Information & Security

A. Brill & J. Fairtlough
vol. 44 (2020): 9-15
https://doi.org/10.11610/isij.4401

Published since 1998

ISSN 0861-5160 (print), ISSN 1314-2119 (online)

Research Article

Fighting the First Battle of Cyberspace Preparedness: Finding Your Reserve Cyber-Warriors

Alan Brill (✉), ***Jonathan Fairtlough***

Kroll Cyber Risk, Secaucus and Los Angeles offices, USA
https://www.kroll.com/en/services/cyber-risk

ABSTRACT:

One of the key resources needed for a nation-state or its military organizations to successfully operate in the cyberspace domain of operations is qualified people. But this is a resource that is universally recognized to be in very short supply. The military competes with other governmental entities and with a private sector that holds qualified cyber security and cyber operations professionals in high regard and which can offer salaries and benefits beyond those that can be offered by most governments. One of the unique potentials that military organizations can consider is supplementing its active-duty and full-time civilian cyber warriors with a reserve component. Virtually all non-cyber military organizations have successfully developed the capability to supplement active duty personnel with reservists. The cyber domain offers the potential to do the same, but also to think innovatively to compete for the limited supply of qualified personnel. This article examines some outside-the-box concepts for building and maintaining a cyber-force reserve component.

ARTICLE INFO:

RECEIVED: 09 Nov 2018
REVISED: 10 Feb 2019
ONLINE: 28 FEB 2019

KEYWORDS:

reservists, recruiting, retention, innovation, cyberwar, cyber operations

✉ Corresponding Author: Tel.: + 1 201 319 8026; E-mail: abrill@kroll.com

Introduction

The NATO Alliance and its member countries are fighting the first battle in the war to be able to respond to the changes and challenges of raised by cyberspace in warfighting and defense.

The Alliance and every member state understand that cyberspace is not just a conceptual domain – it is a very real, active front. Both defensive and offensive cyber-operations are vital missions for every nation and military service. We must defend our existing military and civilian technological infrastructure against adversaries. We must be capable of identifying and protecting strategic technologies and media. We have to be prepared to either respond to attacks with counterattacks, or where appropriate, to initiate offensive cyber operations. Cyber operations may be in support of traditional military operations, or they may stand alone.

The operational shift raised by cyber space has added yet another dimension to warfighting, one that is still being understood by traditional military planning. The natural focus of technology, as both a target and a tool, can lead to an operational oversight – both defensive and offensive cyber-operations are dependent on the same thing: Having the right number of cyber-operators with the right skills at the right times and in the right spots.

The skills that military and government agencies require to operate successfully in cyberspace are in short supply, and there is substantial competition for those with the skills with a private sector that can pay more than the military. The private sector can reward cyber-operators and cyber-security personnel with additional payments through stock options or stock grants which can be worth a substantial amount. They offer a lifestyle that does not require periodic deployments to war zones, that do not subject employees to annual physical fitness tests where failure can lead to termination of the employment relationship, and that do not require the usual relocations, family hardships and separations that are part of a military career.

Can We Divide the Needed Work between an Active-Duty Cyber-Force and a Cyber-Reserve?

There are tasks that need to be accomplished on-site in a theatre of operations. Chain-of-custody and data acquisition (for example, imaging a computer to a file in a forensically-appropriate format) would generally be done in or near the field (although sometimes equipment can be brought back to the homeland for analysis). Working in a military field environment would be carried out by active-duty or deployed "traditional" reserve members. But virtually all analysis can be done remotely (assuming a device is operational enough for the drives to come to the "ready" state. If not, data recovery (which might need a clean room) is needed, and that might be in the homeland.

The concept of dividing tasks between active and reserve units is not unique to cyber. Indeed, virtually every military does this. In the US, reserve and National Guard forces are often called on to assist in natural disasters like floods

or hurricanes. In Norway, the Home Guard (*Heimevernet)* focuses on local defense and civil support. In a sense, this is triage, identifying those operations best performed by professional active duty forces and those that can be successfully performed by trained and qualified reservists.

Within cyber, there is also both the need and the ability to prioritize tasks. Cyber defense of military systems requires full-time monitoring and action, as the velocity of cyber-attacks cannot wait for the call-up of reservists. Indeed, the velocity is such that it seems inevitable that the first line warrior for network defense will be computer programs that can act more or less autonomously to block threats and interdict exfiltration of data. However, the expansion of the target field to include not just national technology infrastructure, but all forms of media and communication, further stresses the traditional model of deployment.

Instead, military operations in cyber space need to follow the triage model. Tasks like computer forensics, cyber-investigations, systems monitoring and incident response lend themselves to triage. There is the capability to triage tasks to be performed to include the availability of various forms of reserve personnel, and to leverage existing network interoperability to allow for the movement of data/evidence to a triage point.

Given the shortage of personnel qualified to perform this work, and the competition from the private sector, the recruitment and maintenance of a cyber-reserve force requires that national military services think creatively and not be limited by traditional military thinking.

Can We Define A Cyber-Reserve that Provides Opportunities that Are not Available in the Active Force?

Every cyber-military service has to do a work analysis. What tasks are the technicians required to do? What proportion of the workload is classified, and at what levels of classification? What tools are used, and what programming skills are needed? For example, what does a specific military cyber-service use for carrying out forensic examinations of Windows-based devices? Do they use X-Ways, Encase, Forensic Took Kit (FTK) or other commercially licensed packages? Do they use open-source forensic tools (like the Eric Zimmerman Toolset)? Once the work to be done is actually understood, it is possible to think outside the box for how to get it done, and to develop an incident triage and assignment matrix.

For example, some work may be able to be defined as a unique task. What if the military cyber organization obtained 10 forensic images of computers in a standard format (such as the Encase “E01” format) and needed a specific set of analyses to be run on each of them. Could this be offered to cyber-reservists using models developed for the so called “gig economy”? (For example, the platforms that ride-sharing services like Uber or Lyft or Didi Chuxing, or the distributed task model operated as “Amazon Mechanical Turk” that brings to-

gether online tasks (such as transcription of recordings) and people qualified to do the work.)

Qualified cyber-reservists could be provided with access to a secure website or app which would list currently available tasks (for example, doing the forensic examination of those 10 computer images) and reservists could respond that they wanted to do them. We anticipate that most if not all tasks would have a deadline, so it might be appropriate to have a capability for a cyber-worker to respond that they could, as an example, do the analysis of 6 of the 10 machines within the deadline. Another worker could then accept the task for the other four work units.

This kind of mechanism has the advantage of permitting a decentralized workforce (including those who have physical or medical issues that limit their travel) to get the work done. It uses the structure of triage, since the cyber-force operating the system can set priorities, determine deadlines, and can code the work-opportunities to display them to specific subsets of the reserve-worker population (because displaying the opportunity to someone without the specific qualification to do the work is inefficient.)

The gig model can even be extended using the concept of a pre-qualified "commercial cyber-reserve" in which commercial vendors can be given access to the gig system and offered specific tasks (presumably not "claimed" by a reservist) in return for a specific payment. It is likely that there will be a correlation between amount offered and the likelihood that a commercial vendor will claim it. So, it might be necessary to adjust offered payments based on priorities and deadlines.

Can We Recruit People with the Right Skills that Would Never Qualify for Membership in a Traditional Military Reserve Organization?

Members of reserve military services must generally meet fitness criteria that are often identical to those of the nation's active military force. This can include guidelines on height, weight, age, body mass index (BMI) as well as eyesight, hearing and physical strength (measured through physical training tests involving running, pull/push-ups and other exercises measured through time or required repetitions. Most military members—even those recruited for direct commissioning as lawyers or physicians—are required to undergo some form of field training and weapons familiarization (or required qualification.)

An active military will generally be unable to compete on salary and benefits for active duty or reserve soldiers in the world of qualified cyber-security and cyber-operators. This is often true even for civilian members of a cyber-operations force.

What is needed is vetted, trained people who can do the job. Deployment is no longer an operational requirement, as many—perhaps most—cyber operations are actually location-independent. Given this operational reality, do the physical criteria that we traditionally use to select service members make sense?

Take the case of a cyber-security person or forensic examiner who is fully qualified to carry out the work that the cyber-force needs, but who is confined to a wheelchair. Or who has another physical handicap or limitation that makes them ineligible for military service, but which does not interfere with their ability to carry out cyber-force tasks. Why cannot we recruit those people? Their patriotism is unquestioned, but they have never been given the opportunity to serve.

Similarly, targeting skilled operators who due to family and existing employment cannot deploy, but can hold a responsible position at a center near where they live or work from their homes, just as they do in the private sector.

Also, cyber-qualified persons, considered physically to be too old to be recruited. They may have 20 or more years of experience in cyber-operations or forensics (and could be trained for the specific tasks required.) They may have retired from the military or from law enforcement cyber-operations or forensic labs. There are entire classes of tasks that they could undertake, if provided the opportunity to do so.

There is still a requirement for appropriate security clearances, and the people have to be able to handle classified information as required for its protection. Technology can help. Where in the past, to do a forensic analysis of a computer required having physical access to the machine to be examined (or to a forensic copy of the machine) that is frequently no longer required. The computer image files can be securely stored on a network device which can be remotely operated by a technician. They can carry out tasks from virtually anywhere. The technician can be provided with access to a virtual computer which accesses both the device image and the software needed to carry out the work.

Can Reserve Cyber Warriors Provide Support Beyond Carrying Out Cyber-Defense and Cyber-Offense Tasks?

In many walks of life, people say things like "if only I had someone like him (or her) available…" The military is no different. There is nothing wrong with this thinking. The problem comes in when it is simply wishful thinking and does not continue on to considering what to do about it. Outside-the-box cyber reserve models provide such an opportunity. Consider the following potentials.

Can We Take Advantage of the Desire of Organizations to Help?

In addition to individuals, organizations often have a motivation to enable employees to be part of military reserve forces. In the U.S. for example, the program known as "Employer Support of the Guard and Reserve" encourages companies to support those participating in military reserve activities. Similar programs exist in other countries.

Additionally, many organizations have a tradition of supporting *pro bono publico* policies in which employees are permitted to do a certain amount of work, without charge, where that work constitutes a public good. Through these pro-

grams, personnel with the skills needed to participate in cyber-reserve activities could receive the encouragement of their firms to perform tasks in support of their nation's cyber-force efforts.

Can We Make Use of Potential Cyber-Reservist Skills in Nontraditional Ways?

In addition to the immediate skills we may think of, e.g. carrying out aspects of cyber-operations, there are other ways of making use of the skills of non-traditional cyber reserve members. For example, they could be tasked with testing potential new forensic tools to assure that they operate properly. They could be tasked with developing and delivering training to members of the active and traditional reserve forces on subjects in which they have specialized knowledge. They can provide quality control reviews, report reviews and other tasks that need to be done, but which may not be a priority for the active or traditional reserve force members.

Conclusion

We should consider whether our current models of military reserve (and supporting civilian service) make sense in the cyber realm. Can we draw on those who cannot join a traditionally defined military organization or those whose personal or family situations do not permit deployments? Can we recruit working cyber-professionals who want to help, but who cannot serve as a full-time reservist? Why cannot we use them as workers in a cyber-gig environment? Can we use them as instructors to raise the skill levels of the active and reserve cyber-forces? Can they serve on advisory panels to assist the senior managers of the cyber force?

Traditional thinking is not going to provide the cyber-workforce that we need to function in a 21-st century cyber-defense or cyber-warfighting domain. With the examples in this article in mind, we encourage thinking about outside-the-box solutions.

Acknowledgements

The authors wish to thank Kroll Cyber Security & Investigations for giving them the time and resources to prepare this paper, and for Prof. Brill to participate in the conference in Sofia, Bulgaria.

About the Authors

Alan **Brill** is Senior Managing Director at Kroll Cyber Security and Investigations. He is a Fellow of the American Academy of Forensic Sciences, and a founding member of the Section on Digital and Multimedia Sciences. An internationally recognized speaker on cyber-security, he served as a Major in the US Army Reserve, and is a graduate of both the US Army Command & General Staff College and the Eisenhower School of the National Defense University. He is an instructor in the Terrorist Use of Cyberspace course at the Center of Excellence – Defense Against Terrorism, and is an Adjunct Professor at the Texas A&M University School of Law. https://orcid.org/0000-0001-8761-9153

Jonathan **Fairtlough** is Managing Director at Kroll Cyber Security and Investigations. A former Los Angeles county prosecutor who specialized in high tech criminal investigations, Mr Fairtlough is an active incident response leader for Kroll. He is an active instructor at the United States Department of Homeland Security's National Computer Forensic Institute.