakthrough in quantum computing to military and governmental secure networks.

Continually identifying one's gaps in knowledge and passionately continuing professional development is a lifetime journey in cyber warfare and even the best formal military training programs will provide only a baseline of necessary expertise. On the job experience, obtained through a sequence of cyber warfare assignments and self-study of emerging technologies, debates, and policies is a mandatory prerequisite for the successful cyber leader.

Importantly, leaders must also know their units and facilitate subordinate's self-improvement. This includes providing opportunities for education and partnership with industry experiences, as well as opportunities to move around to other positions in the cyber warfare field. In short, leaders must seek out every opportunity to feed their subordinates knowledge. True cyber warriors will be hungry for knowledge and satiating this need will help grow more capable cyber warfare units, warriors, and leaders.

Be Technically Proficient

My Boss Didn't Know the Difference Between an IP Address and a Phone Number.

- Anonymous Cyber Soldier

Technical competency is *the* fundamental requirement for a leader in cyberspace. It is impossible to plan and conduct cyber warfare if the leader does not understand the laws of physics as they apply to networks and automation. Mere intuition is not a substitute, however, as the laws of physics are often counterintuitive in cyberspace. Adversaries may walk through walls, become invisible, move at the speed of light, change from male to female, alter history, teleport around the globe, or attack from a million locations at one time.

Consider an artillery fire mission. In the physical world a soldier can pick up a radio, make a request for artillery support, and moments later hellfire and damnation come raining down from the heavens. Easy and intuitive, just don't send in the wrong target map coordinate by accident. The same is not true on a network. If, for example, an attacker wanted to take down a malicious webserver, there is significantly more complexity. The malicious webserver's domain name may be hosted in one country, the webserver itself could reside in another (perhaps friendly) country, and media embedded on each web page may be hosted in dozens of others locations around the globe. Even a single physical server may be an enigma for the uninitiated,

as the webserver may reside in a virtual machine alongside dozens of other legitimate sites, creating ample opportunity for unanticipated collateral damage. Even if a given physical server was destroyed, mirrored copies may instantly be brought online or backups of the site may be moved to another location halfway around the world in minutes.

Technical competence demands continued self-study, formal education, and professional development. Development of traditional battlefield weapons and tactics occurs on the order of years, if not decades, but paradigm shifting developments in cyber warfare may occur overnight. Lack of technical literacy and an understanding of the cyber domain begets ineffective, potentially dangerously incompetent, leaders who will not gain the respect of their personnel and who will fail in cyber war as technically adept adversaries run circles around them on the battlefield. We aren't saying that a PhD in computer science is necessary, however technical fluency is a must. Once technical literacy is gained, it must be maintained. Standing still as a cyber warfare leader will mean one is quickly left behind as current techniques, skills, and tools necessary for cyber warfare rapidly evolve.

Build a Team

Extra attention might have to be devoted to teambuilding in a group of military personnel drawn to an organization focused on network attack and defense. There is a nugget of truth in most stereotypes and the image of a computer hacker plying his or her craft alone in a darkened room for hours at a time is a common one. In general, individuals who are drawn to science and technology are more introverted than your typical military leader, who is extroverted, exuberant, and hard charging. Not only must this group of largely inward looking individuals be forged into a team, but the leader must recognize that the group likely won't interact like other teams. In other words, the team might be forged without the leader even recognizing it!

Some Army organizations forge strong teams though shared adversity, others through cooperative problem solving. The latter approach is probably more effective with a group of technologists. One must be careful, however, to ensure that the problem solving is cooperative and not a single individual trying to work through the problem on his or her own.

Leading in cyber warfare is also inherently about functioning in a team cyber environment – one that is joint, multinational and interagency. Leaders, need to develop a solid understanding of all these dynamics, but still need to understand fundamentals of joint operations to appreciate how to best integrate cyber capabilities of their team into full spectrum operations

Employ Your Team in Accordance with its Capabilities

Rank is nothing: talent is everything. - David Kilcullen

A leader must recognize specific competencies among his or her subordinates and assign duties and responsibilities accordingly. In the cyber arena, perhaps more so than in other domains, leaders may often have to ignore traditional rank-based notions of who "leads" (or manages) a team or organization. A private's skill set might make her more suited to lead a group of non-commissioned officers than the senior sergeant in a group assigned to accomplish a certain task. This is counter to the kinetic leader's traditional viewpoint – only in dire circumstances might a junior infantry squad member lead the group on an attack – but it might make perfect sense to cyberwarriors whose culture is more of a group of peers with varied skills and experiences. Not only must the commander in the above example be able to assess and

make such assignments, but the senior sergeant must understand and be able to subordinate himself to the private.

This is especially true as we try to assemble network warfare units without the benefit of an established pipeline of competent cyber warriors. Privates and Senior Non-Commissioned Officers might join the organization with similar levels of network defense training, but in different focus areas (varied operating systems, network architectures, etc). A junior enlisted Soldier might end up in a cyber warfare unit with significant industry experience and when the time comes to harden a specific network to potential attack, she may have the best mix of skills and experience to lead the team.

Other Cyber Leader Imperatives

Aside from the application of core leadership principles to cyber leadership, there are other behaviors that we consider to be critical to success in this domain.

Use Physical Hardship-based Kinetic Leadership "Best Practices" Sparingly

Success in certain corners of the military is determined by a leader's ability to endure sleep deprivation, eat one meal a day, and set the pace for eight mile runs. In the highly physical world of combat arms operations these techniques prove successful, however they should be used sparingly when dealing with cyber warriors. It is not that cyber warriors shouldn't be fit in order to accomplish their jobs, it is that cyber warriors put a far greater emphasis on intellectual and technical prowess than physical aptitude. From our observations, kinetic leaders will sometimes resort to their comfort zone of morning physical fitness runs, long road marches, and unnecessary field training exercises for their cyber troops which, while they may have succeeded in the past, often prove counterproductive in building a cohesive cyber warfare unit, particularly when the leader is not proficient in cyber warfare.

Communicate Technical Issues Effectively to Non-Technical Audiences

There are 10 types of leaders, those that understand binary and those that don't.

- Common Joke in the Tech Community

A key requirement of a cyber leader is the ability to communicate technical details to a non-technical audience, and vice versa. In particular, a cyber leader must be capable of translating warfighting requirements to technologists for mission execution as well as to communicate technical capabilities and shortcomings back to warfighting organizations. However, as a leader moves up in rank and responsibility, the diversity of audiences increases greatly. For example, it would not be uncommon for a mid-career cyber leader to communicate with tactical military forces, high-level Joint military commands, special operations units, legal professionals, hackers, academics, and computer security business leaders as well as representatives of government agencies including the National Security Agency, Central Intelligence Agency, Department of Homeland Security, Department of Justice, Department of the Treasury, Congress, and the White House to educate, discuss issues and jointly seek solutions. Members of the media and electronic civil liberties advocates are also understandably concerned with cyber warfare activities and deserve the ability to interface with individuals who understand their viewpoint and speak their language.

The perception of the military across these external organizations will range from strong support to inept knuckle dragging troglodyte to callous violator of civil liberties. These are not pleasant things to hear, but the perceptions (and the occasional reality) in certain circles are real. We argue that cyber warfare organizations should seek transparency and engagement whenever possible. By engaging people with clear communications, even to those who think United States Cyber Command shouldn't exist, we have much to learn. Clearly, there must be boundaries that shield ongoing operations and classified information, but a good faith effort to engage and effectively communicate with our partners and the American people will help the cyber warfare community demonstrate its value to those that pay for its existence, making both communities stronger for it.

Understand Cyberwar Policy and Effects

Cyber warfare has profound policy implications. A mistyped keystroke could result in an attack against an entirely different country or a malicious file may propagate far beyond desired targets to non-combatants. Senior kinetic warfighting leaders will look to their cyber warriors to explain the range of authorized actions and their associated risk-benefit tradeoffs. The Law of Land Warfare, the Geneva Convention, and Theater rules of engagement are quite static and mature compared to the rapid change in policy surrounding cyber war. Rapid change does not negate the requirement for cyber leaders to understand current policy, it necessitates it.

Must be Operationally Involved

Mandating operational involvement for a leader may sound counterintuitive to traditional kinetic leaders, but it is possible for cyber warfare leaders to be disconnected from operational activities of those they command, not due to a one-off personal failure of an individual, but as a matter of organizational design. For example, under current structures, a company commander may have very little to do with the operational activities of his or her company. Given the evolving nature of cyber warfare units and their close intelligence community partnerships, a leader's personnel may be assigned across a large headquarters where they work for another, operational chain of command. This may change, as new cyber warfighting units are created, but currently the commander of such a unit risks becoming merely an out of touch administrative functionary isolated from the core functions of their command. In cases where operational involvement for a leader is not built into the organizational structure it is critically important to find innovate ways to stay connected. For example, the Army Network Warfare Battalion deliberately dual-hatted Company Commanders and placed them in key positions in NSA and Cyber Command's operational mission areas lest they became out of touch.

Create a Culture of Innovation that Allows Tackling Hard Problems

I Trust You. - A Cyber Warfare Commander to a Subordinate

Cyber warfare presents challenges that cannot be solved in a matter of days. This isn't unique to the cyber domain, nation building, countering improvised explosive devices, and defeating insurgencies all require long-term efforts to develop solutions. Traditionally, the individuals working on these solutions are mid-career or more senior officers. In cyber warfare the full spectrum of enlisted, warrant officer, and officer talent must be tapped to generate appropriate tactics, strategies, policy, and technology. Cyber warriors of any rank will be bright and capable of solving hard problems, but they require a creative work environment and culture

of innovation that allows ideas to be heard regardless of rank. This notion runs counter to traditional military culture where the senior leader issues a directive and the unit complies. Of course, service members of any discipline should voice their concerns if a directive isn't well thought out, overly dangerous, or illegal, but subordinates do so at potentially career ending risk. We suggest that leaders actively incentivize and operationalize a culture that allows subordinates to explore new ideas. For example, the Army Network Warfare Battalion encouraged soldiers to take half a day off a week to solve hard problems of their choosing. Note that research and creativity is untidy, and will sometimes lead to dead ends (and this is ok), but allowing your subordinates to tackle hard problems will generate surprising successes. Of course it is necessary to impose limits, lest creativity cross ethical, legal, or other boundaries, but commanders should allow a very wide lane for exploration. In other words, a leader should give subordinates the desired goal, lots of latitude, and stand back. Leaders must constantly encourage initiative, power down to the lowest level, stimulate new ideas, and actively seek out people who are change agents and empower them, regardless of rank or place in organizational structure. To facilitate initiative, leaders must allow subordinates to try new things and allow them to fail, underwrite honest mistakes, and trust their subordinates. For the talented cyber warrior the ability to self-select and pursue interesting problems is a highly desirable attribute of their work environment. Creating such an environment will improve morale, increase retention, and generate solutions to pressing cyber warfare problems [10].

Add Value for the Kinetic Warfighter

Cyber warfare does not exist in a vacuum, nor does it exist at just the strategic level. For success, cyber warriors must add value to the larger Army, Navy, Air Force, and Marine institutions that they support through tangible and timely contributions, or else risk becoming marginalized and irrelevant. The key to such support are the right people, with the right expertise actively seeking to add value for kinetic warfighters. Cyber warfare leaders must avoid thinking that cyber capabilities are an end unto themselves or to look with disdain on traditional kinetic personnel and missions. Adding value to the kinetic warfighter will facilitate acceptance of cyber personnel as "operators," warriors and comrades in arms, to the benefit of the joint, combined, and multinational team.

Conclusion

The Army will need this lieutenant 20 years from now when he could be a colonel, or 30 years from now when he could have four stars on his collar. But I doubt he will be in uniform long enough to make captain. [11]

The core principles of leadership remain the same, but the cyber warfare leader must adapt to the needs of the inherently different missions, personnel, weapons, and environment of cyber war. Leaders must be adept lifetime learners who maintain currency with advancing technology, threats, policy, and tactics, and inspire the same in their subordinates. The leader must create an environment which facilitates innovation and initiative by allowing creativity, underwriting honest mistakes, providing goal-oriented objectives, and boundaries upon proper

10 Gregory Conti and Jen Easterly. "Recruiting, Development, and Retention of Cyber Warriors Despite an Inhospitable Culture." Small Wars Journal, 29 July 2010.

11 Lucian Truscott. "The Not-So-Long Gray Line." New York Times, 28 June 2005. Available online at http://www.nytimes.com/2005/06/28/opinion/28truscott.html?pagewanted=2

behavior. Cyber warriors have immense potential, but it is up to the qualified and prepared cyber leader to unleash this potential, and effectively execute cyber warfare missions on behalf of our Nation.

LTC Gregory Conti is Military Intelligence Officer and Director of West Point's Cyber Security Research Center. He holds a BS from West Point, an MS from Johns Hopkins University and a PhD from the Georgia Institute of Technology, all in Computer Science. He is a frequent speaker at leading security conferences including Defcon, Black Hat, RSA, and Shmoocon. He recently returned from a deployment as Officer in Charge of United States Cyber Command's Expeditionary Cyber Support Element in support of Operation Iraqi Freedom. He has also deployed in support of Operations Desert Shield and Desert Storm.

LTC David Raymond is an Armor Officer and Assistant Professor in West Point's Department of Electrical Engineering and Computer Science. He holds a BS from West Point, an MS in Computer Science from Duke University, and a PhD in Computer Engineering from Virginia Polytechnic and State University. LTC Raymond's research interests include wireless sensor and mobile ad hoc networks, wireless network security, and online security and privacy. He has deployed in support of Operations Desert Shield, Desert Storm and Iraqi Freedom.

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

Acknowledgements

We would like to thank LTC Jen Easterly, former commander of the Army Network Warfare Battalion, for sharing her command philosophy and providing important feedback on this paper.