SESSION

5

Defense Support to the Private Sector

New Concepts for the DoD's National Cyber Defense Mission

Jason Healey
School of International and Public Affairs
Columbia University
New York City, New York, United States

Erik B. Korn
Army Cyber Institute
U.S. Army
West Point, New York, United States

ABSTRACT

A primary mission of the Department of Defense (DoD) remains defending the nation in cyberspace, a function which has until this point has been oriented around the traditional Defense Support of Civil Authorities (DSCA) framework. However, conceptual confusion as to the most effective mechanisms for DoD support during national cyber emergencies has generated a perpetual "fog" that restricts the frameworks optimal employment. This paper examines the typical forms of DoD cyber support currently employed, and presents four additional pillars for consideration. These proposed pillars highlight the potential value of the DoD's defined role and functionality as a supporting command to the private sector during national cyber emergencies. Furthermore, this paper recommends new, adaptable structures and defined roles that can serve as a model for the DoD's future composition, disposition, and employment in cyberspace when called upon to defend the nation. Because the private sector is on the front lines of the conflict, a new model of Defense Support to the Private Sector (DSPS) needs consideration.

Keywords– Department of Defense, U.S. Cyber Command, Defense Support of Civil Authorities, Supported Command, Supporting Command, Dowding System, Persistent Engagement, Defensive Cyber Operations Response Action.

I. INTRODUCTION

The DoD has a central mission to "defend the nation" in cyberspace, a mission which has focused on DSCA, and rightly so. After all, almost all cyberattacks are not attacks on the nation, so the Department of Homeland Security (DHS) will often have the lead. It is homeland security, not homeland defense.

But the DoD has significant capability and is regularly called in to provide support. The four main pillars of such DoD support are relatively well known: information sharing and collaboration; "away teams" and other post-incident support to U.S. critical infrastructure companies which have been attacked; counteroffensives to disrupt adversary operations against the United States; and the direct monitoring and defense of networks belonging to U.S. critical infrastructure companies. These types of support are not often so clearly described and, while the first two are relatively straightforward, the last two are controversial.

This paper examines these typical forms of support and takes on the conceptual confusion that surrounds the defense of the Nation. Much of the confusion comes from scenarios that are not sufficiently extreme, so that the roles of DHS and the DoD are still intertwined. To break out of this grey conceptual fog, it is necessary to imagine, as a thought experiment, the role of the DoD in the conceptual clarity of a black-and-white scenario of a true cyber war targeting the private sector, and then work down from there into the fog. Treating the DoD role in such a cyber war as "support to civilian authorities" is missing the point, as the military would have a direct role in fighting the adversary. In addition, civil authorities do not need support, but the private sector does. Given that the private sector is not just the main target of the adversary, but has significant capabilities of its own, the DoD role in defending the Nation is in many ways the "supporting command." This method suggests four additional pillars of support: private-sector call for fire support, coordination of multi-stakeholder defensive actions, response-support forces, and private-sector access to the entire intelligence cycle. Together, these can be a new approach: "Defense Support to the Private Sector" (DSPS).

II. DEFENSE SUPPORT OF CIVIL AUTHORITIES (DSCA)

> "[D]uring a natural disaster, like a hurricane, military troops and helicopters are often used by ...[the Federal Emergency Management Agency] to help deliver relief. In a similar vein, the military's cyber capabilities will be available to civilian leaders to help protect the networks that support government operations and critical infrastructure. As with all cases of military support to civilian authorities, these resources will be under civilian control and used according to civil laws"[1].
>
> –Then-Deputy Secretary of Defense William J. Lynn III

The cyber response is only part of the larger National Response Framework (NRF), a whole-of-nation approach for unified response actions for emergencies and natural disasters, of DHS's Federal Emergency Management Agency (FEMA). The NRF is the central strategy for local, state, tribal, private, and federal entities in conducting joint operations during national emergencies[2]. The DoD is specified in the NRF as a resource authorized for commitment to domestic emergencies upon approval of the secretary of defense or when directed by the president[3]. The NRF is primarily for physical emergencies, like hurricanes or earthquakes, while the National Cyber Incident Response Plan (NCIRP) is only for cyber incidents (an incident which had both

cyber and physical consequences would invoke both—one reason why DHS is a natural choice for national incident response).

Federal Government cyber response is centered on DHS, which has the statutory mission of ensuring cybersecurity through a better understanding of the U.S. risk posture and "reducing or mitigating vulnerabilities, threats, and the potential consequences from cybersecurity incidents"[4]. Per Presidential Policy Directive (PPD) 41 from 2016, DHS is the nominated lead for "asset response activities" (as compared to investigative and intelligence activities, which are the responsibility of the Federal Bureau of Investigation (FBI) and the Office of the Director of National Intelligence, respectively) and oversees the bulk of the federal response to cyber incidents of national significance[5]. When a "significant cyber incident affects critical infrastructure owners and operators" and may "reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security," the government forms a Cyber Unified Coordination Group (UCG) as "the primary method for coordinating between and among Federal agencies in response to a significant cyber incident as well as for integrating private-sector partners into incident response efforts"[6]. Though PPD-41 does not mention the DoD, it would participate in a Cyber UCG as an additional participant.

The NCIRP defines the various responsibilities, capabilities, and coordination efforts for a national response to cyber incidents and, unlike PPD-41, explicitly details DoD responsibilities in the event of a national cyber incident[7]. Securing the DoD Information Network and civil authorities' organic assets is a primary responsibility, but the NCIRP also includes details on providing support to civil authorities when requested to do so through lead federal agencies or when directed to do so by the president[8]. These supporting structures are just a few of the resources that manage the civil-military support relationship in times of national crisis. Of course, the DoD has significant capabilities for responding to cyber incidents, not least of which are those at U.S. Cyber Command (USCYBERCOM) and the National Security Agency (NSA). One of the DoD's key missions is for it to "be prepared to defend the United States and its interests against cyberattacks of significant consequence"[9].

Since DHS has the overall lead, the DoD's cyber defense of the Nation is typically rooted in the larger framework of DSCA. There are a variety of authorities, joint doctrine publications, and federal response plans that oversee the support relationships among the DoD, civil authorities, and industry during disasters. The DoD maintains an inherent role in bolstering civil authorities during national emergencies as well as the responsibility to provide necessary support in the event of a domestic emergency. The Stafford Act and Economy Act constitute a legislative structure that provides state governments and federal agencies a mechanism with which to request DoD support when organic capabilities and resources become overwhelmed during an emergency[10]. U.S. Code (U.S.C.) also specifies authorities for the support relationship between the DoD and civilian entities. Specifically, Title 32 and Title 10 directly permit DSCA, an affiliation generally characterized by DoD reinforcement of civilian entities in response to "domestic emergencies, law enforcement support, and other domestic activities"[11].

This legislative foundation has been further developed with joint military doctrine such as Joint Publications (JP) 3-27, "Homeland Defense," and JP 3-28, "Defense Support of Civil Authorities," as well as previously mentioned federal response action plans like DHS's NRF and NCIRP. JP 3-27 explains the different roles of the responsible commands and clarifies the missions of homeland security, homeland defense, and DSCA; homeland defense involves "defending against traditional external threats or aggression...and against external asymmetric threats" that are outside the scope of homeland security and related DSCA tasks[12].

During DSCA operations, the military typically assumes a supporting role that is subordinate to the designated lead federal department or agency[13]. Titles 32, 10, and 14 of the U.S.C. sanction support from the National Guard, active duty forces, and the United States Coast Guard in the event of national emergencies[14]. DoD Directive 3025.18 further expands on the DSCA request process in accordance with sections 1521, 1535, and 9701 of U.S.C. Title 31[15]. JP 3-27 also further stipulates additional guidance for joint operations in support of homeland defense.

III. CURRENT PILLARS OF DEFENSE SUPPORT

Despite the general strength of the DSCA framework, according to a panel at a 2018 strategy symposium run by USCYBERCOM, "there is little consensus on what it means to defend the Nation and its interests in cyberspace, or on what role the Department of Defense should be for this mission"[16]. Just how should the DoD and USCYBERCOM go beyond DSCA for homeland defense?

There have been four main pillars of support: information sharing and collaboration; "away teams" and other post-incident support to U.S. critical infrastructure companies which have been attacked; counteroffensives to disrupt adversary operations against the United States; and direct monitoring and defense of networks belonging to U.S. critical infrastructure companies. The first two are far more straightforward than the last two, and there are actually far more ways that the DoD can defend the Nation, as this paper discusses in the next section.

A. Information Sharing and Collaboration

DoD efforts (such as the Enduring Security Framework) to share information on threats and vulnerabilities and collaborate with the private sector and other government agencies to reduce the threats and vulnerabilities have been important mechanisms. These operate at levels well below homeland defense and focus more on threat reduction before an event than response once an incident has begun[17].

B. Post-Incident Support

Perhaps the most-used mechanism is the DoD's support to other federal departments after a major incident occurs against (typically) a company that is part of the country's critical infrastructure. The FBI has Cyber Action Teams at all 56 of its field offices, which will "travel around the world" within 48 hours "to assist in computer intrusion cases"[18]. DHS also has

such "fly-away teams" that can deploy with the FBI for incidents which are not just crimes, but have a larger homeland-security nexus, such as attacks against major critical infrastructure companies[19]. DHS and the FBI somewhat routinely call in DoD capabilities to assist; in at least one case, when Google suffered a severe intrusion by China, it reached out directly to the NSA for a "secure tailored solution" which brought in the FBI and DHS[20].

C. Shooting Back

The DoD, of course, has unique authorities, beyond those of the FBI and DHS, and, when directed, "the U.S. military may conduct cyber operations to counter an imminent or on-going attack against the U.S. homeland or U.S. interests in cyberspace...to blunt an attack and prevent the destruction of property or the loss of life"[21]. The National Cyber Mission Teams were created for just this homeland-defense eventuality. Such an order, though, has rarely if ever been given, even during known attacks from nation-state adversaries, such as the 2012 distributed denial-of-service (DDoS) attacks by Iran against the U.S. financial system, when "the Obama administration rejected an option to hack into the adversary's network in Iran and squelch the problem at its source"[22]. As the next section will discuss, there is far more that can be done to develop this pillar.

D. Monitoring and Direct Response

General Keith Alexander, when he was Commander of USCYBERCOM, opined that "within the United States, I do not believe that's where Cyber Command should or will operate"[23]. However, he wanted to improve his ability to monitor and defend the banking sector by installing government "surveillance equipment on their networks" to detect attacks using NSA's "secret sauce" of threat signatures[24]. The plan did not proceed, though the idea of direct monitoring and protection of private-sector assets does live on in some corners. At the 2018 USCYBERCOM strategy symposium, one cyber general asserted that if companies "want to meet us halfway," they must agree to allow the military to monitor their networks, even when those companies spend hundreds of millions on cybersecurity[25]. Indeed, joint cyber doctrine opens the possibility that "National-level CPT [Cyber Protection Team] support can be extended to defend non-DOD mission partner or critical infrastructure networks when ordered" by the secretary of defense[26].

This most controversial of the pillars is worth additional exploration. On one hand, the DoD directly defends U.S. territory; on the other, cyberspace is not the same as physical territory, and it is not always clear that the DoD has the authority or even superior capabilities. Despite these limitations, it is often the default assumption of military cyber defenders that, to defend the Nation, they must take control of the assets themselves. For example, Mark Young in 2010 wrote, "there is little that the DoD could do if the attack came across a commercial network," but a national cyber doctrine and processes could smooth coordination with the private sector "when the networks to be protected by the Cyber Command belong to a commercial entity"[27].

These mechanisms could "address the concerns" of commercial network service providers "to allow a U.S. government organization, such as the Cyber Command, to operate on their networks" for defense purposes[28].

IV. EXPANDING DOD SUPPORT IN THE BLACK-AND-WHITE CLARITY OF CYBERWAR

There are several reasons it is hard to determine the appropriate role for the DoD in defending the nation in cyberspace. Identifying these reasons can help develop additional policy responses.

One of the most critical differences between cyber conflict and conflict in the air, land, sea, and space is that "it is non-state actors, not governments, which typically are decisive in cyber defense...[o]nly uncommonly are governments able to bring the superior resources of their unwieldy bureaucracies in enough time to decisively defend against attacks"[29]. Companies like Microsoft, Verizon, and FireEye have massive security budgets and tremendous agility and routinely change the "terrain" of cyberspace to stop attacks. They are overly burdened with deciding if they have the legal authority to conduct defensive measures; as private entities, they are permitted all which is not specifically restricted—the opposite of what applies to the U.S. Government.

Banks like JPMorgan Chase spend over $500 million on cybersecurity with complex networks[30]. USCYBERCOM only has a limited set of resources and experienced personnel, so it is not clear how it could effectively monitor such networks or help defend them, even if asked to do so. It is like defending a labyrinth: unless you are on the network for long periods of time, you do not know the terrain well enough to defend it. Fortunately, as will be argued shortly, it is not clear that USCYBERCOM's homeland defense mission depends on such on-site defense.

Another critical difference between cyber and conflict in the other domains is that there is constant contact between adversaries, creating an environment of "persistent engagement." Some of these incidents, such as Chinese commercial espionage or attacks on critical infrastructure like the finance sector, can be classified as major national security threats—and, indeed, President Barack Obama declared a "national emergency" to deal with them [31]. This can lead to the recommendation that since the DoD is the part of the Federal Government that deals with national security threats, it should be engaged now in the defense of critical infrastructure networks. Even when that recommendation is rejected (for reasons such as the DoD does not have enough capability to act so routinely and DoD presence is not wanted by the affected companies), the way out of the conceptual fog is usually framed from the bottom up: envisioning scenarios a bit (or a lot) worse than today's and then trying to determine the appropriate role for the DoD and its relationship to DHS and the private sector.

This approach can be useful, but only goes so far when caught up in a conceptual fog. As in any fog, turning up the high beams on your headlights only shows you more grey. In most scenarios that are based in some worse version of today, DoD and DHS authorities will still

be intertwined, and the private sector will still be hesitant regarding a lead role for the DoD. To break out of this grey conceptual fog, it is necessary to imagine the role of the DoD in the conceptual clarity of a black-and-white scenario of a true cyber war and then work down from there into the fog.

Treat this as a thought experiment only—perhaps such a cyber war is impossible—but, to set the scene, imagine that an adversary nation-state is using cyber capabilities to kill thousands of American citizens. More attacks are coming every day. What is the DoD's role in this obvious homeland-defense scenario?

Treating the DoD role in such a cyber war as "support to civilian authorities" is missing the point: "For most contingencies, the usual DoD role of support to civil authorities will apply. However, in the event of a high-end attack, the DoD will likely need to take the lead role"[32]. The republic is at war, and the American people and the president would expect the DoD to be at the forefront of defense. But in such high-tempo operations, USCYBERCOM will certainly not have the resources to deploy CPTs to defend specific critical infrastructure-sector companies; it will likely be having to use every last person to defend the DoD and the U.S. Government and take the fight to the enemy.

So what else can the DoD and USCYBERCOM do to help win in this cyber-war thought experiment? What might be part of a DSPS project? There are several different mechanisms that can enable the expansion of DoD defense of the Nation: private-sector call for fire support, coordination of multi-stakeholder defensive actions, response-support forces, and private-sector access to the entire intelligence cycle. In each case, these measures are not just useful for high-end cyber warfare, but far down into the grey-zone conflicts of today.

V. PRIVATE SECTOR CALLS FOR FIRE SUPPORT

As part of the cyber-war thought experiment, further imagine that the finance sector reports that cyberattacks will turn into a financial crisis unless specific adversary command and control (C2) servers are not attacked and taken offline in three hours.

In one sense, this is a normal Defensive Cyber Operations Response Action (DCO-RA) mission in which "actions are taken external to the defended network or portion of cyberspace without the permission of the owner of the affected system [which] may include actions that rise to the level of use of force, with physical damage or destruction of enemy systems"[33]. Yet there are currently no channels through which USCYBERCOM can receive such private-sector calls for fire or through which such calls can be validated. The banks collectively making the request through official channels are under direct attack by an adversary choosing to target the U.S. by attacking them online. They are the Forward Edge of the Battle Area of the war and their request for fires should be taken just as seriously as if it had come through a combatant command. In cyber conflict, the private sector is the supported command. This will prove much easier for sectors such as finance, which has hired many cyber veterans and has a formal governance structure to make official and time-sensitive requests.

There is already some evidence of such ties, though they are informal. The Financial Systemic Analysis & Resilience Center (FSARC) is sharing malware indicators and other information with USCYBERCOM where "this intelligence is independently evaluated and, if appropriate, Cyber Command *responds under its own unique authorities*"[34].

VI. COORDINATING MULTI-STAKEHOLDER DEFENSIVE ACTIONS

The DoD can work toward supporting the synchronization of defensive actions and establish a joint battle rhythm between the Federal Government, private-sector industries, and additional civil authorities. What might be needed is a cyber equivalent of the Dowding system, the British system for detecting inbound bombers during the Battle of Britain and providing direct defense[35]. The network of sensors, operations centers, and communications acted as a central nervous system for situational awareness of all available information and control defenses. However, in stark contrast to conflict in other domains, it may be the private sector which controls the main tempo, with the DoD supporting it.

In a notional, high-end cyber war, the current mechanisms for coordinating defensive actions would quickly become swamped. The DHS National Cybersecurity and Communications Integration Center (NCCIC) is the main operational coordination body, a "central location where a diverse set of partners involved in cybersecurity and communications protection coordinate and synchronize their efforts [and] coordinate national response to significant cyber incidents in accordance with the National Cyber Incident Response Plan"[36]. The NCCIC also connects with FEMA's NRF for cyber-physical incidents and coordinates with DoD operations centers, including USCYBERCOM. However, NCCIC has suffered persistent staffing and technical training issues, and would be challenged to work at the scale of a cyber war with many separate attack campaigns[37]. For example, when responding to just one past campaign, the Conficker worm, the DHS team not only played no decisive role, but, when it needed to brief the White House, simply used the slides of the private-sector, Microsoft-funded Conficker Working Group, substituted its own logo, "and classified it to boot"[38]. The DoD and USCYBERCOM may have better staffing and capabilities but would also have difficulty scaling quickly. They also do not have the visibility or connections with industry to coordinate the defense of private-sector networks.

There are already many private-sector response organizations. One presidential advisory committee composed of technology executives developed a report with a full set of recommendations for sector "mobilization" that notes that "the vast majority of enterprise incidents are resolved with the support and collaboration" of companies and trust groups, such as Network Service Provider Security (NSP-SEC) and information sharing and analysis centers[39]. Indeed, in most incidents:

> "[T]he fundamental incident management actions occurred through private sector collaboration or mobilization at a [small] scale, limited to a group of actors that had the technical competence and ability to develop and propose appropriate mitigations to address the core

vulnerability. This group is distinct from the affected community, which constitutes those end users with the responsibility for managing the actual manifestations of the consequences of the attack"[40].

The Federal Government simply has a less decisive role than non-states. Even as far back as the 2007 attacks on Estonia, NSP-SEC, "comprised of technical experts of various network provider companies," was sent to Estonia to help coordinate defensive efforts with international telecommunication carriers and "mitigated [these] down to fairly low levels over the course of the next seven hours"[41]. The spirit of the group focuses on immediate action: "If something needs to be taken down, it needs to be taken down, and there isn't time for argument ... that's understood upfront [within NSP-SEC]"[42]. Another alliance of technology companies, the Industry Consortium for Advancement of Security on the Internet, created a Unified Security Incident Response Plan (USIRP) for its membership (which includes Microsoft, CISCO, Intel, Amazon, and Oracle) so that they can "trigger a USIRP event; share critical information about it; and work together effectively on a coordinated response"[43]. The Cyber Threat Alliance coordinates responses between many threat intelligence teams, such as at Palo Alto Networks and CISCO, to generate a common threat picture[44]. Within the critical infrastructure sectors, there are many groups handling various aspects of response. Just the finance sector has three groups: FSARC, the Financial Services Information Sharing and Analysis Center (FS-ISAC, of which one of the authors has been vice chair), and the Financial Services Sector Steering Committee (FSSSC).

Cyber defense has long been recognized as a team sport or, rather, a multi-stakeholder effort, with distributed responsibilities. The main goal of the coordination of all of these defensive efforts as well as the integration of DCO-RA response missions and outright offensive attacks from the DoD is not unity of command centered on USCYBERCOM or NCCIC, but *unity of effort, unity of action*, and loose coordination to keep independent groups working toward the same goal. It may be counterproductive to insist that "clear chains of command for a high-end contingency...be established between the civil authorities and the DoD," or that "private sector cyber security expertise" should be "working under government direction and control in connection with high-end contingencies or in direct support to the ISPs [internet service providers] and grid operators"[45].

Unity of effort through multi-stakeholder coordination would mean that the DoD would not be able to synchronize offensive and defensive efforts as well as if it controlled them both, but this is a small loss to achieve better synchronization *across all* defense, in both the public and private sectors. Efforts to build such a multi-stakeholder Dowding system based on a unity of effort and support to the private sector would be useful at levels well below full cyber war.

The DoD (and the rest of the Federal Government) cannot and should not lead these efforts, but do need to support them. For example, in the "event an incident surpasses industry's mitigation ability," then "industry would want recommendations or direction on the priorities

for...recovery"—that is, a political decision on national security priorities[46]. Industry may also need a "comprehensive, legal, and operational framework," as it would be "operating on a catastrophic" footing, far beyond business as usual[47].

VII. SECTOR-WIDE RESPONSE—SUPPORT FORCES

During high-tempo cyber warfare against the United States, DoD CPTs deployed to directly monitor and protect private-sector networks would only get in the way. However, there may be a role for the DoD, possibly through a new kind of Cyber Support Team (CST), to support the private-sector response process, rather than helping to defend private-sector networks.

To return to the thought experiment of cyber warfare against the private sector, imagine again a massive attack against the finance sector. Sector-wide incident response is handled by groups such as FSARC, FS-ISAC, and FSSSC, typically on conference calls every few hours. These calls cover technical and intelligence issues (usually at the more operationally focused FS-ISAC) as well as top-level policy issues, such as whether the markets will be able to remain open (at the more senior FSSSC). Overwhelmingly, the same people on these calls handling sector-wide response are the same executives overseeing response within their own financial institutions. They are very thinly spread, with some limited 24/7 capability, and if an incident lasts more than a few days, the system may break.

One of the authors (Healey) led the coordination of these calls for the FS-ISAC. What could have been useful was a few, competent, company-grade or senior non-commissioned officers to give more organizational depth and staying power to the response. These officers could help run the response playbook, keep track of the dozens of details needed for a successful response, and provide much-needed continuity and stability to the process. Such officers do not have to be highly trained DoD cyber ninjas and do not necessarily even need much knowledge of the affected sector (though these knowledge and skills could be useful). They only need to be capable responders—the kind of officers which exist in great numbers in all services.

VIII. PRIVATE-SECTOR ACCESS TO THE ENTIRE INTELLIGENCE CYCLE

Intelligence cooperation between the Federal Government and the private sector is improving—especially with more cleared individuals in critical infrastructure sectors and companies, which have hired former intelligence professionals—but it is still far behind the level which might be required in a notional cyber war. Too often, companies (even in key sectors) are only included at the tail end of the intelligence cycle—dissemination. They receive tear-line reports of declassified and watered-down reports. Sometimes, select executives are given a "special one-day, top-secret security clearance" which "scare[s] the bejeezus" out of them[48]. But with private-sector companies on the Forward Edge of the Battle Area, they should not just be receiving reports; they should be active in all phases of the intelligence cycle, especially in the submission of requirements for the collection and clarification of analysis and the provision of

feedback[49]. This would primarily be the responsibility of the Director of National Intelligence, but, as the NSA has had a lead role in such activities in the past, much would fall onto the DoD's shoulders, especially in wartime.

The downsides of this kind of support are obvious: there are currently few ways for a sector to validate any requests or feedback, few if any mechanisms for passing requests and feedback from the private sector, and a major gap between sectors in the sophistication of intelligence consumers. As with the potential support to calls for fires, the finance sector is perhaps a natural place to start, with many cyber and intelligence veterans and a formal governance structure in place.

IX. RECOMMENDATIONS: TO DEFEND THE NATION, SUPPORT THE PRIVATE SECTOR

The DoD possesses unique tools and resources for DSPS. However, large gaps remain.

A recent Government Accountability Office (GAO) report identified some of the challenges and shortcomings in the DoD's current approach and its application to cyberspace. Most glaringly, the report highlights a lack of definition in the DoD organizational roles and responsibilities for providing civil support during a national cyber incident[50]. The DoD's C2 guidance for cyber DSCA operations is highlighted as contradictory and confusing. Additionally, conflicting delineations for U.S. Northern Command and USCYBERCOM as the supporting command to civil authorities for cyber incidents further complicates DoD guidance[51]. With C2 being a primary component of effective military operations, the Pentagon's ability to streamline unity of command policies and processes is vital. Another area identified by GAO as a challenge is the DoD's visibility of capabilities within National Guard cyber units, a limitation that currently impedes timely and effective support to civil authorities[52]. Furthermore, GAO's recent findings of DoD delinquency in the maintenance of a repository of Guard capabilities for each state must be rectified quickly for this option to work effectively[53]. These deficiencies can be debilitating and limit the DoD's ability to provide support to industry and civil authorities in cyberspace.

In order to best leverage DoD cyber capabilities, the Pentagon must go even beyond these recognized gaps and recognize a new role as a supporting command to the non-state actors on the front lines of defending the Nation in cyber conflict. One important early step, highlighted by several former defense and intelligence officials, is to incorporate "establishing and exercising the procedures necessary" for cooperation for high-end crises into the memorandum of understanding between the DoD and DHS[54]. Likewise, the National Security Telecommunications Advisory Committee report on mobilization has several recommendations, which we support, including the identification and organization of the correct public- and private-sector entities, and then conducting training and exercises "to ensure the Nation is prepared to manage a cyber-related event of national significance"[55].

An important capability for expanded support is Reserve and Guard cyber units. The DoD's decision to fully invest in these units and their often-unique capabilities and authorities can provide a force able to build closer relationships among government, civil authorities, and industry. The individuals in these units also typically work in various sectors of industry or with other civilian entities on a daily basis. When operating under U.S.C. Title 32 at the direction of state governors, Guard cyber teams provide a unique flexibility in supporting civil authorities and sectors of industry (and are not subject to the restrictions of the Posse Comitatus Act—legislation that limits military units from operating domestically, such as working with law enforcement)[56]. In order to address civil authority support, the DoD has already worked with the Council of Governors on the establishment of the Joint Action Plan for State-Federal Unity of Effort on Cybersecurity, which provides a collaborative framework to "expedite and enhance the nation's response to cyber incidents" through collaboration, information sharing, capabilities, and resources[57].

The Army National Guard and the Air National Guard have partnered to ensure cyber-team coverage of all 10 FEMA response regions to better integrate with DHS efforts and to help counter large-scale domestic cyber emergencies[58]. This idea should be extended, with a Guard or Reserve team working with each critical infrastructure sector. For example, the Air Force Reserve or Air National Guard might work with the energy sector, as many Air Force cyber assets are in Texas, and the Army might work with the finance sector, as the Army Cyber Institute is just north of Manhattan. Each unit would be a CST, hopefully, composed of officers and enlisted personnel from the supported sector. Each unit could assist with some of the additional support pillars mentioned in this paper: developing processes for calls for fire, backstopping responses, assisting with intelligence requirements, and being better consumers of intelligence. There are some advantages, mostly in simplicity, to these CSTs being run by a single service, though, given the likely lack of qualified people, making them joint (with perhaps a single service as the lead) may make them stronger.

USCYBERCOM has created new joint headquarters for many specialized purposes, from defending its own networks to attacking those of the Islamic State of Iraq and Syria. A new, modestly sized, joint task force or joint forces headquarters might be created solely to support the private-sector fight and, to a lesser degree, work with civil authorities on homeland defense[59]. As the parent command of the Guard and Reserve teams, it would support each sector, with responsibilities to improve operational coordination for high-end cyber incidents and warfare, though it would not conduct response actions itself. Such a headquarters might be largely staffed with Reserve and Guard personnel and located in the San Francisco Bay or Seattle areas to better coordinate with technology companies that control the high ground of cyberspace.

Regardless of whether the DoD creates new units for this purpose, it must make progress on these additional support pillars as well as help create the framework to support a cyber Dowding system. As the finance sector is perhaps the most mature, for the reasons mentioned above,

the DoD should extend its current efforts with that sector, starting with an informal discussion (including DHS and the Department of the Treasury) on how the sector might call for fire from USCYBERCOM, should that ever be required. This can serve as a basic model for the other sectors, especially those with strong governance mechanisms.

One way to support the idea of a cyber Dowding system is for the DoD to encourage, and perhaps match, DHS grants to create new organizations dedicated not to sharing information, but collaborating to respond to each kind of major incident. The goal of these Cyber Incident Collaboration Organizations (CICO) is to streamline the current response process for an incident type to provide an umbrella for making such work easier at a larger scale. As one of us wrote earlier this year:

> "A Counter-Malware CICO could be built, using the lessons learned from the Conficker Working Group, for a faster, more effective response to such incidents. A Counter-Botnet CICO would be similarly global and led by the private sector, with membership including the global organizations that have had the largest role in takedowns—such as, say, Microsoft, FireEye, and the Department of Justice. The Counter-DDoS CICO would bring together the global Tier 1 service providers, content-distribution managers, and other organizations that focus on the core Internet infrastructure … By comparison, the Counter-APT CICO might be led and funded by the U.S. government, working with the "Five Eyes" partners…and, perhaps, with representation from the Defense Industrial Base and key cybersecurity companies. Much of its work would be classified."

Such CICOs, or similar organizations, would make the multi-stakeholder response much easier at scale, both simplifying and clarifying the role of USCYBERCOM and the larger Federal Government.

The DoD has the necessary capabilities, resources, and forces for DSPS. To achieve an effective response to domestic cyber emergencies, the Pentagon will need to understand how it can best bolster these entities as a supporting command when the call for reinforcements is received. Expanded areas of support can include core military functions, such as intelligence, C2, defensive actions, and calls for fire. The question now is whether the DoD can seize these opportunities to provide more effective support functions during significant cyber events, or if it will fall back into the trap of institutional norms where it feels compelled to take the lead.

ACKNOWLEDGMENT

The authors would like to acknowledge Divyam Nandrajog and Augusta Grondquist for their research help and other support. This work was funded in part by the Office of Naval Research under the Office of the Secretary of Defense Minerva program (grant number N00014-17-1-2423).

NOTES

1. W. J. Lynn III, "Deputy Secretary of Defense Speech: Remarks on Cyber at the RSA Conference," U.S. Government, *U.S. Department of Defense*, (February 15, 2011), http://archive.defense.gov/speeches/speech.aspx?speechid=1535.
2. U.S. Department of Homeland Security, "National Response Framework" (Federal Emergency Management Agency (FEMA), June 2016), 1–2, https://www.fema.gov/media-library-data/1466014682982-9bcf8245ba4c60c120aa915a-be74e15d/National_Response_Framework3rd.pdf.
3. Ibid., 17–18.
4. US Department of Homeland Security, "Cybersecurity Strategy," 15 May 2018, A-5, https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf.
5. Ibid.
6. The White House, "Presidential Decision Directive 41, United States Cyber Incident Coordination," 26 July 2016, https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident.
7. U.S. Department of Homeland Security, "The National Cyber Incident Response Plan (NCIRP)," *U.S. Government, United States Computer Emergency Readiness Team*, (2017), 4, https://www.us-cert.gov/ncirp.
8. Ibid., 14.
9. Department of Defense, DoD Cyber Strategy, April 2015, p5, https://www.defense.gov/Portals/1/ features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.
10. U.S. Government Accountability Office, "Civil Support: DOD Needs to Clarify Its Roles and Responsibilities for Defense Support of Civil Authorities during Cyber Incidents" (U.S. Government Accountability Office, April 4, 2016), 5, http://www.gao.gov/products/GAO-16-332.
11. "Joint Publication 3-28: Defense Support of Civil Authorities" (U.S. Joint Chiefs of Staff, July 31, 2013), vii, http://www.dtic.mil/doctrine/new_pubs/jp3_28.pdf.
12. "Joint Publication 3-27: Homeland Defense" (U.S. Joint Chiefs of Staff, July 29, 2013), I-1, I-2, https://www.hsdl.org/?view&did=742874.
13. Ibid., I-5.
14. Ibid., I-7.
15. W. J. Lynn III and A. B. Carter, "Department of Defense Directive 3025.18: Defense Support of Civil Authorities (DSCA)" (U.S. Department of Defense, September 21, 2012), 3–4, https://fas.org/irp/doddir/dod/d3025_18.pdf.
16. US Cyber Command, "USCYBERCOM Cyberspace Strategy Symposium Proceedings, 2018," p7, https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Cyberspace%20Strategy%20Symposium%20Proceedings%202018.pdf?ver=2018-07-11-092344-427.
17. T. Gjelten, "Cyber Briefings 'Scare The Bejeezus' Out Of CEOs," National Public Radio, 9 May 2012, https://www.npr.org/2012/05/09/152296621/cyber-briefings-scare-the-bejeezus-out-of-ceos.
18. Federal Bureau of Investigation, Cyber Crime, https://www.fbi.gov/investigate/cyber.
19. Department of Homeland Security, "Industry Offerings, Products, and Services," https://www.dhs.gov/sites/default/files/publications/DHS-Industry-Resources_4.7.edits_.pdf.
20. E. Nakashima, "Google to enlist NSA to help it ward off cyberattacks," The Washington Post, 4 February 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/02/03/AR2010020304057.html.
21. DoD Cyber Strategy, p8.
22. E. Nakashima, "U.S. rallied multinational response to 2012 cyberattack on American banks," The Washington Post, 11 April 2014, https://www.washingtonpost.com/world/national-security/us-rallied-multi-nation-response-to-2012-cyberattack-on-american-banks/2014/04/11/7c1fbb12-b45c-11e3-8cb6-284052554d74_story.html?utm_term=.45920d5ece84.
23. N. Shachtman, "Military's Cyber Commander Swears: "No Role" in Civilian Networks," Brookings Op-Ed, 23 September 2010, https://www.brookings.edu/opinions/militarys-cyber-commander-swears-no-role-in-civilian-networks/.
24. S. Harris, *@War: The Rise of the Military-Internet Complex*, Houghton Mifflin Harcourt, 2014, Chapter 10.
25. Comment from non-for-attribution participant, a general officer on the "Defend the Nation" panel, US Cyber Command Strategy Symposium, 15 September 2018. Also see, C. Bing, "Inside 'Project Indigo,' the quiet info-sharing program between banks and U.S. Cyber Command," CyberScoop, 21 May 2018, https://www.cyberscoop.com/project-indigo-fs-isac-cyber-command-information-sharing-dhs/.

NOTES

26. Department of Defense, Joint Publication JP 3-12, Cyberspace Operations, 8 June 2018, pII-8, https://fas.org/irp/doddir/dod/jp3_12.pdf.
27. M. D. Young, "National Cyber Doctrine: The Missing Link in the Application of American Cyber Power," Journal of National Security Law & Policy, (4:), http://jnslp.com/wp-content/uploads/2010/08/12_Young.pdf. p186.
28. Ibid.
29. J. Healey, ed, *A Fierce Domain: Cyber Conflict*, 1986-2012, CCSA, 2013, p22.
30. S. Morgan, "Why J.P. Morgan Chase & Co. Is Spending A Half Billion Dollars On Cybersecurity," Forbes, 30 June 2016, https://www.forbes.com/sites/stevemorgan/2016/01/30/why-j-p-morgan-chase-co-is-spending-a-half-billion-dollars-on-cybersecurity/#269503c12599.
31. The White House, Executive Order -- "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities," 1 April 2015, https://obamawhitehouse.archives.gov/the-press-office/2015/04/01/executive-order-blocking-property-certain-persons-engaging-significant-m.
32. F. D. Kramer, R. J. Butler, and C. Lotrionte, "Cyber and Deterrence: The Military-Civil Nexus in High-End Conflict" (Brent Scowcroft Center on International Security: Atlantic Council, January 2017), p14, http://www.atlanticcouncil.org/images/publications/Cyber_and_Deterrence_web_0103.pdf.
33. JP 3-12, pII-4.
34. C. Bing, "Inside 'Project Indigo', emphasis added.
35. G. Rattray and J. Healey, *Chapter: Categorizing and Understanding Offensive Cyber Capabilities and Their Use*, Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy (Washington, D.C: National Academies Press, 2010), p94, https://www.nap.edu/read/12997/chapter/8.
36. US-CERT Webpage, "National Cybersecurity and Communications Integration Center," accessed 25 July 2018.
37. Department of Homeland Security Inspector General, DHS' Efforts to Coordinate the Activities of Federal Cyber Operations Centers," Spotlight OIG-14-02, October 2013, https://www.oig.dhs.gov/assets/Mgmt/2014/OIG_SLP_14-02_Oct13.pdf.
38. M. Bowden, Worm: The First Digital World War, Grove Press, 2011, p180.
39. National Security Telecommunications Advisory Committee, "Report to the President on Information and Communications Technology Mobilization," November 2014, p6, https://www.dhs.gov/sites/default/files /publications/NSTAC%20-%20Information%20and%20Communications%20Technology%20Mobilization %20Report%2011-19-2014.pdf.
40. Ibid.
41. J. Healey, ed. *A Fierce Domain*, p71, quoting Bill Woodcock of the Packet Clearing House, and NSP-SEC member who helped mitigate the attacks on Estonia.
42. Ibid., p71.
43. Industry Consortium for Advancement of Security on the Internet website, https://www.icasi.org/current-activities/.
44. Interview with Neil Jenkins, Cyber Threat Alliance, 17 July 2018.
45. Kramer, Butler, and Lotrionte: Cyber and Deterrence, p2.
46. NSTAC Mobilization Report, pp8,12.
47. Ibid., p13.
48. T. Gjelten, "Cyber Briefings 'Scare The Bejeezus' Out Of CEOs," National Public Radio, 9 May 2012, https://www.npr.org/2012/05/09/152296621/cyber-briefings-scare-the-bejeezus-out-of-ceos.
49. M. Lowenthal, *Intelligence: From Secrets to Policy*, Fifth Edition, Sage Copress, 2012, pp68-69.
50. U.S. Government Accountability Office, "Civil Support."
51. Ibid., 15.
52. U.S. Government Accountability Office, "Defense Civil Support: DOD Needs to Identify National Guard's Cyber Capabilities and Address Challenges in Its Exercises" (U.S. Government Accountability Office, September 6, 2016), http://www.gao.gov/products/GAO-16-574.
53. Ibid., 13–14.
54. Kramer, Butler, and Lotrionte: Cyber and Deterrence, p14.
55. NSTAC Mobilization Report, p31.

NOTES

56. K. M. Donovan, "Expanding the Department of Defense's Role in Cyber Civil Support," Defense Technical Information Center (DTIC) (NORFOLK VA: National Defense University Joint Advanced Warfighting School, June 17, 2011), 53, http://www.dtic.mil/docs/citations/ADA545641.
57. "Joint Action Plan for State-Federal Unity of Effort on Cybersecurity" (Council of Governors, July 15, 2014), 1, https://www.nga.org/files/live/sites/NGA/files/pdf/2014/1407CouncilofGovernorsCyberJointActionPlan.pdf.
58. J. Soucy, "National Guard Set to Activate Additional Cyber Units," United States Army, Www.army.mil, (December 9, 2015), http://www.army.mil/article/159759/National_Guard_set_to_activate_additional_cyber_units.
59. C. A. Hopes, "The Challenges of Defense Support of Civil Authorities and Homeland Defense in the Cyber Domain," Defense Technical Information Center (DTIC) (Newport RI: Naval War College, Joint Military Operations Department, May 20, 2013), http://www.dtic.mil/docs/citations/ADA583525.