America's Cyber Auxiliary: Building Capacity and Future Operators

Lieutenant Colonel (Ret.) Jeffrey J. Fair

ABSTRACT

As the proliferation of cyber threats continues and the complexity and number of online systems grows, the need for updated cyber defenses to appropriately combat the threat will continue to expand into the future. The public and private sectors both heavily rely on accessing and using secure networks. The requirements for defense already outstrip the current capacity the US government has and needs reinforcement.

A cyber auxiliary can provide several ways to augment our cyber defense capacity. Education programs can equip the population with skills and awareness to serve as a solid front-line defense. A cadet program could enhance the educational approach and expose a larger population to in-depth knowledge of cyber defense and network operations, building a cadre for the future. Adult auxiliary members can add capacity to current cyber-defense organizations and be critical actors in aiding civil defense and even DoD. Much like the change in warfare observed during and after World War I, cyberspace is changing and growing. It is time to recognize both the environmental shifts and the opportunities available to the nation to get ahead of the coming cyber tsunami.

Jeff Fair is the Vice President of Cybersecurity and Economic Development for the San Antonio Chamber of Commerce and as the lead for Cybersecurity San Antonio, a public-private partnership between the Chamber and the City of San Antonio charged with enhancing the cybersecurity industry in the city. Fair is a Ph.D. candidate at the George Washington University's Trachtenberg School of Public Policy and Administration.

His dissertation research includes governmental transparency in the U.S. Intelligence Community. He retired as a LTC after a 22-year career in the U.S. Army where he served in several organizations including the National Security Agency and U.S. Cyber Command. Fair holds a BA from George Washington University's Elliott School of International Affairs, an MBA from Hawaii Pacific University, a MPA from the University of Washington's Evans School, and a MSSI from the National Intelligence University (NIU). He later served as an adjunct for NIU, teaching courses at its NSA Academic Center.

Malicious cyber actors pose one of the greatest contemporary threats to the United States, but the country continues to fall well short of the capability and capacity needed to adequately protect itself in real-time. Cyber-attacks in the public and private sectors feature regularly in news reports, while increased post-attack mitigation efforts can aim only at limiting the damage. America and its allies even contend with threats to electoral systems and their democratic way of life as adversaries manipulate social media and other information flows. The threats are continuous, innumerable, and widespread, and the US is struggling to keep pace and identify better ways to defend against them.

As the number of government, military, and private cyber activities increases, the threat continues to grow and evolve. Several initiatives have been aimed at increasing US capacity in cyberspace. The federal government elevated U.S. Cyber Command (USCYBERCOM) to full combatant command status, expanding its purview and power structure. The move was joined by the military services, which initiated a rapid expansion of their own cyber units and specialists. The Trump administration adopted a new approach to dealing with malign cyber actors called persistent engagement, bringing a more active defense to bear on cyber threats that the Biden administration has decided to continue to practice. The involvement of USCYBERCOM in the pursuit of ransomware actors marks a new turn in the fight against threats that targets private sector companies, non-profits, school systems, and other government organizations at all levels.

The threat, however, remains real and continues to adversely affect organizations in all sectors: public, private, and non-profit. Some estimates show cyber-related crime and industrial espionage cost the US economy over $2.1 trillion between 2015 and 2019.[1] Several high-risk sectors like health care, financial services, and manufacturing have been heavily targeted.

Not only will additional threats emerge over time, but an explosion in the number of online devices is adding more opportunities for malicious cyber actors. As government continues to invest in defense, so does the private sector, but the losses continue to mount.

Even with the additional steps taken by the US government (USG), it will continue to be difficult to stem the rising tide of cyber-attacks and cyber-espionage. It can be compared to plugging holes in a boat riddled with small holes and more holes appearing all the time. Some have advocated the rapid employment of artificial intelligence, advanced machine learning, and other high-technology tools to augment the professionals battling myriad current threats, but those solutions may be years or more away. The need for more cyber-defense capacity has never been more acute.

The answers to achieve a higher capacity are generally not quick wins, as evidenced by the push for rapid fielding of new technological solutions. The remedies, however, can be lasting and must be multi-dimensional. The concepts of using machine learning and artificial intelligence, teamed with human analysts, are maturing but that technological advance will not solve the entire capacity problem. Initial attempts to increase capacity by utilizing the military services have included a more traditional approach, using the total force. The Air Force not only has reserve cyber units to augment its active-duty cyber warriors, but has also fielded cyber units in the Air National Guard. In addition to reinforcing active-duty efforts, the Texas National Guard activated cyber units to assist school districts and local municipalities affected by ransomware attacks.[2]

Current efforts involve officials creating additional capacity in the face of a growing threat. Congressman Tony Gonzales (R-TX), a former Navy cryptologist, is sponsoring legislation to create a National Digital Reserve Corps. The organization would comprise "a group of civilian individuals with relevant skills and credentials to address digital and cyber needs across the federal government."[3] It would fall under the General Service Administration (GSA) and rely on the GSA to allocate additional resources to agencies in need.

The most audacious plans, however, would provide both a relatively short-term increase in manpower and a long-term, possibly multi-generational, approach to building a cyber-smart military, workforce, and citizenry. Some lessons from current organizations provide possible paths to that bold objective.

Using Lessons from History

In the past, the US has been able to successfully react to rising threats in relatively new domains of warfare. Studying analogous situations and environments and drawing implications for cyberspace provide apt analogies that can help investigate possible strategies for cyber-related approaches.[4] Two organizations provide examples of how we can proceed in adding capacity and improving the nation's cyber readiness.

By the First World War, the air domain had demonstrated its potential and the US was devising ways to gain advantage. Although the air domain could arguably include balloon observations in the Civil War, the direct destructive power of the airplane had manifested in the First World War and made clear to all that airpower would have a significant role in the future of warfare.

There were several organizations and initiatives aimed at improving the military capability of the US in this new domain. Many of these organizations found it was also important to generate civilian enthusiasm in this area for commercial and research purposes. One such organization was the Civil Air Patrol (CAP), founded by a World War I aviator, Gill Robb Wilson.[5] He returned to the United States from Germany in 1936 convinced that a war was brewing in Europe and realized the US needed additional aviation capability, capacity, and education. The CAP was official established by the Commerce, Navy, and War Departments in late 1941 after Wilson's organization consolidated several other flying organizations into a larger, more organized group. Before and during World War II, the group flew anti-submarine patrols off the Atlantic and Gulf coasts. In 1942, the group added a Cadet program that educated teenagers in aviation. Following the war, the CAP was placed under the newly created Department of the Air Force as the branch's civilian auxiliary.

In addition to augmenting patrols on the West coast of the US during World War II, CAP worked with local civil defense programs in planning and execution drills. Later, CAP began to assist local authorities in search and rescue operations. As crash locator beacons became more prevalent in civil aviation, the Air Force directed CAP to begin assisting in search and rescue operations responding to possible incidents with small civil aircraft. Today, the CAP also assists in mass casualty and disaster relief operations/exercises around the country. Thus, CAP provides invaluable additional capacity and sometimes free up assets to work in other areas.

Beyond its operational missions, CAP runs a robust cadet program that includes several benefits. First, it teaches cadets ages 12-21 leadership through a testing regimen and participation in exercises, search and rescue missions, and other programming. More importantly, however, cadets learn about all aspects of aviation. Educational materials provide a thorough history of aviation, from the Wright Brothers to some of the most recent developments in the aerospace industry. CAP has programs to teach cadets to fly with both ground school and flying instruction. The programs instill a lifelong interest in aviation and help propel many to careers in the aviation industry.

The U.S. Coast Guard Auxiliary (CGAUX) is another organization that can be an example for a future cyber auxiliary. The CGAUX was created in 1939 and for over eighty years has assisted the Coast Guard with patrolling, search and rescue, and educational programs. It provided 50,000 members at the beginning of World War II to assist in patrols, and over time, increased capacity by placing many private vessels into service.[6]

Today the CGAUX is visible on US waterways and is well known for its boater education and outreach. To promote and improve safety, the CGAUX provides instruction at all levels, thereby improving proficiency, and instilling a love for boating. Courses include operations, maintenance, navigation, and safety topics as well as what to do in an emergency. The CGAUX also plays an important role in providing additional capacity for the Coast Guard during disaster relief, search and rescue, and pollution response. The additional capacity provided by the CGAUX has saved many lives and allowed the Coast Guard to focus on core missions and situations that demand its more specialized equipment and training.

A New Approach

What then, can cyber policy experts gain from familiarizing themselves with CGAUX and CAP? Both organizations offer insight into how cyber leaders can organize, train, and develop capacity in citizens thus providing additional capacity in times of crisis. First, a United States Cyber Auxiliary could embrace education as a core mission. There are several groups that provide cyber education and training, but none resemble an organization like the CGAUX, which is respected, well known, and offers a lifelong education. A cyber auxiliary could provide classes around the country at little or no cost. The audiences would be varied, from novice users to system administrators from those undergoing elementary education to senior citizens. Classes would likely have to concentrate on the defensive side of cyber activity, including basic concepts of information security, password strength/protection, and how to identify suspect emails and websites.

Education options would include a mixture of online and in-person courses and could also bridge the gap between the general population and organizations like the Department of Homeland Security (DHS), the Federal Bureau of Investigation (FBI), and the National Security Agency (NSA). A cyber auxiliary could help those organizations push critical messaging to the public and educate them regarding available resources. Another education-related role would include the advertisement of cyber-related grants and scholarships, coordination of educational efforts in cyber education, and incentivizing cyber careers through scholarships and grants.

The second approach a cyber auxiliary should consider is the inclusion of a cadet program. The shape and feel of such a program would ultimately be dependent on the parent organization of the auxiliary, but a cadet program would accomplish several goals that cyber experts have advocated for many years. First, a cadet program is another way to deliver cyber education, albeit the program would likely be much more rigorous than what would be offered to the general population through the auxiliary. Next, a cadet program builds leadership skills and develops youth who may be interested in government, military, and/or adult auxiliary service in the future. Finally, the program would inculcate an appreciation of cyber skills and instill a desire for lifelong learning in the cyber environment.

Another reason to create a cyber auxiliary would be to build greater capacity for USG cyber organizations. This aspect of the auxiliary might raise concerns, but a few key items can make it focused and effective. The auxiliary would have to be granted authorities to operate but would likely be limited to defensive cyber operations. Much like the educational curricula, any auxiliary cyber operations will be limited to augmenting defensive cyber protection and recovery. The auxiliary could, like the CGAUX, perform regular patrols and assist local government and businesses with network assessments in conjunction with the educational mission. Alternatively, a cyber auxiliary could be activated by a USG parent organization during times of crisis to work on a portion of cyber response or work along USG cyber operators to build capacity, although still limited to defensive cyber operations.

A cyber auxiliary could deliver education and house a cadet program under several elements within the USG. For an organization to assist in active cyber defense operations, it would have to be associated with a department with an active cyber mission and existing authorities. The sponsoring organization would have to exercise tight control over the adult auxiliary volunteers through training, exercises, and emergency procedural powers. Although, the CAP and CGAUX are associated with the Air Force and the Coast Guard respectively, there is nothing preventing a cyber auxiliary from being associated with USCYBERCOM, under the Department of Defense (DoD). A possible alternative could be DHS, which has a much closer tie to civil defense and local protection and mitigation needs. A third option could involve both DoD and DHS, activating auxiliary members to support DoD in case of a national emergency.

No matter what organization a cyber auxiliary eventually falls under, the controls on using auxiliary cyber personnel online must be stringent. The Army has exercised pairings between the active and reserve/national guard components for training and readiness. Cyber auxiliary members could sit alongside USG personnel (military or civilian) during training and exercises, ready to return for operations if the need arises. This portion of the auxiliary would likely take the longest to realize, but could be transformational. Any organizational approach, however, would need to retain an education aspect and possible cadet program to realize the long-term, multi-generational benefits such programs could ultimately achieve.

CONCLUSION

Cybersecurity is now viewed as an important ingredient to myriad functions of society, from the public sector to private industry. The opportunity technology presents must be protected by strong security from a growing number of threats, both state-sponsored and non-state actors. As the threat grows, so too must the effort to protect vital technological resources.

As detailed in this article, a cyber auxiliary can provide both a near-term and long-term solutions to a dynamic threat landscape, which will continue to grow and evolve. There are, however, actual costs involved and significant bureaucratic hurdles to overcome to implement such a multifaceted solution. The expense of establishing any organization can be daunting, especially in an environment that has growing regulatory requirements. There are ways to structure an auxiliary that could limit initial costs and continuing operational expenses. A Public-Private partnership has been a favorite approach of late to cybersecurity and could help jump-start an auxiliary. Another option, similar to CAP or CGAUX, you can tie the organization to an existing agency or service.

In analyzing the options for structures to address concerns with costs or oversight, bureaucratic impediments and resistance to new models will need to be addressed. Unlike CAP or CGAUX, there is no service to attach a cyber auxiliary to, but several organizations have possibilities. To explore options like the U.S. Digital Service, USCYBERCOM, or GSA, new forms of oversight and operational control will have to be developed, tested, and trusted to make a cyber auxiliary work. Legislators and administrators must about the present and the shape of things to come to ensure a capable and nimble organization is formed that can provide the additional capacity the nation requires.

Although the costs of creating a cyber auxiliary can be viewed as an uphill battle, the benefits of an organization that can bring capacity, education, workforce development, and awareness would be truly revolutionary. Recent events have demonstrated the need for the ability for everyone to understand the threat and the necessity of additional cybersecurity capacity during a crisis. The nation will not have the luxury of debating how to increase its capacity to defend against cyber adversaries much longer. The time to find solutions is now.

NOTES

1. William T. Eliason, "An Interview with Paul M. Nakasone," *Joint Force Quarterly* no.9, 2 (2019).
2. "'Holy moly!': Inside Texas' fight against a ransomware hack," KALB, accessed January 15, 2022, https://www.kalb.com/2021/07/26/holy-moly-inside-texas-fight-against-ransomware-hack.
3. "Representatives Tony Gonzales, Robin Kelly Introduce Bill to Form National Digital Reserve Corps," press release from July 29, 2021, accessed on January 15, 2022, https://gonzales.house.gov/media/press-releases/representatives-tony-gonzales-robin-kelly-introduce-bill-form-national-digital.
4. Robert Axelrod, "A Repertory of Cyber Analogies," in *Cyber Analogies* (Monterey: DoD Press, 2000), 108-116.
5. "History of Civil Air Patrol," Civil Air Patrol, accessed August 25, 2020, https://www.gocivilairpatrol.com/about/history-of-civil-air-patrol.
6. "About the Auxiliary," United States Coast Guard Auxiliary, accessed August 25, 2020, http://cgaux.org/about.php.