Can you hear me now?

Colonel Stephen Hamilton, Ph.D.

VOLUME 9 • NUMBER 1

SPRING 2024

THE CYBER DEFENSE REVIEW

Operational Perspectives from the Field – ARCYBER in the Cyberspace Domain
Lt. Gen. Maria B. Barrett

Mission Thread Analysis: Establishing a Common Framework in a Multi-discipline Domain to Enhance Defensive Cyberspace Operations
Col. George I. Corbari, Col. Neil Khatod, Col. John F. Popiak, Pete Sinclair

Beyond USCYBERCOM: The Need to Establish a Dedicated U.S. Cyber Military Force
Col. Jeffrey Couillard

2023 Executive Order on Trustworthy AI Misses Issues of Autonomy and AI Multi-Threat Challenges
Dr. Chris C. Demchak and Dr. Sam J. Tangredi

Violent Limitation: Cyber Effects Reveal Gaps in Clausewitzian Theory
Maj. David Greggs

Quantum Leap: Improving Cybersecurity for the Next Era of Computing by Focusing on Users
Maj. W. Stone Holden and Michael Gerardi

How the Collapse of the Soviet Union Made Russia a Great Cyber Power
Alec Jackson

Communities, Agency, and Resilience: A Perspective Addressing Tragedy of the Cyber Commons
Dr. Samir Jarjoui, Dr. Renita Murimi, Robert Murimi

FROM THE EDITOR — *Deborah S. Karagosian*

INTRODUCTION *Can you hear me now?* — *Col. Stephen Hamilton*

ARMY CYBER INSTITUTE • WEST POINT PRESS

While serving at USCYBERCOM, shortly after it was created, I began to make my way around various parts of the agency and one day, I had an interesting conversation with a senior civilian. He asked me a rhetorical question I had to think hard about: "What matters more: the message or the ability to send that message?" I pondered it momentarily, trying to decide on what message was critically important—was it a 911 call? A call for fire at a critical point in battle? These are critically important. However, the message is meaningless if you do not have a way to send it. It suddenly became clear to me where he was going: it is the ability to send a message that is important. The ability to communicate is paramount to just about everything we do, and cyber turns that ability on or off. After more than a year as the Director of the Army Cyber Institute, I'm not so sure anymore.

COL Stephen Hamilton is the Director of the Army Cyber Institute at the United States Military Academy (USMA) located at West Point, New York. In his position as Director, COL Hamilton leads a multi-disciplinary team of military and civilian scholars who provide advisement and research for the U.S. Army. He has a B.S. in Computer Science from USMA, an M.S. in Software Engineering from Auburn University, and a Ph.D. in Computer Science from Johns Hopkins University. COL Hamilton additionally teaches Cloud Computing in the Department of Electrical Engineering and Computer Science. He began his career as a signal officer and deployed in support of Operation Iraqi Freedom in 2004 where he commanded Alpha Company 57th Signal Battalion. Following a tour at USCYBERCOM, he transferred to the Cyber Corps. He holds an extra class amateur radio license, and his research interests include software-defined radios, cloud computing, and data visualization.

Communication is always challenging, especially in the highly technical cyber domain. To pull this thread a little more, consider the following example. If the message is important, then it must make it to the destination intact, and the sender needs confirmation it was received (i.e., syn-ack in TCP). This is generally good enough for short concise communication; however, what if the message is not clear? What is the syn-ack equivalent of understanding the *meaning* of the message? In computer terms, this is typically solved with a hash function. However, there is no equivalent for humans other than possibly having the receiving person explain back to the sender what they understood about the communication. If what I just wrote went over your head, is that my fault as the message sender or your fault as the receiver? Did just reading that – the ability to send the message – accomplish what either of us hoped for?

However, with some thought and work, it is possible to communicate technical topics succinctly. During the beginning of the COVID lockdown, I was teaching a web application course, and since we went completely remote, the cadets used our private VPN to connect to the department's hypervisor server to build web applications on virtual machines. This allowed me to see each of their screens in a browser tab, giving me direct feedback on what the cadets were doing while I instructed them how to set up the web framework. I quickly realized that as I spoke, they often interpreted my words to result in different outcomes than expected. Since I could see this in real-time, I could correct what I was saying to explain further how to perform a task. This made me think about how we may believe in our head that we have communicated something perfectly; however, all too often, we do not realize that the person listening may not receive the message that we intended to communicate.

A quote widely attributed to Mark Twain says, “I didn’t have time to write a short letter, so I wrote a long one instead.” While most topics are complicated and experts tend to push back against writing short summaries of their work, as the director of ACI, I am constantly looking for ways to take difficult-to-understand topics and break them down so we can successfully communicate them in no more than one page. These one-page documents are essential for senior leadership, as there is not enough time in the day to go down the rabbit hole on all the topics within cyber. The problem is that it takes more time to boil down certain topics into their essence and communicate them clearly – but it is also a mark of an expert to be able to explain something simply. Several of our academic programs at USMA require cadets to write shorter papers, and while they initially think these will be easier, they quickly learn the errors in their assumptions.

Cyber experts have not always excelled in clearly communicating issues around their field to non-experts. The depth of technical expertise required to understand cyber operations and actions is critical to our mission, and so is communicating clearly to non-experts. Therefore, it is vital to communicate as thoroughly as possible to ensure we create a shared understanding of our cyber world – the ability to send the message is equally essential to ensuring the content of the message is received as intended. It is common to use a baseline of what someone knows to explain something new. However, the delta between what is known, and unknown can easily lead to misunderstanding. In “Mission Thread Analysis: Establishing a Common Framework in a Multi-Discipline Domain to Enhance Defensive Cyber Operations,” COL Corbari et al. directly state, “Miscommunication results in a different understanding of mission requirements and similarly the expectations between those requesting support and those providing support.” They propose a method of tackling this problem by proposing a Mission Thread Analysis (MTA) concept to help close this communications gap.

Other articles in this edition focus on combining traditional warfighting knowledge with cyber expertise to help bridge the gap between cyber and other warfighting functions. The range of articles in this edition goes from examining Clausewitzian Theory on war (Violent Limitations: Cyber Effects Reveal Gaps in Clausewitzian Theory) to the future of cybersecurity in a post-quantum world (Quantum Leap: Improving Cybersecurity for the Next Era of Computing). Finally, LTG Barrett’s article discusses ARCYBER’s enterprise capabilities. She first discusses NETCOM, which operates the world’s largest network of its kind. This network provides the Army with the ability to communicate worldwide. All of these articles display that even in this one cyber journal, we look to the history of what we know to help describe the future of cyber, yet there are gaps, and it is difficult.

I hope you enjoy this edition of the CDR, and I challenge you to not only read these articles but also think about how you can better communicate about cyber in your work!