Department of Defense Cyber Workforce Challenges

Gregory Cox

The Challenge: "Everybody" knows that the demand for skilled cyber workers exceeds the supply, but "nobody" knows how to solve this dilemma. There is no evidence that an approach based only on expanding the workforce pool will lead to a satisfactory solution. However, before viable solutions can be meaningfully explored, we need to understand the cyber landscape.

It has proven impossible to determine the size of DoD's cyber workforce because it depends on who is "in" and who is "out" of that workforce.

The Cyber Landscape Has Poor Resolution

There is a consensus that cyber threats pose serious and growing challenges, but that consensus begins to evaporate over the dimensions of those challenges. In part, this is because the full extent of the cyberspace domain landscape is still debated—what is included and what is not? While it is natural to desire a bounded and crisp description of the landscape, sometimes that desire can lead to a narrow interpretation of the challenges. For example, the Defense Science Board (DSB), expanding on the Department of Defense's (DoD) formal definition of the cyberspace domain, offered its fairly broad interpretation (DoD Defense Science Board January 2013), (DoD Defense Science Board February 2017).

> *The term "cyber" is broadly used to address all digital automation used by the Department and its industrial base.* ***This includes weapons systems and their platforms; command, control, and communications systems; intelligence, surveillance, and reconnaissance systems; logistics and human resource systems; and mobile as well as fixed-infrastructure systems.*** *"Cyber" applies to, but is not limited to, "IT" and the "backbone network," and it includes any software or applications resident on or operating within any DoD system environment.*

Likewise, the interpretation of DoD's cyber workforce might be narrow or broad. Under DoD Directive 8140.01 (Cyberspace Workforce Management), the cyberspace workforce comprises four endeavors: (i) cyberspace effects, (ii) cybersecurity, (iii) cyberspace information technology, and (iv) cyberspace-related intelligence. However, if we adopt the DSB's interpretation of cyber, workforce members must perform duties that might not be viewed as falling into these bins, such as those to do with the cyber-related attributes associated with weapons systems and logistics systems.

This leads to an observation: it has proven impossible to determine the size of DoD's cyber workforce because it depends on who is "in" and who is "out" of that workforce. Despite this uncertainty, it is safe to say that DoD's cyber workforce size is currently over 100,000, and perhaps over 200,000.

The Cyber Mission Force: An Experiment in Progress

If we accept the premise that the current DoD cyber workforce exceeds 100,000, it is apparent that the Cyber Mission Force (CMF), with its 6,187 authorized billets spread among 133 individual teams, is a small fraction of that workforce.[1] Nonetheless, the CMF tends to become the focus of discussions about DoD's cyber capabilities, with many of those discussions about which teams have reached initial operational capability (IOC) and which have reached full operational capability (FOC) (Department of Defense April 2015).

A casual reader might be excused for believing that once a CMF team has reached FOC, it will continue to have full capability. That is not the case, however, because constant personnel rotations change the teams' *readiness*. Fortunately, there is growing recognition that readiness, rather than IOC/FOC status, is a more-appropriate team attribute; unfortunately, however, readiness is still largely measured in terms of on-hand personnel, currency of personnel training, and equipment condition, which are essentially the same metrics used to establish IOC/FOC status.

Cyclical readiness is a fact of life for many military units (e.g., Army Brigade Combat Teams) as they undergo readiness ups and downs in their cyclical prepare-deploy-reset processes. However, IDA has found no evidence of plans to manage the inevitable cyclical readiness of the CMF, but rather an implicit assumption that all teams are ready all of the time. But unless there are sufficient redundancies to compensate for personnel turnover—a significant workforce impact—we should expect to see ups and downs in CMF team readiness.

Workforce for the Entire Cyber Landscape, and Beyond

In his recent book, Bruce Schneier writes about computers in a broad sense. (Schneier 2015) Although his characterization is hyperbolic, it nonetheless speaks to a largely unappreciated facet:

> *Your phone is a computer that makes calls. Your car is a computer with wheels and an engine. Your oven is a computer that bakes lasagnas. Your camera is a computer that takes pictures.*

[1] The five types of CMF teams are Cyber Protection Teams (68), Combat Mission Teams (27), Combat Support Teams (17), National Mission Teams (13), and National Support Teams (8). Additional teams beyond these are currently being created from Army Reserve Units.

Schneier is not alone; Joshua Marcuse, Executive Director of the Defense Innovation Board, describes the F-35 this way (Marcuse n.d.).

> *The F-35 is not a plane with a supercomputer onboard; it is a supercomputer with wings.*

Indeed, we might go one step further and say that the F-35, with its multiple sophisticated sensors and requisite data fusion, is a *networked* supercomputer with wings. This implies that a prominent capability for the F-35 resides in the cyberspace domain and leverages the air domain, even though this clashes with the general characterization of this aircraft as operating in the air domain and leveraging the cyberspace domain. This observation is not unique to the F-35; we could talk about many (or most) modern weapon systems (e.g., Navy ships) or concepts this way. None of these weapon systems are immune to cyber threats, and thus there are cyber workforce implications for them.

Source:https://www.defense.gov/News/Article/Article/1218741/us-showcases-f-35-lightning-ii-aircraft-at-paris-air-show/,

This highlights a fundamental problem with the cyber workforce. The workforce will not—because it cannot—scale proportionately to the (growing) challenges. Although initiatives to enlarge and strengthen the workforce are important and helpful, DoD may not succeed in balancing workforce supply with demand by seeking more talent. It is time to start thinking outside the proverbial box.

First, a root cause of cyber vulnerabilities in weapon systems is that their relevant requirements were developed at a time (many years ago) when our understanding of the cyber landscape was less mature. (This assertion will also apply 10 years from now.) This demands a different mindset in the systems engineering process for weapon systems. In his book on security engineering, Ross Anderson observes that traditional system engineers deal only with error and mischance rather than malice. (Anderson 2008) Automobile manufacturers (who rely on profits) have come to accept responsibility for the "malice factor" after some highly publicized events, such as the *Jeep Cherokee* hack. (After Jeep Hack 2015) Why shouldn't major defense contractors (who also rely on profits) be held to similar standards?

Workforce solutions may also come from automation, which can help especially with challenges that are too fast, boring, or expensive for people to handle manually. As Dan Geer eloquently predicts: "The skills shortage in cyber security will not be solved. Governmental sectors will remain unable to retain those they have nurtured. The enterprises able to pay any price for talent will get all or most of that talent. Algorithms will therefore be deployed to do what we ourselves cannot do, which is to protect us from other algorithms." (Geer 2017)

However, as Geer is careful to articulate, caution is the watchword. There can be a steep (perhaps irreversible) downside to algorithmic automation as cyber challenges become more demanding in both scope and sophistication. Thus, we see potential use of pattern recognition and preprogrammed responses for cyber defense and intelligence as an aid to human operators, but we remain wary of visions with automation as "the workforce solution."

Finally, lest we think too narrowly about the many cyber workforce challenges, what about broader information operations and electronic warfare? There is some recognition that these are not cleanly separated from "cyber." In this sense, even the broad DSB interpretation of cyber may be too narrow. Indeed, with hindsight it may prove that DoD should have declared the "information domain" as the fifth warfighting domain instead of the cyberspace domain. But regardless of whether cyber and broader information elements are formally merged, they will compete for many of the same skilled workers. In an area where worker talent is in short supply, there is a compelling case for eliminating duplication and pooling workforce resources to the largest extent possible.

References

2015. "After Jeep Hack, Chrysler Recalls 1.4M Vehicles for Bug Fix." *Wired*. https://www.wired.com/2015/07/jeep-hack-chrysler-recalls-1-4m-vehicles-bug-fix/.

Anderson, Ross. 2008. *Security Engineering*. 2nd. Wiley Publishing Company.

Department of Defense. 2015. *The Department of Defense Cyber Strategy*. April.

Department of Defense Defense Defense Science Board. 2013. *Resilient Military Systems and the Advanced Cyber Threat*. January.

Department of Defense Defense Science Board. 2017. *Defense Science Board Task Force on Cyber Deterrence*. February.

Geer, Dan. 2017. *Keynote speech to SOURCE*). Boston, April 27. http://geer.tinho.net/geer.source.27iv17.txt.

Marcuse, Joshua. n.d. https://www.youtube.com/watch?v=eatGvBU18MU.

Schneier, Bruce. 2015. *Data and Goliath*. W.W. Norton and Company.

Dr. Gregory Cox is a Research Staff Member in IDA's Information Technology and Systems Division. He holds a Doctor of Philosophy in mathematics from Auburn University.