Selecting Qualified Airmen for the Cyber Mission Force

The Pitfalls of Hiring Operational "Analysts"

Maj David J. Ortiz, USAFR

Disclaimer: The views and opinions expressed or implied in the Journal are those of the authors and should not be construed as carrying the official sanction of the Department of Defense, Air Force, Air Education and Training Command, Air University, or other agencies or departments of the US government. This article may be reproduced in whole or in part without permission. If it is reproduced, the *Air and Space Power Journal* requests a courtesy line.

```
1 packets transmitted, 1 received, 0% packet loss,
rtt min/avg/max/mdev = 540.528/540.528/540.528/0.000
[root@localhost ~]# pwd
/root
[root@localhost ~]# cd /var
[root@localhost var]# ls -la
total 72
drwxr-xr-x. 18 root root 4096 Jul 30 22:43 .
drwxr-xr-x. 23 root root 4096 Sep 14 20:42 ..
drwxr-xr-x.  2 root root 4096 May 14 00:15 account
drwxr-xr-x. 11 root root 4096 Jul 31 22:26 cache
drwxr-xr-x.  3 root root 4096 May 18 16:03 db
drwxr-xr-x.  3 root root 4096 May 18 16:03 empty
drwxr-xr-x.  2 root root 4096 May 18 16:03 games
drwxrwx--T.  2 root gdm  4096 Jun  2 18:39 gdm
drwxr-xr-x. 38 root root 4096 May 18 16:03 lib
drwxr-xr-x.  2 root root 4096 May 18 16:03 local
lrwxrwxrwx.  1 root root   11 May 14 00:12 lock ->
drwxr-xr-x. 14 root root 4096 Sep 14 20:42 log
lrwxrwxrwx.  1 root root   10 Jul 30 22:43 mail -> sp
drwxr-xr-x.  2 root root 4096 May 18 16:03 nis
drwxr-xr-x.  2 root root 4096 May 18 16:03 opt
drwxr-xr-x.  2 root root 4096 May 18 16:03 preserve
drwxr-xr-x.  2 root root 4096 Jul  1 22:11 report
lrwxrwxrwx.  1 root root    6 May 14 00:12 run ->
drwxr-xr-x. 14 root root 4096 May 18 16:03 spool
drwxrwxrwt.  4 root root 4096 Sep 12 23:50 tmp
```

Setting the Stage

The Air Force, like each service, is charged with providing cyber operations and intelligence professionals for the Cyber Mission Force (CMF) being built by US Cyber Command over the last four years. The CMF build-plan calls for dozens of teams serving in offensive, defensive, and supporting roles. Inside the CMF, the combat mission teams are aligned to the combatant commands to serve the offensive cyber needs of the combatant commanders. US Cyber Command manages over a dozen national mission teams aligned to conduct a defend-the-nation mission called the Cyber National Mission Force. Both the combat mission teams and the national mission teams also have support teams assigned to help with development and analysis. Finally, a large number of Red Team–like units called cyber protection teams are under operational control of the combatant commands and the Cyber National Mission Force for defensive purposes. Most of these teams are trained inside the National Security Agency (NSA) under its rules and high standards, using its capabilities.

From the NSA's birth, military intelligence, communications, and scientific units have provided personnel to supplement offices in support of the collection of signals intelligence and the requirements of information assurance. Over the past decade, the services—in varying forms—have also established cyber-focused units to supply qualified personnel to various cyber missions within the NSA. Thus, when the CMF began in 2012, needing over 60 people apiece to serve in national mission teams or combat mission teams, many of these service members found themselves realigned to a cyber team of one stripe or another. At the time, no ready source of individuals existed to meet the substantial manning needs of the new CMF, so converting the majority of service-billeted people and service civilians already embedded in the NSA made good sense.

After the in-place turnovers, the functional managers within the services faced the difficult prospect of hiring en masse a workforce of cyber professionals. It must have been hard for them to divine exactly what the CMF needed for obscure work roles that didn't exactly translate into many mapped military career paths. There were some exceptions because some services created career-code "shred-outs" (i.e., "markers" to track skills or experience) to specifically align people to the NSA's cyber work roles.

In the past, finding a handful of qualified service members per squadron or company for the NSA who possessed unique technical skills was totally feasible with the flexibility given to local training managers and superintendents. However, the CMF has dozens of sizeable teams, so the demand for these low-density, high-demand cyber, development, and intelligence skills went through the roof over the last four years. Whereas previously a unit may have been asked to provide only a handful of qualified service members, now it eventually had to supply dozens. (Furthermore, they will be permanently changing station every two-to-three years, so a dedicated pipeline will be necessary.) When the integration numbers within the NSA were lower, units had the luxury of farming out resumes and sending Airmen, Soldiers, and Marines to interview within the agency to find the right office. The advent of the CMF limited that freedom of placement because the teams had to meet readiness requirements set down in their manning layouts, which could not be altered (i.e., each team must be built exactly the same way). This inflexibility further increased throughput to specific NSA offices and now from specific military career codes. Consequently, how does the Air Force cope with these challenges and serve the needs of the CMF mandate to produce qualified cyber professionals?

The Air Force and possibly other services may be exacerbating the difficulty of finding a greater quantity of qualified applicants for some CMF/NSA work roles by self-imposing self-limiting rules based on career codes (Air Force specialty codes [AFSC], military occupational specialties, and others). Since the need for qualified cyber Airmen is high and not likely to change anytime soon, this article recommends a few reasonable steps to better position our beloved Air Force and the other services to meet readiness requirements through more flexible applicant searches, skill tracking, and a reexamination of what it means to be "operational" in cyber.

Background: Why Should We Listen to You?

Where you stand often has much to do with where you sit. In the interests of full disclosure, most of the work week I am an NSA deputy division chief, leading an operational cyber force of awesome civilians, contractors, and military personnel. Integrated into my division are more than a dozen CMF teams with all the US Cyber Command people I could ever want. My alter ego is the Reserve assistant director of operations for a cyber operations squadron whose job it is to supply interactive operators (ION) right back to my own NSA mission space and other offices. Therefore, I believe I am in a unique position to experience both sides of the problem and can see some already viable solutions that the Air Force and other services should consider to improve exploitation analyst (EA) throughput specifically. (Note that some of the lessons learned could be applied to other work roles in the CMF as well.)

Inside my civilian mission space, we integrate two types of CMF- and NSA-recognized work roles: EAs and IONs. From an operational perspective, they are two peas in a pod, working together daily conducting cyber missions—not exactly "pilot and navigator" or "Maverick and Goose," but for the purposes of this discussion, these analogies are useful.

As a reservist, I help my squadron supply quality ION trainees to attend a long, structured NSA pipeline that lasts anywhere from 18 to 24 months. It's a demanding program that begins with passing a standardized test and a personal interview after completion of initial training. The pass rate in this complex cyber training course was slightly less than 60 percent over the last year (civilian and military), but, thankfully, our squadron has had about a 100 percent pass rate among its students.[1]

My division hires, trains, and certifies EAs to work in the same cyber mission space as our IONs. Think of EAs as cyber (sniper spotters) and mission planners for the IONs since they work hand-in-hand on the same complex operations. The training program for EAs is about six to nine months long (depending on class dates) and is similarly demanding. The work role requires many of the same skills but asks the EA to accomplish different tasks. To begin EA training, applicants go through a resume review and a technical interview. The pass rate for the interview process was not high among our Air Force applicants over the last year, running at a very dismal 12 percent.[2] Granted, even for civilians with university degrees, the pass rate is not 100 percent.[3] Therefore, it is problematic just to get EA trainees in the door, much less through the six-to-nine-month training program. The good news is that, as a whole (civilian or military), the pass rate for the EAs who enter the program is around 90 percent.[4]

An obvious question would be, "Why is the Air Force having great success staffing IONs but struggling with getting Airmen into the EA pipeline on exactly the same cyber operational team?" Imagine the problem this way: would it be acceptable for an Air Force training squadron prepping a pilot and navigator team to fly an airframe to have a 100 percent pass rate for the pilots but just a 12 percent rate of acceptance for the navigator pipeline (to say nothing of their pass rate once they enter the program)? Probably not—so is the Air Force somehow identifying the right Airmen to fill ION positions yet looking in the wrong direction for EAs? My theory is that it may have to do with the *analyst* part of the "exploitation analyst" name and the perceived skills associated with that title.

An Analyst Is an Analyst Is an Analyst . . . until He or She Is Not

In the military, the words *operator* and *analyst* evoke very real, distinct impressions. In the Air Force, the *analyst* conjures scenes of Airmen diligently typing on a keyboard and working through tough scientific or intelligence problems. Perhaps these analysts are also drafting air campaign plans or collection requirements. Regardless of the task, most people would agree that an "analyst" is not executing an "operational" mission on a daily basis—just a rough estimation. (Clearly, there are exceptions for Airmen serving on various airframes who are intel folks.)

On the other hand, the term *operator* easily brings to mind the flying or space world—Airmen on stick, loadmasters, boom operators, pararescuers, combat controllers, or Airmen serving on missile crews. Although many of us may not work in these "operational" career fields, it is easy to envision the Airmen in them flying, employing weapons systems, or serving on security details. The line between analysis and operations is easy to grasp. Unfortunately, in the cyber "operational world," that line is not so easily visible because of the way operations are conducted and the way many people are involved on a single operation. Even worse is trying to draw these lines based on AFSCs and military occupational specialties, which is counterproductive and might make it harder for the Air Force and other services to find qualified cyber professionals.

Current Alignment of Air Force Specialty Codes

To further explore the AFSC problem, we have to look at how the Air Force fills ION and EA billets across the CMF and NSA right now.

Interactive operators. In light of the fact that the term *operator* is in the ION work-role title, Twenty-Fourth Air Force fielded cyber operations squadrons (formally network warfare squadrons) to provide qualified Airmen to train at the NSA for complex cyber operational jobs. Undoubtedly, the agency and the CMF are looking for cyber-ready individuals whose A-school prepped them for this type of training pipeline. For the Air Force, that is Undergraduate Cyber Training (UCT). The AFSCs, such as 17Ds, 17Ss, and 1B4s, awarded after UCT and follow-on training denote Airmen destined for cyber operations. These professionals would largely go on to work in positions like base communications, cyber operations, or network defense, to name a few. UCT's stated focus is to prepare Airmen to establish, secure, operate, assess, and actively defend multiple types of networks, including command and control systems, Internet, telephony, satellite, and mobile telecommunications, among others.[5] An operationally minded course ensures that Airmen understand they are prepping to fight and win in another military domain. When Airmen graduate from UCT, the best of them continue to take supplemental cyber warfare officer training, with the best of this school usually selected to take the NSA's difficult ION entrance exam. Those who pass are usually slotted for a 300-series squadron such as the 315th or 390th Cyber Operations Squadron and then come to Fort Meade, Maryland, to prep for their training. In the 315th, potential IONs are interviewed and further screened when they arrive, just to make sure they are technically ready for the long training pipeline. It is no wonder that the Air Force has an admirable pass rate, producing some of the best operators serving in the CMF and the agency.

Exploitation analysts. As exploitation "analysts," these Airmen are staffed by Twenty-Fifth Air Force under an intelligence function. Units like the 16th and 41st Intelligence Squadrons receive intelligence officers and enlisted service members who have likely gone through the JCAC (Joint Cyber Analysis Course) in Pensacola, Florida, and are then slotted against EA positions on the CMF that the squadrons support. The JCAC is designed to give personnel with minimal computer skills a wide range of cyber and analytical instruction over six months.[6] The goal is to prepare them to conduct technical network analysis in support of computer network operations effects and national intelligence requirements. When potential EAs arrive at their squadrons, many of them enter the US Cyber Command / J7 pipeline—an amalgamation of NSA, industry, and military training programs designed to prepare a person for the EA role. Unfortunately, this path is not working as well for our Airmen as the one above for the IONs even though they both need to perform at the same operations station and support each other to conduct the same mission. How, then, is the Air Force succeeding extremely well with one work role yet struggling with the other?

Work-Role Requirements

From the training statistics, the Air Force seems to have cracked the code in finding Airmen to become successful IONs. Twenty-Fourth Air Force understands the requirements and has a training program that readies Airmen for the world of cyber operations. The Twenty-Fourth knows that its mission is to prep cyber Airmen for an operational war-fighting role.[7] I fear, however, that a mismatch exists somewhere for EAs when people see the word *analyst* and then collectively pivot to intelligence units and AFSCs to fill the bill. Unfortunately, for a job like EA, intelligence analysts are not what the NSA is looking for to populate its training program. The EA position is a cyber-operations job, regardless of its name, because that is what EAs do with IONs—conduct operations. EAs are at the nexus between cyber intelligence analyses, requirements, effects-based planning, cryptology, cyber operations, cyber development, and operations security. Threading that line demands a deep knowledge of the cyber world, not just a concentration on either network analysis or reporting.

What is the National Security Agency looking for in an exploitation analyst? Many of the daily work-role functions of an EA are classified, but the way the NSA hires civilian EAs or interviews military applicants is entirely unclassified. Below are the five major knowledge categories that hiring managers look for in an EA applicant.[8] The first screen is a resume review, and the second is an in-person interview to assess critical thinking, problem solving, teamwork, collaboration, professional development, and the applicant's currency in technology, the last of which is very important in cyber.

- Programming Concepts /Application Development
  - Secure code or other exploitation concepts
  - Scripting
  - Programming languages
- Operating System Fundamentals—Windows/Linux
  - Command-line concepts
  - Key file locations
  - System configuration and running state
  - Client/server concepts
- Networking Fundamentals
  - Open systems interconnection concepts
  - Routing/switching
  - Subnetting
  - Network services
- Network Security Architecture
  - Segmentation
  - Firewalls
  - Virtual private networks
  - Proxies/guards
- Computer Network Defense
  - Penetration testing
  - Vulnerability assessment
  - Intrusion detection and network forensics
  - Incident response and host forensics
  - Malware analysis

What's in a work role? This list makes it much easier to see why a technical mismatch exists at the EA desk within the intelligence squadrons. For example, the NSA's EA technical interviewers are not looking for traditional intelligence analysis skills like reporting and all-source analysis. Instead, they want to see a decent concentration in three of the five technical categories listed above, such as network administration, programming, or malware analysis. EA applicants don't have to be experts in each, but they should have some background in most of the subjects and, hopefully, thorough knowledge of a few. The division's hiring managers regularly remind the CMF and other partners that the EA work role is not a place to learn basic computer and networking skills. Rather, it's a position to enhance and apply already good cyber skills for a difficult mission. This is not just their opinion. In fact, the NSA considers the EA work role to lie within the *networking and telecommunications* skill community, not as it happens within the *intelligence analysis* skill community.[9] Naturally, the ION work role is also within the *networking and telecommunications* skill community.[10]

Unfortunately, the Air Force's manning model is asking an intelligence analyst to do a very "cyber" job. The JCAC, the class that many intelligence personnel attend for cyber analysis instruction, is not exactly paying the bill for this specific work role regularly. Intelligence professionals with AFSCs like 1N4 and 14N, as well as other AFSCs who are not cyber-focused, usually don't pass the interview or complete the training. Although the division has had successful intelligence professionals from JCAC, they have mostly come with cyber skills of their own via a personal hobby, additional schooling, college courses, or self-paced study in cyber.[11] Other factors can contribute to lower pass rates as well in this population. For example, the length of time between the JCAC and a CMF position could take six months to a year as they wait for a clearance. This makes it hard for some people to recall key technical details from the JCAC or other schools during an interview if they don't have an innate interest in cyber as a hobby. The secret for our successful career intel-trained applicants and other noncyber AFSCs is that they are already interested in networks, hacking, malware analysis, and digital forensics anyway, so they are keeping current all by themselves.[12] *We call them keepers*.

From the point of view of our civilian hiring managers, they are confounded as to why the Air Force sees the EA work role as an "intelligence analyst" job because it has always been a cyber job to them. Then again, our civilians don't have the military background to cloud their interpretation of the term *exploitation analyst* either. The division's hiring managers only care about the critical functions within the work role that need to be done. For example, EAs conduct the lead-up cyber-target development and preoperations analysis, draft operational plans, guide operations that IONs conducted on-keyboard, help keep operations safe, and conduct postoperations analysis. Airmen can roughly equate the EA to a navigator on a spice freighter, but the work has more of a mission-management focus to it as well—similar to a mission commander on an Airborne Warning and Control System crew who shares mission-execution responsibilities with the pilot. One can't effectively get the job done without the other. EAs are target-subject-matter experts, knowing all there is to know about a target. They are responsible for ensuring that the operational team secures national intelligence or prepares to support the commander's intent. Frankly, with these responsibilities comes the need for a wide variety of cyber skills not necessarily related to either intelligence analysis or reporting, which are traditional core functions of intelligence analysts.

Applicants

Successful Applicants

At this point, readers could point out that many 1N4s, 14Ns, and 1N2s have passed the EA interview and are succeeding in their positions. That is true, of course. The fact that our division employs skilled intelligence analysts as EAs supports that argument. What, though, are the common threads that have led to their success?

Experience matters. In the initial days of the Cyber National Mission Force, many EA slots were billeted from Airmen already EA-qualified or from the best cyber analysts scattered among the all-source-analysis community at the NSA. These individuals were E-5s and above with a tour or two in network analysis shops, Red Teams, or Blue Teams—or they were network administrators who were good enough after their interview to walk in the door outright. To acquire that baseline knowledge, some took on work roles in their shops that were more cyber focused than perhaps advertised, and others sought out mostly cyber shops that wouldn't usually be offered to their AFSC in the greater Air Force. That can happen in the NSA because a civilian office may not care what someone's AFSC is—only that he or she can do the job or be willing to learn the skills for the work role. Finally, some IONs also came over to the EA work role with their cyber skills and shine brightly. Intelligence folks have also succeeded as IONs.

Interest. The most successful analysts (enlisted, officer, civilian, or contractor) are at-home cyber enthusiasts.[13] Just for fun, these applicants like to create networks of their own to study at home. Some have created "honeypots," used to attract hackers and capture malware on the Internet, and stand-alone networks called "sandboxes" to analyze malware they find. They monitor their inbound and outbound connections with netstat and similar network utility tools to learn more about their craft. Others still are practicing with openly available network security testing tools like Backtrack (legally, of course) on their own closed networks. Some of these career intelligence Airmen in the division are also working on their computer science degrees, and that foundational academic knowledge helps out a great deal with the interview and EA training.[14] Whether they began as intelligence analysts or weeds-and-seeds workers, these are the Airmen we want!

Dedication. I don't have to tell these types of Airmen to keep up with current technology or get trained on something new. They do it on their own, aggressively. These Airmen will bleed a training manager dry by signing up for anything available on cyber. Doing so pays off for both the member and the office as long as they retain and then apply their skills at work. What is great about the NSA is that Airmen with experience know how to look for and take a wide variety of agency classes available to service members integrated into the agency. Many classes are exceptional and have prepared them for success within the division as cyber professionals, regardless of where they started or what AFSC badge was pinned on their shirt.

Dogged determination. Some people have failed the entrance interview and have worked for six months, taking courses and studying to close knowledge gaps with added training. I am impressed with them because of the self-discipline needed to improve their skills. Despite the option to reattempt the interview, not everyone passes the second and final time around. Just for reference, six to eight months is the estimated time it would take to prepare a cyber novice within the division so that he or she could simply begin formal training (we've done it before). It is one good reason for the screening process because the division has neither the manpower nor the time to teach basic skills on a regular basis.

Not-So-Successful Applicants

Unfortunately, this category represents a significantly higher number than we would like for the Air Force. At last count, within the previous year, Airmen were batting about one for eight on recent interviews, some of them not clearing the interview on the second try.[15] The other services are doing better, largely due to two factors: prescreening of applicants before the interviews by qualified EAs (some of the best) and sending their version of cyber professionals to the interviews. Not all of them make it, but they enjoy a higher rate of acceptance than does the Air Force at this time. Nobody wants to see this trend continue, and the squadron director of operations and other local experts are trying hard to look for viable solutions to improve the throughput. This article is one of those efforts—an appeal to senior Air Force cyber and intelligence leaders to take notice of the problem and explore some of the solutions recommended below.

Proposed Solutions

Changing the Perception of Cyber Operations

If those of us in the cyber operations field were to walk a group of pilots through the operations floor, they would likely understand many of the positions and functions we have, even if they've never plugged in a router. They could appreciate that place as our "battlefield" and the support elements on the watch keeping our troops and infrastructure safe. They would understand the senior watch officer position monitoring the assets and teams during operations. Finally, they would see kindred spirits/professionals diligently working to carry out the mission in real time. That is their professional world—real-time operations. It is the same world of our IONs and EAs as well when they complete a mission together. If nothing else, this visual could help Air Force leaders grasp that the EA position is a cyber-operational job and that any plans to classify the work role as anything else should be halted.

Recommendations for the Exploitation Analyst Pipeline

The Air Force has tried the same thing for more than three years but has not improved its results. In fact, a case can be made that it has gotten worse at staffing EAs using the current pipeline process. Therefore, I highly recommend that the Twenty-Fourth and Twenty-Fifth Air Forces seriously reconsider how they normally staff and train EAs and other cyber analytical positions.

They should consider sending 14Ns, 1N4s, and 1N2s identified for future EA positions to UCT as a secondary AFSC training requirement. This action would give intelligence professionals a firm foundation in cyber operations and the technical skills needed to succeed at a higher percentage than is the case today. Although doing so may cost more and extend the timeline for preparing an intelligence officer / enlisted Airman for the CMF, it would significantly increase the types of skills needed for this work role.

Furthermore, they should begin drawing directly from UCT the Airmen who already have an exceptional cyber background to qualify for the EA work role. The first option may lie outside the acceptable timelines for 14N, 1N4, and/or 1N2 development, but then again something has to change to improve the numbers.

Another consideration to improve the EA pipeline involves following some of the steps that the 300-series cyber squadrons use to pick IONs. The Twenty-Fourth and Twenty-Fifth could select the best of the UCT or JCAC graduates, interview them before they come to the squadron (if possible), and then screen them again when they arrive. They should provide Airmen more focused training, and then mentor them to ensure knowledge retention. *After all, if personnel do not perform these tasks regularly, then the skills atrophy fast*. Nothing is perfect, but the 315th Cyber Operations Squadron's near–100 percent ION throughput is unmatched by the other services.[16] We must keep in mind that this program is one of the most rigorous in the US government for cyber training, so the squadron has some proven processes.

Process Recommendations

The Air Force has a diverse talent pool, and it should identify applicants early. I am a firm believer that the service needs to open up positions like ION and EA to any Airman qualified to carry out the mission. These positions need to be advertised internally, and since the IONs have an entrance test for training, anyone should be able to take it if he or she is eligible. As for the EAs, a records review and prescreening interview would be a good way to gauge cyber competence. Perhaps using the ION test could also be useful, but keep in mind that it's not directly meant for the EA position. (Note that the NSA is working on a standardized entrance test for EAs as well, but it is not certified yet. In the meantime, we will have to wait for the review board to finish.)

If the Air Force is not already doing so, it should consider testing Airmen for cyber aptitude right out of basic training and in college programs during the junior and senior years to identify cyber talent early. Other services are developing or are already employing these tactics to quickly identify the individuals most interested in cyber careers.[17] The Air Force should consider doing the same with our captive audiences in ROTC and the academy before they enter active duty.

Finally, those of us who have been around the service for a while know that there are some brilliant Airmen walking around with us who may not be in the job they are best suited for. How can we identify them? The key is getting better at tracking skills and training classes that are not currently on an Air Force training report. As a case in point, let us examine the last 1N4 to pass the EA interview in my division. He is one of the eight Airmen who attempted the interview in the past nine months. When I first met him, I knew after five minutes that he was going to pass the interview and do great things with us. Later during an interview for this article, I asked him about his background and why he thought he was prepared for this job. The following are some highlights from the Airman's interview.

Employment background. He spent seven years within the NSA working in multiple intelligence analysis and data forensics shops.[18] Network- and host-based forensics positions are superb training grounds for Airmen wanting to work as IONs or EAs.

Training. Since his intelligence analysis shops required considerable understanding of networking technology, data analysis, and forensics, he had to learn about them. Initially, he took a variety of NSA classes to hone his skills and then never stopped. His NSA training records look like a rap sheet of cyber and analysis classes heading into the sunset.[19] The EA interview was a breeze for him largely because he had seen so much of it before and was already an expert in one of the technical skills that our hiring managers value. The problem for the Air Force is that it didn't really know anything about his training.[20] Word of mouth in the squadron was that he was smart, but his Air Force records were only mildly impressive. Most of his training with the SANS Institute, certifications, and NSA class work just didn't show up on the Air Force's radar.[21]

Aptitude. He is also succeeding because he still wants to learn more, not because he was in a forensics shop or because he has a technical degree. He is in awe of the people he serves with, and they are in awe of him. The best EAs and IONs are humble in expressing the extent of their knowledge and always believe they can learn something new from their counterparts. These stars are usually the brightest in the bunch. Screening for this quality is difficult, but it is part of the interview when we ask how the applicant keeps up with technology and works with others. Those who study cyber at home for fun or experiment with networks are usually terrific applicants.

Conclusion

My hope is that Air Force cyber leaders get more out of this article than replacing 1N4s with 1B4s. That is not the point. I would like the service to really appreciate the fact that in cyber, the line between operations and support analysis is often hard to draw. Airmen whose job title may suggest that they are out of the operational loop are actually on the front line. Airmen with hard-to-find skills are out there in the force, so we shouldn't make it harder for them to sign up. Devising an economical way to identify their talent and being flexible with AFSCs will allow the

Air Force Personnel Center to locate Airmen who want to serve where they are most needed. That is good for the Air Force and great for the Airmen.

The venerable AFSC is a fine idea, but it has somewhat lost its luster in cyber. This article has addressed 1N4s, 1N2s, 14Ns, and the cyber-operational AFSCs, but let us not forget the engineers, scientists, mathematicians, and other career Airmen who have completed NSA tours and received the same training and certifications. Who are we to tell them they can't do the job just as well? Why would the Air Force want to do so when it is so hard to find qualified Airmen? Some of the smartest people we have in my division are our transient Airmen in special programs on nine-month or one-year tours. These individuals are usually in the scientific, engineering, and computer-maintenance career fields, but the Air Force never lets these Airmen serve very long as EAs or IONs because of their pedigree. That's a shame. The ever-dreadful unit manning document should be a helpful guide, not a means to remove the odd person out because his or her AFSC is different from the one on the spreadsheet. The adversary doesn't care what our AFSCs are—guaranteed—so we shouldn't either.

Lastly, the Air Force has to do a better job of identifying its talented people by their skills and outside training. If nothing else, we should be able to ingest the training records and certifications from another Department of Defense school like the NSA's Associate Directorate for Education and Training so that cyber functional managers can make more informed decisions. What if we needed someone in a crisis or, worse yet, had to pay contractors to come in when the Air Force already had the talent on the flight line? It's just not good resource management, so I hope this article can help us move in a better direction. ✪

Notes

1. Deputy chief of ION training, interview by the author, subject: Statistics, 2016.
2. Branch chief, interview by the author, subject: Managing EA Hiring, 2016.
3. Ibid.
4. Ibid.
5. 81st Training Wing Public Affairs, "First Cyber Class Graduates," 8 December 2010, http://www.afspc.af.mil/News/Article-Display/Article/250046/first-cyber-class-graduates.
6. Thom Seith, "Joint Cyber Analysis Course Challenges New and Veteran Sailors," US Navy, 22 January 2015, http://www.navy.mil/submit/display.asp?story_id=85292.
7. Twenty-Fourth Air Force Public Affairs Office, "24th Air Force Fact Sheet," 2014, http://www.24af.af.mil/library/factsheets/factsheet.asp?id=15663.
8. National Security Agency (NSA), "Unclassified Interview Concepts" (Fort George G. Meade, MD: National Security Agency, 2014).
9. NSA Associate Directorate for Education and Training, "Work Role Titles" (Fort George G. Meade, MD: NSA Associate Directorate for Education and Training, ca. 24 November 2014).
10. Ibid.
11. 17S, 1N2, and 1N4 Airmen, interviews by the author, subject: Backgrounds and Training, 2016.
12. Ibid.
13. Ibid.
14. Ibid.
15. Branch chief, interview.
16. Deputy chief of ION training, interview.
17. S3 operations officer, 780th Military Intelligence Battalion, interview by the author, 2016.

[18] 17S, 1N2, and 1N4 Airmen, interviews.
[19] Ibid.
[20] Ibid.
[21] Ibid.

Maj David J. Ortiz, USAFR

Mr. Ortiz (BS, MS, Norwich University, the Military College of Vermont) serves as a leader in cyber operations, planning, and analysis as a Department of Defense (DOD) civilian. He has led an eclectic civilian career after leaving active duty in the Air Force in 2002 to work full time as a scientist and developer. Mr. Ortiz traveled the world to secure some of our nation's most important facilities. In 2008 he switched careers and moved to the Joint Staff where he advised the J-6 on multiple DOD cyber and information assurance programs. He then began work in division-level leadership jobs that created, sustained, and managed cyber operations centers. Mr. Ortiz's military career is similarly diverse, spanning more than 4 years of active duty and another 14 as a reservist. He has worked in 4 distinct career fields, including air battle management, intelligence, research, and cyber operations. Currently, he serves as the individual mobilization augmentee (IMA) to the director of operations for the 315th Cyber Operations Squadron. In his spare time, he volunteers on the Norwich University Alumni Association Board of Directors, providing career and resume counseling to many alumni. Mr. Ortiz resides in Maryland with his wife and four children, who fill his leisure time with an endless supply of hilarious soliloquies and craziness.

Let us know what you think! Leave a comment!

Distribution A: Approved for public release; distribution unlimited.

http://www.airpower.au.af.mil