Self-Development for Cyber Warriors

By Greg Conti, James Caroland, Thomas Cook and Howard Taylor

Journal Article | Nov 10 2011 - 12:04pm

Download the Full Article

From the battlefields of Iraq and Afghanistan, the inner ring of the Pentagon, and the Defense Industrial Base, to our home computers, mobile devices, and Facebook accounts, cyber warfare permeates virtually every aspect of our personal and professional lives. Once obscure groups like Wikileaks, Anonymous, and LulzSec and rarefied technologies such as the Stuxnet worm are now part of everyday discussions in classified military command centers as well as pubs and living rooms around the world. Rapid technological change, the low-cost asymmetric advantage afforded attackers, and the resultant clear and present danger to critical information systems have not gone unnoticed by military organizations, governments, educational institutions, and kids in the basement, some allied with the United States and some not. As a result, informed experts consider cyberspace an area of prime concern for the United States and a key warfighting domain alongside air, land, sea, and space.

As United States Cyber Command enters its second year, the military services are actively seeking to recruit, develop, and retain a world-class cyber workforce. Tailored education, training, and developmental experiences for the cyber domain, as well as an understanding of the knowledge, skills, and abilities required for planning, executing, supporting, and interfacing with cyber warfare operations are now beginning to emerge. However, unlike the mature career paths found in kinetic warfighting, the day when service members will benefit from decades of continuous experience and development in the cyber domain lies far into the future. Even as appropriate training and career paths come to fruition, the rapid rate of technological change demands active self-development and unit-level cyber professional development activities to remain current. Such outside the military classroom self-development must be embraced and encouraged by the military services who have to provide the requisite time and resources. At its core, the cyber warfare ethos must consider self-development a critically important activity, to do otherwise risks less than world class professionals and performance.

Today, most personnel are drawn from career fields with varying degrees of intersection with cyber warfare including: signals intelligence, all source intelligence, and telecommunications, as well as from the larger kinetic warfighting community. While this diversity brings much to the table, every donor group has its own blind spot - gaps in experience, education, and training that must be filled to provide a baseline of common understanding and operate most effectively in the cyberspace domain. This challenge isn’t new, military services have frequently faced the challenge of retraining personnel as they transition from one career specialty to another. In many ways, the birth of Cyber Command is as dramatic as the creation of the United States Air Force and similarly brings both the opportunity to create a powerful new culture and the challenge of transitioning many diverse personnel. Our goal with this article is to aid in such a transition by helping readers self-assess their own preparation, identify gaps in expertise, and provide techniques for filling knowledge gaps and facilitating currency through self-development.
activities. An important part of our discussion is the appropriate trade-off between depth and breadth of expertise across the many facets of cyber warfare.

While additional learning resources are available in classified environments, a solid foundation can be built upon on easily accessible and publicly available information and techniques. In addition, while this article is written to help the individual practitioner, many of our recommendations may be used to help create unit professional development programs and inform other more formal education and training activities. There are many important open questions surrounding the cyber workforce, such as the role of Officer, Warrant Officer, and Enlisted personnel as leaders or as technical experts. Other important questions consider the appropriate roles for DoD civilians and contractors. We do not attempt to answer these questions here and instead seek to provide a framework for professional development that can be appropriately tailored to an individual’s given circumstances and can adapt to future decisions regarding these and similar questions.

In this article, we use the terms cyber, cyber warrior and cyber workforce. Widely accepted definitions of these terms have yet to emerge. For purposes of this article, we define cyber broadly as Computer Network Attack (CNA), Computer Network Exploitation (CNE), Computer Network Defense (CND) and Global Information Grid (GIG) operations. We define a cyber warrior as someone who conducts, plans, or directly supports Computer Network Attack (CNA), Computer Network Exploitation (CNE), or Computer Network Defense (CND) operations. Cyber warriors form the larger cyber workforce which staff organizations that conduct CNA, CNE, and CND activities. For additional information on the attributes of a cyber warrior see our previous work.

A culture that respects and supports self-development is critically important to the cyber warfare profession, especially as we transition large numbers of diverse individuals into the cyber workforce. Historically, many military personal have had to develop their cyber warfare expertise despite the system, but we are seeing positive change occurring on a daily basis. The most immediate advantages to encouraging professional development are a more capable workforce, more effective operations, and more pleasurable working environments and culture. In addition, for those desiring to work in the cyber warfare domain, perhaps for the first time, working to develop the necessary knowledge, skills, and abilities provides other advantages. For example, by building a resume of experiences, individuals can demonstrate their desire, motivation, and expertise to the leaders, selection boards and human resources personnel that often serve as the gateways to cyber warfare assignments.

Download the Full Article

About the Authors

Greg Conti

LTC Gregory Conti is a 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 has served as an advisor in US Cyber Command Commander’s Action Group (CAG), as Officer in Charge of US Cyber Command’s Expeditionary Cyber Support Element in support of Operation Iraqi Freedom, and co-developed US Cyber Command’s Joint Advanced Cyber Warfare Course with CDR Caroland.
<table>
<thead>
<tr>
<th>Name</th>
<th>Bio</th>
</tr>
</thead>
<tbody>
<tr>
<td>James Caroland</td>
<td>CDR James Caroland is a Navy Information Warfare Officer, member of the US Cyber Command Commander’s Action Group, and an adjunct Associate Professor in University of Maryland University College’s Cybersecurity Program. He co-developed US Cyber Command’s Joint Advanced Cyber Warfare Course with LTC Conti.</td>
</tr>
<tr>
<td>Thomas Cook</td>
<td>COL Thomas Cook is an Armor Officer, Assistant Professor, and Senior Research Scientist at West Point. He holds a BS in History from Brockport State University, an MS in Industrial Engineering from the University of Louisville, and an MS in Computer Science and a PhD in Software Engineering from the Naval Postgraduate School.</td>
</tr>
<tr>
<td>Howard Taylor</td>
<td>Mr. Howard Taylor is West Point’s National Security Agency Fellow. He holds a BS from Brigham Young University and an MS from the Naval Postgraduate School. He spent 28 years on active duty in the US Navy, advancing through the ranks from Seaman Recruit to Commander. He then continued as a career NSA civilian where he managed complex interagency projects and systems for the US Intelligence Community.</td>
</tr>
</tbody>
</table>


Links:
6. [http://smallwarsjournal.com/comment/reply/11760#comment-form](http://smallwarsjournal.com/comment/reply/11760#comment-form)

Copyright © 2015, Small Wars Foundation.

Select uses allowed by Creative Commons BY-NC-SA 3.0 license per our [Terms of Use](http://smallwarsjournal.com/terms/). Please help us support the [Small Wars Community](http://smallwarsjournal.com/community/).