Civil Cyber Defense – A New Model for Cyber Civic Engagement

Dr. Mark Grzegorzewski
Major Margaret Smith, Ph.D.
Dr. Barnett Koven

ABSTRACT

In a world of ubiquitous connections, cybersecurity is everyone's responsibility. Gone are the days when the actions of others had little impact on a person's day-to-day activities. We are now completely digitally interdependent, meaning the actions of one individual can be the vulnerability that allows adversaries to target a soft spot in the United States' (U.S.) digital infrastructure. We argue a whole-of-society approach to cybersecurity is needed. The involvement of all members of society is required to defend against the scourge of cyber intrusions emanating from Russia, China, North Korea, and Iran. We do not promote individuals or corporations engaging in offensive cyber operations, but instead advocate that the U.S. already has a non-governmental model for citizen involvement in entities like the Civil Air Patrol (CAP), to adopt for cyberspace. We build on Estonia's Cyber Defense League (CDL) organizational model and the works of others, advocating for establishing a Civil Cyber Defense (CCD) in the U.S. We conclude with specific actions this new entity could take to increase the overall cybersecurity posture of the U.S. and identify potential issues with our CCD concept.

INTRODUCTION

In cyberspace, we find ourselves in an era of ebbing United States (U.S.) dominance. Like actions in the physical space, America's adversaries are engaging in asymmetric tactics and strategies in cyberspace and the information environment to degrade the U.S. physical and cybersecurity posture and capabilities. At this moment, there

This is a work of the U.S. Government and is not subject to copyright protection in the United States. Foreign copyrights may apply.

Dr. Mark Grzegorzewski is an assistant professor of cybersecurity at Embry-Riddle Aeronautical University in the Security Studies and International Affairs Department. He is also an Army Cyber Institute Fellow. His recent publications include: "911? We Have an Emergency: Cyberattacks on Emergency Response Systems," "In Search of Security: Understanding the Motives Behind Iran's Cyber-Enabled Influence Campaigns," and "Why the United States Must Win the Artificial Intelligence (AI) Race," Dr. Grzegorzewski worked for over 11 years in the Department of Defense, seven of those years for U.S. Special Operations Command. He holds a Ph.D., M.A., and B.A. in Political Science/Government from the University of South Florida and a graduate certificate in Globalization Studies.

is both an opportunity and a need for the U.S. to do something creative in addressing cybersecurity to better arm itself against asymmetric and irregular threats. Estonia, given its democratic government and proactive cyber defense posture, is an ideal case to examine. In 2007, Estonia was targeted by Russian cyber proxies, and in response, developed the Cyber Defense League (CDL), which relies on civilian talent to help fill security gaps and to augment its traditional government defense apparatus. To integrate the CDL, Estonia leveraged its hacking community's social capital and national pride, providing everyday hackers and enthusiasts (who may or may not work professionally with computers) an opportunity to protect their country against foreign aggression in the cyber and information spaces.

At present, the U.S. is in a similar situation as Estonia in 2007: America is experiencing a constant barrage of cyber intrusions and foreign operations in the information environment. It is at great risk from the actions taken by its adversaries and their cyber proxies. To date, the U.S. has no plans to build a civilian program comparable to Estonia's CDL or to leverage civilian knowledge in its cyber defense strategy. We argue that the U.S. should create an American Civil Cyber Defense (CCD) – civilians working to defend the nation from cyber threats – because civilians and civilian talent are necessary components of an effective and robust approach to cybersecurity and a whole-of-society response to cyber threats and cyberattacks. To be clear, our proposal does not include promoting civilian engagement in offensive cyber activities or espionage but is instead focused on building a framework for developing an all-volunteer force of civilian cyber defenders and leveraging civilian talents to augment the ongoing law enforcement, government, and military efforts to defend the nation and U.S. networks against cyber threats.

In this article, we make a case for the CCD by articulating what a "whole-of- society" approach to cyber-

MAJ Maggie Smith, Ph.D., is an Army Cyber Officer currently serving as a Strategic Planner for HQDA. She is also a Senior Fellow at the Atlantic Council's Cyber Statecraft Initiative, Director of the Irregular Warfare Initiative's Cyber Project, and graduate faculty at the University of Maryland, College Park.

security should include, proposing how to implement and incorporate a CCD into America's national defense strategy, and providing an organizational structure for the CCD that is modeled on the Civil Air Patrol (CAP) concept. We also demonstrate the effectiveness of the CCD model by investigating the Estonian example. Finally, we address potential pitfalls and difficulties to employing citizens in a defensive-oriented CCD to augment our national cyber strategy and how to mitigate those risks.

THINK SMALL: STRENGTHENING THE NETWORK AT THE LOCAL LEVEL

In cyberspace, one individual's vulnerability can quickly become the network's security compromise, and in terms of overall U.S. cybersecurity and interconnectedness, that means less secure organizations pose a direct risk to organizations that have hardened and resilient systems. In short, all networks are less secure due to interconnectivity and all networks are increasingly at risk as more and more devices and users become connected. Once an adversary gains a foothold into a network through an unsecured system, they can laterally move in and through that network to cause damage upstream or downstream. While many large organizations allocate extensive resources to cybersecurity, many more small businesses simply do not have the resources or expertise to protect their systems.

For example, in 2016, Cate Machine & Welding's "dusty old computer humming away in the back office" of the small Wisconsin business was taken over by Chinese hackers.[1] Even though the hackers were not interested in Cates' data, they used a jumbled maze of compromised computers as the launchpad for their attacks. "Mom and pop" businesses are equally important as any other node in the network and need greater security to make the broader cybersecurity ecosystem stronger.

Dr. Barnett S. Koven is a Manager at Deloitte working as a data scientist in the firm's federal sector strategy & analytics practice. Dr. Koven is a national security specialist and data scientist with over a decade of experience in counterterrorism, counterinsurgency and strategic competition. He has deep expertise in leading analytics teams applying quantitative and qualitative approaches to national security combining research design, inferential statistics, machine learning and applied AI, survey experimental research, and data visualization. He has received research funding from the U.S. Departments of Defense (DoD), Homeland Security (DHS), State, Justice, and Energy, as well as from the Horowitz Foundation for Social Policy, George Washington University (GWU) and University of Maryland (UMD). He received his Ph.D., M.Phil. and M.A. degrees in Political Science, as well as a B.A. degree in International Affairs and Latin American and Hemispheric Studies from GWU.

Just like the owners of Cate Machine & Welding "had no idea [their business computer] could be used as an infiltration unit for Chinese attacks,"[2] most small businesses do not view cybersecurity as a major priority or problem. Yet, 28 percent of data breaches occur at small businesses and of those 28 percent, "37 percent suffered a financial loss, 25 percent filed for bankruptcy, and 10 percent went out of business" in the year following the breach. Data also indicate that less than half of small businesses[3] believe they can quickly respond to a data breach.[4] Coupled with the fact that many small businesses cannot promptly respond to and remediate a cyber intrusion, 67 percent of small business owners deny they are even vulnerable to an cyberattack.[5] Additionally, ransomware attacks are increasing and 55 percent occur against businesses with less than 100 employees.[6] The result is a dangerous combination: small businesses do not think malicious actors will target them, and they are ill-equipped to handle a breach when one does occur.

Small businesses are not the only local or community concern – cybersecurity risks that state and local governments face are also alarming. Investors and insurance providers are increasingly worried about the spiking number of attacks against local government IT services and data. Specifically, the onslaught of ransomware attacks targeting the public sector at a time when most state and local governments are still trying to figure out how to deliver and sustain services online. A recent survey of "150 municipal bond credit analysts and specialists (excluding those at rating agencies) carried out by HillTop Securities shows digital risks are increasingly on investors' minds – and practically none of those investors think state and local governments are prepared" for a cyberattack.[7] Additionally, only six percent of respondents thought state and local governments were "on their way to being prepared" for cyberattacks, and not a single survey respondent thought that small governments were "prepared," or "very prepared," to face a cybersecurity incident.[8] The implications of an insecure public sector are vast and far-reaching and, with smaller budgets and smaller staffs, local government cybersecurity efforts are likely to remain underfunded and understaffed.

Of course, small businesses and local governments are not purposefully negligent or willfully ignorant. In many cases, small businesses and government entities do not have the proper conceptualization of cyber risk.[9] In other cases, small organizations do not have a sufficient budget allocated to cybersecurity or do not have the funding or technical resources to implement proper security measures.[10] While the proposed CCD model cannot address small business or local government resource allocation, the model can address owner and worker education to raise awareness and knowledge of cyber risks and advise on rudimentary remediation plans. A CCD and its cadre of volunteers could help small businesses and mayoral offices with cybersecurity tasks, like updating their systems and installing patches. Estonia provides a case study for how a CCD can make a difference in national defense by encouraging and enlisting the help of civilian talent.

IMITATION IS THE SINCEREST FORM OF FLATTERY: ESTONIA

Estonia is one of the most digitally connected—and digitally dependent—countries in the world.[11] To make a decisive break with its Soviet past and chart its own future by embracing democracy and capitalism, Estonia incorporated technological solutions to leap past many other developing, former-Soviet states. But Estonia still struggles against the pull of Russia's influence—the northern Estonian border is just over 90 miles from Russia's second largest city, St. Petersburg.[12] Russia does not respect Estonia's sovereignty,[13] and to offset Russian influence in the country, Estonia actively pursued membership in the European Union and North Atlantic Treaty Organization.[14] Despite—or perhaps because of—these memberships, Estonia was the target of Russian cyber aggression in 2007 following the "Bronze Night" protests.[15] Adding to the Russian proximity problem is Russia's extant desire to reclaim its former great power status by expanding its sphere of influence.

In response to its 2007 cybersecurity failures, Estonia decided that it should scale its cyber capabilities by tapping into the civilian and private sectors to defend against hacks orchestrated by Russia (The IP addresses linked to the computers responsible for the 2007 attack on Estonia emanated from Russia, but the government denied direct involvement.). The Estonian cybersecurity community and the Ministry of Defense proposed the creation of a Cyber Defense League, modeled on the Estonian Defense League, which is a "voluntary national defense organization" under the Estonian Ministry of Defense.[16] The CDL was designed to augment the existing defense league and is tasked with a civilian cyber defense capability.[17]

Estonia divides its CDL forces into regional units composed of a diverse set of members whose skills are aligned with local concerns. Since the units are composed of volunteers, individuals cannot be compelled to always participate, and members maintain a commitment that works around their family and business obligations. The volunteer format has the benefit of flexibility,[18] and since there is no permanent CDL staffing, a region could experience a lapse in support. Still, Estonian citizens broadly understand their precarious national security situation and that every Estonian has a role to play in homeland defense[19]—particularly in the cyber realm.

After gaining independence, Estonia made concerted efforts to become "E-stonia," an internet-based society. The country was quickly wired after it became independent and began teaching programming to young schoolchildren (beginning at age 5). More importantly, it was a country whose population understood well the need to be free from the former Soviet Union, and its successor state, the Russian Federation, as Russia remained a tangible threat to the new country's sovereignty. To be effective against Russian aggression, the Estonian CDL focuses citizen participation on improving critical information infrastructure security by pursuing three main efforts.[20]

- ***Developing a network of cooperation including for crisis response.*** This is accomplished by strengthening cooperation among qualified volunteer IT specialists, as well as through the creation of a network to combine the expertise of public and private sectors to act in a crisis.
- ***Improving the security of critical information infrastructure*** by regularly sharing threat awareness information and disseminating best practices to the public and private sectors, as well as enhancing preparedness for operating during a crisis.
- ***Promoting awareness, education, and training*** by providing continuous information security education and training to members as well as actively participating in cybersecurity training networks, including international ones.

In addition, the CDL can be reassigned to support the Estonian Computer Emergency Response Team (Estonian-CERT), a team that analyzes and disseminates cyber threats and vulnerabilities to coordinate responses during times of crisis involving critical information infrastructure and systems.[21]

Estonia's comprehensive security approach recognizes that integrating the public into a whole-of-nation defense *after* the state is already at risk is too late. Taking a proactive security approach and engaging citizen defenders during a time of relative peace is critical to ensuring Estonia has a more robust defensive posture during conflict. Therefore, Estonia's cyber defense strategy has created and fostered the connections among citizens, the commercial sector, and the government necessary to establish the networks for a collective defense *ahead* of a major crisis.[22] This also has the added benefit of promoting security, safety, and stability during peacetime.

THE VOLUNTARY SERVICE MODEL

Derivatives of the three main efforts for the CDL described above include the voluntary service model as a cost-effective way to improve national defense.[23] In the case of Estonia, CDL members are not paid unless they are mobilized.[24] Additionally, members provide their time and expertise without compensation and most participate out of a sense of patriotism. Of course, the opportunity to network among fellow professionals and gain workplace training is a non-financial benefit to all CDL volunteers, but it may not be sufficient to offset the opportunity cost of donating time. However, by drawing from, and depending on, its existing cyber-qualified workforce, Estonia saves on resources that would otherwise be allocated to training soldiers or government civilians on cybersecurity tradecraft. Regional cyber defense unit (CDU) members, in most cases, already maintain extensive cyberspace expertise and only need to learn organizational processes to be effective defenders. Furthermore, given the voluntary nature of the CDU, its members do not have to be housed on a full-time basis when compared to the costs of sheltering a traditional military member.

Another benefit of CDL's volunteer model is that it gives individuals that may not be qualified or capable of serving in the armed forces an opportunity to serve their country. That is to say, those who cannot serve in the armed forces are still able to work in the service of the state through the CDL. For instance, a cyber security expert with a physical disability may want to serve the country out of a sense of patriotic duty but traditional military qualification requirements would prevent them from serving. By opening CDL volunteer opportunities to traditionally excluded individuals allows many more volunteers to contribute to defense of the country. Given that the CDL is a voluntary organization, it also allows individuals to join who are not looking to commit to full-time military service.[25] The path to fulfilling patriotic service in cyberspace via the CDL allows for many more Estonians to contribute service in defense of their county at a very low cost to the government.

Another aspect of cost-saving is a shortened incident response time.[26] By not centralizing CDL volunteers, response times are shorter because mass mobilizations of personnel and equipment normally take time. Critically, quick response times and rapid remediation are key in any cyber incident.[27] When the decision to deploy CDL forces is made, the regionally aligned and trained CDUs are quick to respond. While larger strategically focused cyber forces are certainly important, having a local, quick reaction cyber force enables swift documentation and remediation of any cyber incident without having to expend the resources required to rapidly pull in strategic-level forces. CDL volunteers build upon the resilience of Estonia's cyber infrastructure by providing an on-demand service should the Estonian national cyber force be needed on a different mission set.[28]

CREATING A COLLECTIVE INTEREST: ESTONIAN SOCIAL CAPITAL AND NATIONAL PRIDE

Any form of civilian cyber defense coordination requires trust among members and, by extension, the trust of their government. The trust between citizens and government is often referred to as a "psychological contract," wherein a person and organization both gain from the partnership since their beliefs and principles largely overlap.[29] Moreover, in the psychological contract model, individuals understand the needs of the organization and how supporting the organization benefits them, which creates an obligation for the individual to protect their individual interests and the organizations' (the state) interests. Accordingly, any psychological contract is demonstrably at its strongest when there are high levels of public support between citizens and government. An example of a strong psychological contract between the state and citizens is the 78 percent of Estonian respondents who in 2018 agreed (with only 6 percent disagreeing) that the entire society was responsible for the defense of the nation.[30]

Critical to the notion of a psychological contract between individuals and the state, is the idea that corporations also have a role to play. Businesses can maximize outcomes by working in a stable environment in which actions in cyberspace are regularized and surprises minimized. By viewing themselves as part of a cybersecurity collective or ecosystem, in which private entities provide much of the information technology (IT), operations technology (OT), and skilled labor that underpin modern communications infrastructure for a state, IT and OT-related corporations increasingly see their interests as overlapping with the interests of the citizen and the state.[31] In the case of Estonia, the shared cybersecurity interests between the state, its citizens, and corporations has prompted private companies to view employee participation in the CDL as in their own best interest.[32]

Additionally, trust between individuals is just as important as trust between the citizen and the state. CDL members come together to provide expertise and education, they share information with each other and gain trust.[33] Trust and interoperability allows the CDL to resolve issues quickly and collectively. Trust also allows members to work outside of the traditional bureaucratic structures and thereby streamline responses.[34] Moreover, trusted connections exist outside the CDL. For example, CDL members can also call each other in their private or personal lives to resolve cyberspace issues. Regarding the Estonian collaborative model, Piret Pernik and Emmet Touhy write, "as people know each other personally, they tend to trust others more than in impersonal interactions, and greater flexibility enables them to share information swiftly as cyber incidents evolve very fast."[35]

Estonia has built resilience into their comprehensive security approach by emphasizing that every citizen has a role to play in national security.[36] Estonia's approach maintains the notion that all citizens may be called upon to contribute to a collective defense should Estonia's sovereignty or security be threatened. Additionally, given its small size, proximity to Russia, and its history of occupation, the government proactively looks for security gaps, anticipates emerging gaps, and identifies potential solutions should the traditional defense model for the state fail. Estonia's comprehensive security approach also recognizes that integrating the public into a whole-of-nation defense *after* the state is already at risk, is too late. Ultimately, taking a proactive security approach and engaging citizen defenders during a time of relative peace is critical to ensuring Estonia has a more robust defensive posture in war or during an attack. Estonia's strategy has created and fostered the connections between citizens, the commercial sector, and the government necessary to establish the networks for a collective defense *ahead* of a major crisis and, has the added benefit of achieving security, safety, and stability goals during peace time.[37]

ALWAYS VIGILANT FOR AMERICA: CIVIL AIR PATROL

The Civil Air Patrol (CAP) dates to 1941, when Gill Robb Wilson, a World War I aviator launched a program he had dedicated his post-war years to designing: the Civil Air Defense Services (CADS).[38] In the end, CADS was approved by the Commerce, Navy, and War Departments in November, and the newly dubbed CAP opened its national headquarters on December 1, 1941. As an organization, CAP provides a model for what an American civilian cyber defense program could look like. CAP offers its members a way to serve the nation without joining the military, and a CCD can do the same.

As an all-volunteer organization that educates young individuals and trains the next generation of aviation leaders, CAP is committed to service and development. Science, technology, engineering, and math (STEM) education is considered its capstone mission, and CAP has invested heavily in STEM initiatives since the organization's beginning.[39] Additionally, emergency preparedness and response are central to CAP's mission, as evidenced by its critical imagery collection of Ground Zero after 9/11.[40]

Organized like the U.S. Air Force (USAF), CAP provides a military leadership structure that promotes accountability and ensures that the CAP mission, values, and goals are supported by its affiliated chapters. The link to the military chain-of-command allows for a set of detailed and understandable consequences for any individual who breaks rules or regulations. It is especially critical to CAP's legitimacy that it remains accountable and transparent—as it receives federal funding for its programs and is a part of the USAF's operational mission. The oversight provided by a congressionally mandated program is important for at least two reasons. First, it guarantees that the CAP and all its local units are aligned with national priorities by synchronizing efforts across state lines. Second, congressional oversight helps ensure that citizens' groups act within the confines of the law.

The principles that shape CAP's relationship with the USAF—such as volunteerism and saving lives—provide a framework for nesting a CCD under the leadership of the newest branch of service, U.S. Space Force, which does not have a reserve or auxiliary component. While CAP already designates funding and efforts to STEM and cyber education, a dedicated CCD can take the CAP model and expand on its STEM mission to bring in a broader range of cybersecurity professionals, veterans, and businesses to help construct a dynamic cybersecurity ecosystem within the U.S. CCD's vision. Developing this infrastructure would help to bring cybersecurity awareness to the American public and promote responsible digital citizenship.

A SPACE MAP: CREATING A CIVIL AIR PATROL FOR CYBERSPACE

The principles that shape CAP's relationship with the USAF provide a framework for nesting a CCD under the leadership of a military branch. To create regionally and community aligned volunteer units, the CCD should be the Space Force Auxiliary Force. Aligning the CCD under Space Force would give the organization clear funding lines and pre-existing oversight mechanisms and, since the successful CAP model already exits, policymakers should be optimistic about the CCD concept too. Further, while aligning a CCD to U.S. Cyber Command (USCYBERCOM) may seem more natural, Space Force recruited its current members from the highly technical branches of the pre-existing military services - all of which also comprise the jointly staffed USCYBERCOM. Furthermore, with the Triad concept,[41] Space Force has started working closer with USCYBERCOM and U.S. Special Operations Command (USSOCOM) to defend in and across domains. As such, situating the CCD within Space Force reserve's component would develop a network of cooperation that could cross domains and Services. Ultimately, placing the CCD under Space Force oversight would integrate it into a highly technical service with a streamlined, singular line of authority, avoiding the potential for a cumbersome and financially contentious bureaucratic structure.

Oversight is important for at least two reasons. First, it guarantees that the CCD, and all its local chapters, are aligned with national priorities by synchronizing efforts across state lines. Second, a military hierarchy allows for the establishment and enforcement of parameters couched within legal confines to prevent citizens' groups from turning into localized cyber militias. While we do not deny that the U.S. government (USG) will have to accept additional risk by adopting the CCD model, we also hold that embedding the CCD within the Space Force hierarchy will manage that risk. By operating within the military framework, there will be greater control over the activities of citizen groups, reducing the potential for them to evolve into localized cyber militias. When thinking through the risk calculus for a CCD program, policymakers must weigh the risk of *not doing anything* versus the risk of utilizing non-military citizens to aid in national defense.

Beyond providing oversight, tying the CCD to DoD, and specifically to Space Force, makes sense for at least three additional reasons. First, just as with the Estonian model, the CCD offers everyday citizens a chance to give back to their nation. Many seek out alternative service opportunities, like AmeriCorps or the Peace Corps, and the CCD will provide another service option for cyber-skilled individuals to use their talents for the benefit of national defense. For these individuals, tying the CCD to a military service will help replicate the unique *esprit de corps* found in the armed forces, and may provide a powerful incentive to join the CCD. Additionally, veterans of the armed forces with cyberspace experience will be an important asset for CCD regional teams. As skilled individuals cycle out of uniformed service, the CCD will provide them an opportunity to continue their work of defending the nation and to experience a camaraderie with like-minded volunteers.

Second, alternative agencies, such as the Cybersecurity and Infrastructure Security Agency (CISA), are already under-resourced. Not only is Space Force's proposed government fiscal year 2022 budget nearly an order of magnitude larger than CISA's,[42] Space Force also has more than five times the personnel.[43] To date, Space Force does not have a reserve or auxiliary component, something experts have argued is essential for future national security.[44] It is in the Space Force's interest to keep its highly skilled workforce, and particularly its officers leaving active duty, in a part-time status to retain their skills. USCYBERCOM and all cyber-trained military service members are likewise valuable assets that USG is trying to retain. A CCD could address the persistent issue of talent attrition and brain drain that cyber-focused military roles and government entities face, as outlined in the Cyberspace Solarium Commission's report.[45] A CCD is necessary to provide both a way for separating personnel to continue to serve and can provide the Space Force with critical civilian experience.

Third, DoD is uniquely positioned to provide a far larger amount of on-the-job professional training and education than any other USG department or agency.[46] This capability is essential given the large variation in backgrounds and skillsets a volunteer organization like a CCD will attract. Professional education and training can help ensure that all volunteers, despite diverse backgrounds and skillsets, possess a common knowledge base. It can also help further instantiate *esprit de corps* and help educate members on the importance of accountability and their obligations to the organization. Cybersecurity and IT-related certifications are expensive when not provided by employers and CCD will be an avenue for professionals to gain and maintain key certification credentials and help build a more cybersecurity-educated public. Finally, CAP trains, mentors, and provides its members and cadets with an opportunity to serve their community, state, and nation and, a CCD can do the same for technology professionals.

Using CAP as a model, a CCD will provide cyber-focused community education and emergency response efforts by recruiting a broad range of cybersecurity professionals, veterans, and businesses to help foster a more robust cybersecurity ecosystem within the U.S. The CCD's vision should be to bring cybersecurity awareness to the American public to ensure that every citizen is also a responsible digital citizen and every business, and local government, is a secure one. To achieve that vision, the CCD should capitalize on CAP's community-oriented approach to training, education, and security. Critically, the volunteer nature of the CCD does not mean the units will be staffed by amateurs – like CAP, with its skilled pilots and alternatively skilled, but equally essential, supporting positions, the CCD will be a group of volunteers dedicated to the collective cybersecurity of the U.S. and comprised of technical experts, cadets and students, and community members interested in supporting CCD's mission.

CYBERSECURITY IS A SHARED RESPONSIBILITY: CIVILIAN CYBER DEFENSE

As a program modeled on CAP, the CCD will be a congressionally chartered, federally supported non-profit corporation that serves as the official civilian auxiliary of the U.S. Space Force and will be established as an organization by Title 10 of the United States Code with its duties, roles, and responsibilities detailed by legislation. A key tenet of the CCD is educating the public on cybersecurity and how to recognize and manage attacks and vulnerabilities. Importantly, CCD members will not require security clearances as they will not be using or accessing critical systems. Any abnormalities or vulnerabilities would be reported, potentially to CISA, to enhance the nation's overall cybersecurity posture by informing federal-level entities about cyber threats at the local level and by engaging in two-way sharing. The focus of the organization will be on resiliency, response, and rebuilding with a strict mandate to advise, educate, and remediate.

As a volunteer organization, a CCD will seek to influence cybersecurity awareness, beginning at the local levels – from the individual to the small businesses that make up American communities. And, due to its local focus, the CCD would have a natural affinity to other civic minded groups. These groups, in addition to their local concerns, are passionate about teaching people. The CCD can leverage those connections and provide seminars on improving cybersecurity and understanding cyberspace risk. Partnering with local chapters of organizations like the Neighborhood Watch, Rotary, Toastmasters, Chamber of Commerce, Veterans of Foreign Wars, and others, would enable a CCD to deliver education in STEM and cyber-related issues to increase awareness and digital literacy skills among professionals, seniors, and youth.

Emergency preparedness and response is another central tenet – a CCD could leverage its local resources and talent to aid in the rebuilding of systems and advise on defensive measures. Advising local businesses, assisting school and education systems wanting to establish or improve cybersecurity baselines, better protect student data, and working to deter attacks like ransomware, are all services an all-volunteer auxiliary service could provide. Should these proactive efforts not suffice, local individuals and organizations could also activate their local branch of the CCD to help them remediate and report cyberattacks. Like its CAP counterpart, the CCD will be a critical component of emergency response by helping to restore services and provide networks in the event of a natural or physical disaster.

As alluded to throughout this article, a CCD, like an Estonian CDL, would be a local organization. This has several benefits. First, it gains trust with the local community. In fact, ideally, members of the CCD would come from the communities they serve. Local participation is important as it allows the CCD to access users like a small business owner who may not welcome government assistance. Rather, by having someone from the community who may know the person experiencing a cybersecurity issue, there is a higher likelihood that the person requesting support will be open to CCD help or more likely to ask for help when needed, which could raise overall awareness of cybersecurity issues across all levels of government and provide policymakers with a clearer picture of the threat landscape. Moreover, once the CCD member is accepted into the social space of the person requesting support, they can educate them further on their individual role in providing collective cyberspace security. As research has noted, individuals are more likely to trust information from people they know and trust already.[47]

CONCLUSION

U.S. adversaries have mastered how to operate in the gray zone and are consistently conducting operations in and through cyberspace that fall below the threshold of armed conflict.[48] Despite the large number of cyberattacks that target private and small businesses, the USG remains risk-adverse to involving the public in defending the nation in cyberspace. Meanwhile, adversaries employ their own civilian actors within cyberspace and continue to impose cost.[49] The U.S. has been slow to respond to this evolving landscape because its traditional framework does not adequately account for this gray zone or persistent competition. However, by adapting and creating the CCD and incorporating it into the national defense strategy it will enhance domestic resilience in the face of cyber threats and bring the U.S. closer to developing a more effective cybersecurity ecosystem to address the challenges posed by constant competition in cyberspace.

This article does not advocate for allocating offensive capabilities or authorities to a civilian cyber force,[50] rather encourages policymakers to consider the benefits of a CCD to community cyber response efforts as part of a national defense.[51] The CCD's focus would include providing localized cybersecurity resilience and response resources, educating citizens on cyberspace risk and cyber hygiene, and other education and resilience focused programs designed to elevate cybersecurity awareness and knowledge. Because U.S. adversaries directly target private citizens, businesses, and local governments, we are engaged in an undeclared conflict in cyberspace and to effectively respond, the American public needs to be involved.

The CCD's actions collectively amount to a localized defensive effort to deny an adversary access to our systems and networks. CCD efforts also would be scalable and reactionary in times of national need. Moreover, since the CCD would be a civilian auxiliary force focused on building community resiliency, its work would be unclassified, allowing for a broader and more diverse membership. The U.S. should use citizen volunteers to defend (and report) in cyberspace to augment its broader strategic-level efforts and bridge the public-private divide. With CCD support at the local and community levels, the U.S. military and other national-level cyber assets can focus their concern on achieving strategic objectives.

Acknowledging that the American public needs to be involved in cybersecurity for national defense is a crucial first step toward developing a holistic cybersecurity ecosystem and resilient civilian network. A robust and layered cybersecurity strategy requires citizen engagement and participation. The U.S. must think unconventionally about who can, and should, defend the nation and get *everyone* involved in securing cyberspace. It is time for a Civil Cyber Defense.

NOTES

1. Nicole Perlroth, "The Chinese Hackers in the Back Office," *The New York Times*, June 11, 2016, https://www.nytimes.com/2016/06/12/technology/the-chinese-hackers-in-the-back-office.html.
2. Ibid.
3. Jeff Bell, "Small Business Cybersecurity 101: Simple Tips to Protect Your Data," *Forbes*, June 14, 2021, https://www.forbes.com/sites/forbestechcouncil/2021/06/14/small-business-cybersecurity-101-simple-tips-to-protect-your-data/.
4. Ibid.
5. David Blisson, "The State of Small Business Cybersecurity in 2021," *Security Intelligence*, May 20, 2021, https://securityintelligence.com/articles/state-small-business-cybersecurity-2021/.
6. Jason Johnson, "6 Security Challenges Facing SMEs Heading Into 2021," *InformationSecurityBuzz*, December 11, 2020, https://informationsecuritybuzz.com/6-security-challenges-facing-smes-heading-into-2021/.
7. Andrew Peterson, "Why Wall Street is worried about state and local government cybersecurity," *The Record*, https://therecord.media/why-wall-street-is-worried-about-state-and-local-government-cybersecurity/.
8. Andrew Peterson, "Why Wall Street is worried about state and local government cybersecurity," *The Record*, https://therecord.media/why-wall-street-is-worried-about-state-and-local-government-cybersecurity/.
9. U.S. Small Business Administration. "Stay safe from cyber threats" 2021, https://www.sba.gov/business-guide/manage-your-business/stay-safe-cybersecurity-threats.
10. Paola Peralta, "Small businesses are leaving themselves vulnerable to cyber attacks," May 3, 2022, *Employee Benefit News*, https://www.benefitnews.com/news/small-businesses-arent-investing-in-cybersecurity.
11. Peter High. "Lessons From The Most Digitally Advanced Country In The World." *Forbes*, January 15, 2018.
12. Sharon Cardash, Frank Cilluffo, and Rain Ottis. "Estonia's cyber defence league: A model for the United States?" *Studies in Conflict & Terrorism* 36, no. 9 (2013): 777-787.
13. Samuel Stolten, "Estonian president calls for more NATO troops to defend against Russia threat," January 13, 2022, Politico, https://www.politico.eu/article/estonian-president-calls-for-more-nato-troops-to-defend-russian-threat/.
14. Kevin Kohler, "Estonia's National Cybersecurity and Cyberdefense Posture." *Center for Security Studies (CSS) at ETH Zurich*, September 7, 2020, https://css. ethz. ch/en/services/digital-library/publications/publication. html/2dd8caf3-6741-435b-8b4d-a4df92e67bcb.
15. Kevin Kohler, "Estonia's National Cybersecurity and Cyberdefense Posture." *Center for Security Studies (CSS) at ETH Zurich*, September 7, 2020, https://css. ethz. ch/en/services/digital-library/publications/publication.html/2dd8caf3-6741-435b-8b4d-a4df92e67bcb.
16. Kaitseliit, "Estonian Defence League," https://www.kaitseliit.ee/en/edl.
17. Nasser Abouzakhar, ed., "ECCWS2015-Proceedings of the 14th European Conference on Cyber Warfare and Security 2015: ECCWS 2015." *Academic Conferences Limited*, 2015.
18. Sharon Cardash, Frank Cilluffo, and Rain Ottis. "Estonia's cyber defence league: A model for the United States?" *Studies in Conflict & Terrorism* 36, no. 9 (2013): 777-787.
19. Viljar Veebel, Illimar Ploom, Liia Vihmand, and Krzystof Zaleski. "Territorial Defence, Comprehensive Defence and Total Defence: Meanings and Differences in the Estonian Defence Force." *Journal on Baltic Security* 6, no. 2 (2020).
20. Kadri Kaska, Anna-Maria Osula, and Jan Stinissen, "The cyber defence unit of the Estonian defence league: Legal, policy and organisational analysis." 2013, *NATO Cooperative Cyber Defence Centre of Excellence*, https://ccdcoe. org/sites/default/files/multimedia/pdf/CDU_Analysis.Pdf.
21. Sharon Cardash, Frank Cilluffo, and Rain Ottis. "Estonia's cyber defence league: A model for the United States?" *Studies in Conflict & Terrorism* 36, no. 9 (2013): 777-787.
22. Greg Austin, ed., National cyber emergencies: The return to civil defence. *Routledge,* 2020.
23. Monica Ruiz, "Establishing volunteer US cyber defense units: A holistic approach." In 2017 *International Conference on Cyber Conflict* (CyCon US), pp. 45-58. IEEE, 2017.
24. Sharon Cardash, Frank Cilluffo, and Rain Ottis. "Estonia's cyber defence league: A model for the United States?" *Studies in Conflict & Terrorism* 36, no. 9 (2013): 777-787.
25. Monica Ruiz, "Establishing volunteer US cyber defense units: A holistic approach." In 2017 *International Conference on Cyber Conflict* (CyCon US), 45-58. IEEE, 2017.

NOTES

26. Viljar Veebel, Illimar Ploom, Liia Vihmand, and Krzystof Zaleski. “Territorial Defence, Comprehensive Defence and Total Defence: Meanings and Differences in the Estonian Defence Force.” *Journal on Baltic Security* 6, no. 2 (2020).
27. Ģederts Ģelzis, “Estonian voluntary cyber-soldiers integrated into national guard.” *Deutsche Welle,* May 4, 2011.
28. Ruiz, "Establishing volunteer US cyber defense units: A holistic approach," 5-58. IEEE, 2017.
29. Ibid.
30. Viljar Veebel, Illimar Ploom, Liia Vihmand, and Krzystof Zaleski. “Territorial Defence, Comprehensive Defence and Total Defence: Meanings and Differences in the Estonian Defence Force." *Journal on Baltic Security* 6, no. 2 (2020).
31. Tom Gjelten, “Volunteer cyber army emerges In Estonia.” National Public Radio (4 January 2001), http://www. npr.org/2011/01/04/132634099/in-estoniavolunteer-cyber-army-defends-nation (2011).
32. Monica Ruiz, “Is Estonia’s Approach to Cyber Defense Feasible in The United States?” *War on the Rocks*, January 9, 2018.
33. Ruiz, “Establishing volunteer US cyber defense units: A holistic approach," 45-58. IEEE, 2017.
34. Ibid.
35. Viljar Pernik and Emmet Tuohy. “Interagency Cooperation on Cyber Security: The Estonian Model.” In *Effective Inter-Agency Interactions and Governance in Comprehensive Approaches to Operations*, NATO STO Symposium Proceedings AC/323 (HFM-236) TP/579. 2014.
36. Viljar Veebel, Illimar Ploom, Liia Vihmand, and Krzystof Zaleski, "Territorial Defence, Comprehensive Defence and Total Defence: Meanings and Differences in the Estonian Defence Force.” *Journal on Baltic Security* 6, no. 2 (2020).
37. Eneken Tikk, “Civil defence and cyber security: A contemporary European perspective.” In *National Cyber Emergencies*, 76-92. Routledge, 2020.
38. Civil Air Patrol, “History of Civil Air Patrol,” https://www.gocivilairpatrol.com/about/history-of-civil-air-patrol
39. Legal Information Institute, “36 U.S. Code § 40302 - Purposes,” https://www.law.cornell.edu/uscode/text/36/40302.
40. Jim Moore, “The Only Skyhawk in The New York Sky,” *AOPA*, September 10, 2020, https://www.aopa.org/news-and-media/all-news/2020/september/10/the-only-skyhawk-in-the-new-york-sky.
41. Jen Judson, “Army Space, Cyber and Special Operations commands form ‘triad’ to strike anywhere, anytime.” *Defense News*, August 11, 2022, https://www.defensenews.com/smr/space-missile-defense/2022/08/11/army-space-cyber-and-special-operations-commands-form-triad-to-strike-anywhere-anytime/.
42. Maggie Miller, “House Lawmakers Propose Major Budget Increase for Key Cyber Agency.” *The Hill*, June 29, 2021; Pope, Charles. “FY22 Budget Gives Air & Space Forces the Strength to meet Threats, Roth, Brown, Raymond Tell Senate.” *Space Force News*, June 8, 2021.
43. Eric Geller, “Senate Confirms Jen Easterly as Head of U.S. Cyber Agency.” *Politico*, July 12, 2021; Pope, Charles. “Space Force selects more than 900 personnel to transfer FY22.” *Space Force News*, September 30, 2021.
44. Brent Ziarnick, “An aggressive Space Force begins with a Space Force Reserve,” *The Hill*, May 5, 2020, https://thehill.com/opinion/national-security/494796-an-aggressive-space-force-begins-with-a-space-force-reserve.
45. Cyberspace Solarium Commission, 2020. US Cyberspace Solarium Commission Final Report.
46. Barnett Koven and Katy Lindquist, *Barriers to Special Operations Forces-Led Counterterrorism Effectiveness.* Joint Special Operations University Press. 2021.
47. Roderick Kramer. “Rethinking Trust.” *Harvard Business Review*, June 2009.
48. Joseph Votel, Charles Cleveland, Charles Connett, and Will Irwin. "Unconventional warfare in the gray zone.” *Joint Forces Quarterly* 80, no. 1 (2016): 101-109.
49. Mark Grzegorzewski and Chris Marsh. “Incorporating the Cyberspace Domain: How Russia and China Exploit Asymmetric Advantages in Great Power Competition.” *Modern War Institute,* March 15, 2021.
50. Wilson VornDick. “From Minutemen to Byteforce: Unleash an American Cyber Auxiliary & App,” *19fortyfive*, June 29, 2021, https://www.19fortyfive.com/2021/06/from-minutemen-to-byteforce-unleash-an-american-cyber-auxiliary-app/.
51. U.S. Department of Defense. “Department of Defense Law of War Manual.” Accessed September 14, 2021. https://dod.defense.gov/Portals/1/Documents/pubs/DoD%20Law%20of%20War%20Manual%20-%20June%202015%20Updated%20Dec%202016.pdf?ver=2016-12-13-172036-190.