The need for a National Cyber Academy:
The United States Cybersecurity Academy

In the 21st century, the landscape for war has extended from land, sea, air, and space to a fifth domain- cyberspace. America's digital strategic infrastructure is now considered a "strategic national asset" and protecting this has become a national priority. The state of cybersecurity for the nation has reached a critical status. There is an urgent need for skilled cybersecurity professionals across the workforce and for leaders in the federal government, across the security agencies. The National Science Foundation's Scholarship for Service program is one vehicle geared towards encouraging the best cyber talent to work for the government, at least for several years, before being lured to industry for higher salaries. This program has encouraged many students to work for agencies such as NSA, CIA, etc.

The cybersecurity crisis requires a multifaceted solution and the time is right for another service academy focused in cyber. Dr. Mark Hagerott and Admiral (Ret.) James Stravridis formally recommended this in March 2017 in their Foreign Policy article entitled "Trump's Big Defense Buildup Should Include a National Cyber Academy." Additionally, Dark et al. propose the idea in the 2018 CISSE paper entitled: The Cyber Cube: A Multifaceted Approach for a Living Cybersecurity Curriculum Library.

There is a history for this. After the Revolutionary War, soldiers and legislators, including Washington, Hamilton and John Adams, concerned about American reliance on foreign engineers and artillerists, lobbied for the creation of an institution devoted to the arts and sciences of warfare. In 1802, Thomas Jefferson signed legislation to establish the United States Military Academy at West Point, a strategic military center. In addition to providing military officers, the USMA became the first accredited civil engineering school and its early graduates helped construct the nation's first railway lines, bridges, harbors and roads. The mission of the USMA is: "To educate, train, and inspire the Corps of Cadets so that each graduate is a commissioned leader of character committed to the values of Duty, Honor, Country and prepared for a career of professional excellence and service to the Nation as an officer in the United States Army."

Similarly, the United States Naval Academy was founded in 1845 in response to a need for trained officers at sea. The curriculum of the USNA has shifted to accommodate the high tech fleet of nuclear-powered submarines and surface ships and supersonic aircraft .The USNA, located in Annapolis, MD, states the following mission – "To develop Midshipmen morally, mentally and physically and to imbue them with the highest ideals of duty, honor and loyalty in order to graduate leaders who are dedicated to a career of naval service and have potential for future development in mind and character to assume the highest responsibilities of command, citizenship and government."

Most recently, the Air Force academy was built to address our needs in aerospace including missiles and atomic weapons. Following decades of political pressure to increase America's air power, it was not until 1954 that President Eisenhower (ATC) initiated a detailed curriculum for the Academy program. The United States Air Force (USAF), formed as a separate branch of the U.S. Armed Forces in 1947, is the aerial and space warfare service branch of the United States Armed Forces. The Air Force defines its core missions as "air and space superiority, global integrated ISR, rapid global mobility, global strike, and command and control." While each of the military academies have their own cyber programs, their primary aim is to provide officers to their respective military branch. The numbers are relatively small - the USMA produces 15 graduates per year and the USNA's freshmen class has 110 cyber operations majors (the class of 2018 had 22 cyber majors). While some service academy graduates eventually work for the federal agencies, generally this is after they have completed their service requirements.

The defense and military landscape has changed, and the nation's infrastructure and public safety are at stake. The United Stated Cybersecurity Academy (USCA) that produces the much-needed cyber specialists for the federal government would bolster the status of the US in the international arena and help protect our critical infrastructure. Additionally, the USCA would provide a center or hub for the cybersecurity community and foster synergistic activities, such as workshops, training, lectures, competitions and other cyber events, to vitalize national workforce development.

The USCA would in many ways resemble the existing academies, accredited, free, and selective, but graduates would be required to serve as civil servants for the federal government. The cybersecurity major could resemble the NSA cyber Ops program, be deeply technical, and include computer science, cybersecurity offense and defensive skills as well as a solid liberal arts courses including history, government, and cyber laws. Given the technical landscape, the USCA should be adaptive and include significant virtual infrastructure to allow cybersecurity leaders and experts across the world to provide instruction remotely. The faculty of the USCA would not be tied to the traditional doctoral requirement as for most four-year schools, but instead facilitate the cybersecurity experts in the country to serve as faculty. Additionally, the entrance requirements would allow for students with disabilities. A prep school or ROTC program geared towards cyber would be a good complement, perhaps following a model as being kicked off in Huntsville Alabama.

Obviously, the costs for such a brick and mortar institute are high, so I propose that the academy begin as a virtual infrastructure, including a "national credit" model where the USCA offers full courses in critical areas such as reverse engineering and cyber operations. National credit would allow schools that are trying to build cyber programs supplement their programs by accepting the USCA courses for credit. The academy should include a library of cybersecurity resources for K-20, including curriculum that is mapped to national standards and aligned to learning taxonomies, including labs and exercises and different modes of instruction. Additionally, a cyber range, both public and private, is necessary to support the academy and the digital library. Given the national shortage of cybersecurity faculty, this would help better prepare the cyber workforce.

In addition to start-up and operating costs, another significant challenge to a national cybersecurity academy is diversity. Since women were permitted to enter the military academies in 1975, each of the academies have worked hard to achieve diversity and each has struggled against perceptions of hostile environments. The USCA must be created with an eye towards fostering diversity, not only for women but across ethnicity, to provide an inclusive environment. Socialization and courses on inclusion and acceptance would be key to producing cyber leaders with these attributes.

Cyberspace is the new battlefield. It is imperative that the United States prepare for it on all fronts.