Military Cyber Affairs

Volume 4
Issue 1 *Command and Control of Cyberspace Operations*

Article 1

2019

Introduction to Command and Control of Cyberspace Operations

Bobbie Stempfley
Software Engineering Institute at Carnegie Mellon University, rgs@cert.org

In 2011, Marc Andreessen published his view of the future as an op-ed in the *Wall Street Journal* when he asserted that "software is eating the world."[1] Over the past 8 years, his assertion has proven true as software impacts an ever-growing share of our economy. We no longer think of Amazon as a bookseller, Netflix as a DVD distributor, or Verizon as a phone company—software has empowered these and many other corporations to respond with the agility that the market has both enabled and required. In short, they succeeded because they viewed software as a "strategic asset." This same transformation has been occurring in the U.S. military as warfighting capability has become even more connected and data driven. The recognition of cyber as an operating domain in 2011 not only underscored DoD's dependence on it—the code, connections, and information important to warfighters—but also laid a foundation for the kind of multi-domain operational concepts being discussed today.

The U.S. Air Force Chief of Staff predicts that "victory in future combat will depend less on individual capabilities and more on the integrated strengths of a connected network available for coalition leaders to employ."[2] This dependence is key to the current digital transformation going on across the Air Force, and it is not alone. The Air Force strategy for increased power reinforces the tenants of the DoD's Cyber Strategy, highlighting an approach of persistent engagement, persistent presence, and persistent innovation. In the U.S. Army's recently released Mission Command 2028, "[t]he central idea in solving this problem is the rapid and continuous integration of all domains of warfare to deter and prevail as we compete short of armed conflict."[3] And to deter our adversaries' engagement, we must create and thrive in a multi-domain environment that reduces the adversaries' desire to engage.

It is within this context that we look at the means and doctrine for command and control today and in the future. The physical and temporal limitations of land, sea, air, and space don't exist in cyber. The players extend beyond the military and the industrial base to include the private sector, civil society, civilian infrastructure, and even the public. The constructed nature of cyber and space allows for new ways of approaching engagement but also spawns new complications to the clarity of messaging across domains. These are but some of the challenges facing leaders at all levels as they grapple with how to integrate operations within and across land, sea, air, space, and cyberspace and enable rapid, agile, and effective information flow and decision making.

---

[1] Andreessen, Marc. "Why Software Is Eating the World." *The Wall Street Journal*. 20 August 2011. https://www.wsj.com/articles/SB10001424053111903480904576512250915629460

[2] Pope, Charles. "Goldfein Details Air Force's Move Toward a 'Fully Networked' Multi-domain Future." U.S. Air Force. 17 September 2019. https://www.af.mil/News/Article-Display/Article/1963310/goldfein-details-air-forces-move-toward-a-fully-networked-multi-domain-future/

[3] U.S. Army. *The U.S. Army in Multi-Domain Operations 2028*. TRADOC Pamphlet 525-3-1. 6 December 2018. p. iii. https://www.tradoc.army.mil/Portals/14/Documents/MDO/TP525-3-1_30Nov2018.pdf

Recently, Stanley McChrystal shared this insight: "The ability to adapt to complexity and continuous unpredictable change [is] more important than authority and carefully prepared plans."[4] How military operators understand and internalize this need for speed, experimentation, and persistent engagement is the crux of what we wanted to study in this edition of *Military Cyber Affairs*. We chose papers that looked at command and control from a variety of perspectives—How do the players perceive cyberspace as an operating domain? How do these perceptions impact their imagination and their approaches? What are the differing needs for technical forensics based on the purpose of the participants? And what do we really understand about how command and control in the cyber domain is the same and different as in other domains?

Over my time engaged in cyberspace, I have seen how far we've come as a community, but the continuous evolution of cyber and our experience operating in and integrating the domain require continuous learning to leverage and protect it. I look forward to engaging on these and other emergent topics as military cyber professionals explore the interconnected nature of cyber and information in global multi-domain operations.

[4] Denning, Steve. "How Fake Agile at DoD Risks National Security." *Forbes*. 22 September 2019. https://www.forbes.com/sites/stevedenning/2019/09/22/how-fake-agile-at-dod-risks-national-security/