January 2016

A Challenge for the Military Cyber Workforce

Michael S. Rogers
US Cyber Command

Follow this and additional works at: <https://digitalcommons.usf.edu/mca>

Recommended Citation

Rogers, Michael S. (2016) "A Challenge for the Military Cyber Workforce," *Military Cyber Affairs*: Vol. 1 : Iss. 1 , Article 2.
<http://dx.doi.org/10.5038/2378-0789.1.1.1012>
Available at: <https://digitalcommons.usf.edu/mca/vol1/iss1/2>

This Article is brought to you for free and open access by the Open Access Journals at Digital Commons @ University of South Florida. It has been accepted for inclusion in Military Cyber Affairs by an authorized editor of Digital Commons @ University of South Florida. For more information, please contact digitalcommons@usf.edu.

A Challenge for the Military Cyber Workforce

ADMIRAL MICHAEL S. ROGERS

Commander, US Cyber Command
Director, National Security Agency
Chief, Central Security Service

Powerful and networked computing has transformed our world. In just the last year, Sony Pictures, Anthem health insurance, and the Office of Personnel Management each experienced significant cyber hacks. The victims included corporate and government entities, as well as millions of individuals who work for and with these enterprises. Public awareness of the harm caused by malicious cyber activity is growing, but not quickly enough to keep pace with the increasing dependence on cyberspace in our daily lives.

No single entity has all the necessary insight, authorities, capabilities, or resources to protect and defend U.S. and allied interests in cyberspace. Nor does anyone own a monopoly on good ideas. Improving security for all and achieving cyber resilience takes a broad and coordinated effort with unprecedented degrees of joint, interagency, coalition, and public-private sector collaboration. We need sustained interaction, exchanges of ideas, and regular exercises that bring the military and civilian cyber communities together across government, industry, and academia to share information, coordinate planning, exercise, and brainstorm together.

The U.S. military has made significant strides in developing digital capabilities, building cyber capacity, and integrating cyberspace operations into the joint force. The progress made to date could not have been achieved without the focus, energy, and persistence of our Soldiers, Sailors, Airmen, Marines, and Coast Guardsmen working side-by-side with their civilian counterparts. But there is much more to do. The necessary cyber workforce, defensible architecture, situational awareness, operational concepts, and enabling capabilities are not yet fully in place. Growing investment in tactical and strategic network defenses is essential, but we also need a shift in mindset and culture across the entire workforce. In short, we must appreciate how it is that we are all potential points of vulnerability.

The technological convergence that underpins our civil, commercial, government, and personal interactions poses a challenge for the security of military networks and the missions performed by the joint force. This convergence, combined with the actions of adversaries in cyberspace, presents novel and at times unique challenges that are stressing existing domestic and international legal frameworks. How, for instance, should we apply the Law of Armed Conflict in cyberspace? Our understanding of such new legal and policy challenges needs to evolve to account for this altered landscape. We need to generate options to narrow the gaps between federal and local government as well as civil, military, and commercial stakeholders in cyberspace. We must build the partnerships, develop structures and processes, and forge policies to close the seams that our adversaries exploit, while ensuring our actions comply with the Constitution and governing law.

We require ideas to guide us as we grow, develop, and maintain the Cyber Mission Force, and as we chart the cyber experiences and leadership qualities needed for the future joint force. The challenges of the cyber battlespace are distinct in some respects but not entirely unique. Specific certifications, highly technical training paths, continuous maintenance of skills, and rigorous operating parameters are familiar to most military communities. The talent pipelines and supporting tools and infrastructures, however, took time, commitment, and innovation to develop. In addition, the interlinking of skill sets between cyber warfare and industry practice creates new opportunities for building our nation's extended cyber enterprise. Sustained cross-pollination across the military, federal, and private sector cyber workforces will help those in industry understand national security threats and requirements, and allow our government workforce to learn from an entrepreneurial

culture that embraces innovation, risk-taking, agility, and speed to achieve mission impact in a rapidly changing technological landscape.

Operations in and from cyberspace are crucial to the future of the joint force. Regardless of mission, all joint force commanders need to understand their networks and how those networks affect the execution of their missions. With dedicated thought we can create an understandable joint concept for cyberspace, and also a lexicon, which will facilitate cyber planning and operations across the government, commercial, and civilian sectors, and translate technical concepts for non-technical audiences.

Cyberspace is a dynamic domain. It changes every time someone connects a networked device. The only certain feature of this environment is uncertainty. To address cyberspace challenges now and in the future, our nation needs a strong, national cyberspace posture built on a whole-of-nation effort. The ability to tap into our nation's intellectual capital will drive how our future unfolds. This is my challenge to you: contribute! Contribute through your work center, your command, and through submissions to scholarly journals. Contribute as mentors and in exercises and operational venues. Make your ideas heard, and help us shape our future.