VOL. 7 ◆ NO. 4

The Only Constant is Change...

Colonel Jeffrey M. Erickson

The ancient Greek philosopher Heraclitus is credited with the quote "The only constant in life is change." While Heraclitus was certainly not thinking of cyberspace or modern technologies, it occurs to me that he may have been onto something with respect to the larger world of cyber related issues as we have seen continual evolution since the founding of the Army Cyber Institute (ACI) at West Point.

This Fall marks ten years since the creation of the ACI by the Secretary of the Army, John McHugh, and the Chief of Staff of the Army, General Raymond Odierno, in 2012 to serve as "a national resource for research, advice, and education in the cyber domain, engaging military, government, academic, and industrial cyber communities in impactful partnerships to build intellectual capital and expand the knowledge base for the purpose of enabling effective Army cyber defense and cyber operations."

At the time, the Army was trying to figure out the best approach to address the uncertain environment and growing demand for a deeper understanding of the cyberspace environment, as well as its potential positive and negative impacts on the Army, the Department of Defense, and the Nation. In the past decade, the Army's Cyber Community has seen significant changes across many areas. Some of the highlights include:

Colonel Jeffrey M. Erickson is the Director of the Army Cyber Institute at the United States Military Academy (USMA) located at West Point, New York. As Director, COL Erickson leads a 60-person, multi-disciplinary research institute focused on expanding the Army's knowledge of the cyberspace domain. He began his Army career as an Armor officer before transitioning to the Simulation Operations functional area, where for the last 15 years, he has been using simulations to train from the individual to the Joint and Combatant Command levels. He has a B.S. in Computer Science from the United States Military Academy, an M.S. in Management Information Systems from Bowie State University, and an M.S. in National Resource Strategy from the Eisenhower School (formerly the Industrial College of the Armed Forces). His fields of interest are simulations for live-virtual-constructive training, testing, and wargaming.

- The creation of the Cyber Branch in 2014, recognizing the necessity for a dedicated cadre of cyber experts for the Army, and marking the Army's the first new branch since the Special Forces was established in 1987
- The designation of Ft. Gordon from the Signal Center of Excellence to the Cyber Center of Excellence and the creation of the U.S. Army Cyber School in 2014
- ACI published the first issue of *The Cyber Defense Review* in 2016, the first DoD-sponsored cyber-focused journal
- The creation of the Army Futures Command in 2017 to develop future Army readiness
- U.S. Cyber Command's (USCYBERCOM) elevation to a unified combatant command in 2018
- The creation of the 915th Cyber Battalion in 2019 to provide an organic expeditionary capability to Army Cyber Command (ARCYBER)
- The move of ARCYBER from Fort Belvoir to Fort Gordon in 2020 to achieve synergy between the operational and institutional sides of the cyber force

These milestones were steps in the evolution of the Army Cyber Community towards greater capability, a more defined identity/culture, better integration from the tactical to the strategic levels, and a widespread recognition of the necessity for improved cyber capabilities.

A key component of these changes is the open and continuous dialogue and debate among operators, senior leaders, academics, industry leaders, and government officials in analyzing courses of action, making decisions, and implementing plans. The CDR authors continue to add to the dialogue and debate by presenting new and developing perspectives on the challenges of cyberspace.

I thank all our Fall authors for their invaluable contributions and would like to recognize a few for their focus on change:

- **What do leaders need to know to navigate the cyber domain?** LTC Andrew Farina's article ("The Impending Data Literacy Crisis Among Military Leaders") captures key points about leaders struggling to achieve data literacy in understand new technologies and paradigm shifts, in this case related to data literacy.
- **How should we organize to operate in cyber?** LCDR Michael McLaughlin advocates for the creation of a "Seventh Service" for the United States with authorities more akin to the Coast Guard and National Guard.
- **How do we adjust our approach?** In "Tactics and Technicalities Undermining Strategy," Australian Brigadier Martin White argues that the downfall of our current approaches is the focus on analyzing too much information, resulting in an overall weaker posture.
- **How do we change our enemy's perception?** LTC Ryan Tate and COL Chad Bates argue for increased deterrence by being more transparent with operations in their article "Deterrence Thru Transparent Offensive Cyber Persistence."

These authors argue for changes to the people, processes, and technologies we use to see ourselves, our adversaries, and the terrain in cyberspace. As the ACI begins its next decade, expect to see constant changes across the Cyber Force with CDR authors constantly seeking solutions to future problems.