Atlantic Council

SCOWCROFT CENTER
FOR STRATEGY AND SECURITY

THE SIXTH DOMAIN: The Role of the Private Sector in Warfare

Franklin D. Kramer

Atlantic Council

SCOWCROFT CENTER
FOR STRATEGY AND SECURITY

THE SIXTH DOMAIN: The Role of the Private Sector in Warfare

Franklin D. Kramer

The **Scowcroft Center for Strategy and Security** works to develop sustainable, nonpartisan strategies to address the most important security challenges facing the United States and the world. The Center honors General Brent Scowcroft's legacy of service and embodies his ethos of nonpartisan commitment to the cause of security, support for US leadership in cooperation with allies and partners, and dedication to the mentorship of the next generation of leaders.

***Forward* Defense (*F*D)**, housed within the Scowcroft Center, generates ideas and connects stakeholders in the defense ecosystem to promote an enduring military advantage for the United States, its allies, and partners. Our work iden-tifies the defense strategies, capabilities, and resources the United States needs to deter and, if necessary, prevail in future conflict.

Table of Contents

EXECUTIVE SUMMARY

The United States and its allies have for some time recognized, as NATO doctrine provides, five operational domains—air, land, maritime, cyberspace, and space.[1] Each of those arenas fully fits with the understanding of a domain as a "specified sphere of activity" and, in each, militaries undertake critical wartime actions.[2] But in the ongoing Ukraine-Russia war, certain key operational activities have been undertaken by the private sector as part of the conduct of warfare. By way of example, private-sector companies have been instrumental both in providing effective cybersecurity and in maintaining working information technology networks. As part of such efforts, these firms have established coordinated mechanisms to work with relevant government actors.

These operational and coordinated activities by the private sector demonstrate that there is a "sixth domain"—specifically, the "sphere of activities" of the private sector in warfare—that needs to be included as part of warfighting constructs, plans, preparations, and actions if the United States and its allies are to prevail in future conflicts. As will be elaborated below, that sphere of activities focuses mainly on the roles of information and critical infrastructures, including their intersections—ranging from the transmission and protection of information to the assurance of critical infrastructure operations.

Many of the United States' activities in the sixth domain will take place in the United States homeland. However, while "defending the homeland" is listed as the first priority in the 2022 National Defense Strategy, insufficient attention has been paid to the actions that will be required of the private sector beyond just the defense industrial base as part of accomplishing an effective defense.[3] Likewise, when US military forces are engaged in overseas combat, private-sector companies in allied countries (as well as US companies operating overseas) will be critical for the effectiveness of US forces, as well as for the allies' own militaries. In short, establishing an effective strategy for the private sector in warfare is a key requirement for the United States and its allies.

This report sets forth the elements of such a strategy.[4] In substantial part, the paper builds on lessons regarding the sixth domain derived from the ongoing Ukraine-Russia war. The report discusses the key operational activities that fall within the sixth domain and how such activities need to be included in war planning with a focus on the organizational structures and authorities required for effective implementation of private-sector activities in warfare. For clarity of exposition, the report focuses its recommendations for the most part on the United States, though comparable approaches will be important for allies and partners.

The report recognizes the existing frameworks that have been established in the United States for interactions between the government and the private sector as set forth in Presidential Policy Directive 21 (PPD-21) of 2013 on critical infrastructure security and resilience,[5] the statutory requirements including those in the FY 2021 National Defense Authorization Act, the National Infrastructure Protection Plan, which addresses the resilience of critical infrastructures, and the role of the Cybersecurity and Infrastructure Security Agency (CISA) as the national coordinator for critical infrastructure security and resilience.[6] The report expands on those existing structures to recommend actions that will provide the framework for effective operational activities by the private sector in wartime.

Specifically, the report recommends:

1. Congress and the administration should work together to expand the existing national framework to provide for effective engagement with and coordination of the role of the private sector in wartime. This expanded framework for coordination between the private sector and federal government should include the requisite authorities and resources to accomplish each of the recommended actions below.

2. A Critical Infrastructure Wartime Planning and Operations Council (CIWPOC) with government and private-sector membership should be established to oversee planning for, and coordination of, government and private-sector wartime activities in support of national defense.

3. Regional resilience collaboratives should be established in key geographical locations to plan for and coordinate US government and private-sector activities in wartime and other high-consequence events and wartime efforts, including by the creation of regional risk registries that evaluate systemic risks.

4. Private-sector systemic risk analysis and response centers should be established for key critical infrastructures: a) using as an initial model the Analysis and Resilience Center for Systemic Risk that has been established by large private-sector firms for the financial and energy sectors, and b) focusing on cascading as well as other high-consequence, sector-specific risks. New centers should include key firms in the transportation, health, water, and food sectors.

5. An integrated corps of cybersecurity providers should be established whose private-sector members would provide high-end cybersecurity in wartime to key critical infrastructures and, if requested, to states, localities, tribes, and territories (SLTTs).

6. A "surge capability" of cybersecurity personnel in wartime should be established through the creation of a national cybersecurity civilian reserve corps and expansion of National Guard military reserve cybersecurity capabilities.

7. Cyber Command's "Hunt Forward" model of operations should be expanded in wartime to support key critical infrastructures in the United States and, if requested, to provide support to SLTTs.

8. An international undersea infrastructure protection corps should be established that would combine governmental and private activities to support the resilience of undersea cables and pipelines. Membership should include the United States, allied nations with undersea maritime capabilities, and key private-sector cable and pipeline companies.

9. The Department of Defense should continue to expand its utilization of commercial space capabilities including the establishment of wartime contractual arrangements and other mechanisms to ensure the availability of commercial space assets in wartime.

10. Congress should enact the necessary authorities and provide the appropriate resources to accomplish the actions recommended above.

I. HOMELANDS AT RISK IN WARTIME

While the United States has largely not been subject to armed attack on the homeland, the National Defense Strategy now makes explicit that the "scope and scale of threats to the homeland have fundamentally changed . . . as the "PRC and Russia now pose more dangerous challenges to safety and security at home."[7] Gen. Glenn VanHerck, commander of US Northern Command, has similarly testified that the:

> primary threat to the homeland is now . . . significant and consequential. Multiple peer competitors and rogue states possess the capability and capacity to threaten our citizens, critical infrastructure, and vital institutions.[8]

As Gen. VanHerck has stated, the challenges are particularly acute regarding critical infrastructures. The cyber attack on Colonial Pipeline, the attack on SolarWinds software supply chains, and multiple major ransomware attacks are illustrative of the types of attacks that have taken place in the United States.[9] Such attacks could be expected to be substantially expanded in the event of armed conflict.

The potential for attacks on critical infrastructures in a conflict with Russia is significant. The Annual Threat Assessment of the US Intelligence Community has stated that, while "Russia probably does not want a direct military conflict with US and NATO forces, . . . there is potential for that to occur," including in the context of the Ukraine-Russia war where "the risk for escalation remains significant."[10] The 2023 Annual Threat Assessment is unequivocal regarding Russia's capabilities to attack infrastructure in such an event:

> Russia is particularly focused on improving its ability to target critical infrastructure, including underwater cables and industrial control systems, in the United States as well as in allied and partner countries, because compromising such infrastructure improves and demonstrates its ability to damage infrastructure during a crisis.[11]

Similarly, the 2023 report speaks to China's capacity to threaten critical US infrastructures:

> If Beijing feared that a major conflict with the United States were imminent, it almost certainly would consider undertaking aggressive cyber operations against U.S. homeland critical infrastructure and military assets worldwide. . . . China almost certainly is capable of launching cyber attacks that could disrupt critical infrastructure services within the United States, including against oil and gas pipelines, and rail systems.[12]

Moreover, Chinese intrusions into US critical infrastructures appear to have already occurred, according to media reports:

> The Biden administration is hunting for malicious computer code it believes China has hidden deep inside the networks controlling power grids, communications systems and water supplies that feed military bases in the United States and around the world, according to American military, intelligence and national security officials.[13]

Of course, as the foregoing indicates, Russia or China could be expected not only to attack critical infrastructures in the United States, but also to undertake comparable actions against US allies. Indeed, such actions have already occurred in the context of the Ukraine-Russia war, in which Russia's attack on the Viasat satellite network disrupted information networks in multiple countries, including Germany, France, Greece, Italy, and Poland.[14] Other Russian activities in its war against Ukraine have similarly targeted allied critical infrastructures including "destructive attacks with the Prestige ransomware operation against the transportation sector in Poland, a NATO member and key logistical hub for Ukraine-bound supplies," and additionally "compromis[ing] a separate Polish transportation sector firm, and later increas[ing] reconnaissance against NATO-affiliated organizations, suggesting an intent to conduct future intrusions against this target set."[15]

Moreover, as noted above, China has comparable capabilities that could be utilized in a conflict against US allies and partners. For example, as the Department of Defense's 2022 report on China's military activities states, in the context of a conflict over Taiwan, the PRC "could include computer network . . . attacks against Taiwan's political, military and economic infrastructure."[16]

In sum, in the event of a conflict with either Russia or China, US, allied, and partner critical infrastructures and information flows will "almost certainly" be subject to attacks. But most of those critical infrastructures, including information and communications technology capabilities, are owned and operated by the private sector. As discussed below, those private-sector capabilities will be critical for military operations, continuity of government, and maintaining the performance of the economy in the event of conflict. Accordingly, a key issue for the United States and its allies and partners is how to effectively engage the private sector in wartime in order to offset the consequences of expected adversarial actions.

II. LESSONS FROM THE UKRAINE-RUSSIA WAR—THE ROLE OF THE PRIVATE SECTOR IN WARFARE

A useful starting place for understanding the sixth domain, and the role of the private sector in establishing an effective defense, comes from an overview of the efforts of private-sector companies in the context of the Ukraine-Russia war.

A worthwhile report by Irene Sánchez Cózar and José Ignacio Torreblanca summarized the actions of a number of companies:

> Microsoft and Amazon, for example, have proven fundamental in helping Ukrainian public and private actors

> secure their critical software services. They have done so by moving their on-site premises to cloud servers to guarantee the continuity of their activities and aid in the detection of and response to cyber-attacks. Moreover, Google has assisted Ukraine on more than one front: it created an air raid alerts app to protect Ukraine's citizens against Russian bombardment, while also expanding its free anti-distributed denial-of-service (DDoS) software-Project Shield-which is used to protect Ukraine's networks against cyber-attacks.[17]

Similarly, Ariel Levite has described how Ukraine, the United States, and the United Kingdom have utilized their technical capabilities in cyber defense and other areas during the Ukraine-Russia conflict:

> Ukraine and its Western allies have fared much better than Russia in the competition over cyber defense, early warning, battlefield situational awareness, and targeting information. This is due in large part to the richness and sophistication of the technical capabilities brought to bear by the U.S. and UK governments as well as various commercial entities (including SpaceX, Palantir, Microsoft, Amazon, Mandiant and many others), some of which received funding from the U.S. and UK governments. These actors came to Ukraine's help with intelligence as well as invaluable space reconnaissance sensors, telecommunications, and other technical assets and capabilities for fusing information and deriving operational cues. The Ukrainians skillfully wove these assets together with their indigenous resources.[18]

The discussion below elaborates on these points, focusing on five functional sectors (which have some degree of overlap) where the private sector has had key roles: cybersecurity, cloud computing, space, artificial intelligence, and communications.

A. Cybersecurity

Effective cybersecurity has been a key element of Ukraine's defense against Russia—achieving a degree of success that had not been generally expected:

> The war has inspired a defensive effort that government officials and technology executives describe as unprecedented—challenging the adage in cybersecurity that if you give a well-resourced attacker enough time, they will pretty much always succeed. The relative success of the defensive effort in Ukraine is beginning to change the calculation about what a robust cyber defense might look like going forward.[19]

The key to success has been the high degree of collaboration:

> This high level of defense capability is a consequence of a combination of Ukraine's own effectiveness, significant support from other nations including the United States and the United Kingdom, and a key role for private sector companies:
>
> The defensive cyber strategy in Ukraine has been an international effort, bringing together some of the biggest technology companies in the world such as Google and Microsoft, Western allies such as the U.S. and Britain and social media giants such as Meta who have worked together against Russia's digital aggression.[20]

A crucial part of that effort has been the private sector's willingness to expend significant resources:

> The cybersecurity industry has thrown a huge amount of resources toward bolstering Ukraine's digital defense. Just as the United States, European nations and many other countries have delivered billions of dollars in aid and military equipment, cybersecurity firms have donated services, equipment and analysts. Google has said it's donated 50,000 Google Workspace licenses. Microsoft's free technology support will have amounted to $400 million by the end of 2023, the company said in February. In the run-up to the invasion there was a broad effort by industry to supply Ukraine with equipment like network sensors and gateways and anti-virus and endpoint-detection and response tools.[21]

These combined actions have been highly effective. Ukraine was able to proactively foil Russian cyber operations at least two times, according to Dan Black. The threats involved were, he wrote, "a destructive malware targeting a shipping company in Lviv and the Industroyer2 operation against Ukraine's energy infrastructure at the onset of the Donbas offensive." Ukraine, with international, nongovernmental entities, disrupted them "through coordinated detection and response."[22]

B. Cloud Computing

Another critical set of activities—likewise focused on resilience—has been undertaken by private cloud companies. Ukraine has:

> worked closely with several technology companies including Microsoft, Amazon Web Services, and Google, to effect the transfer of critical government data to infrastructure hosted outside the country. . . . Cloud computing is dominated by . . . hyperscalers—[and] Amazon, Microsoft, [and] Google . . . provide computing and storage at enterprise scale and are responsible for the operation and security of data centers all around the world, any of which could host . . . data.[23]

The result has been consequential for both assuring continuity of governmental functions and for supporting the performance of the economy:

> Ukraine's emergency migration to the cloud has conferred immeasurable benefits. Within days of the war breaking out, key [critical infrastructure] assets and services came under the protection of Western technology companies, allowing Ukrainian authorities to maintain access and control over vital state functions. The uptime afforded by the public cloud cut across various critical services. Banking systems kept working, trains kept run-

> ning on schedule, and Ukraine's military kept its vital connections to situational awareness data. Physical risks to data centres and incident-response personnel were likewise mitigated.[24]

C. Space

Private-sector space capabilities have been crucial factors in Ukraine's defense efforts. Most well-known perhaps are the activities of the satellite company Starlink, a unit of SpaceX. As described by Emma Schroeder and Sean Dack, Starlink's performance in the Ukraine conflict demonstrated its high value for wartime satellite communications:

> Starlink, a network of low-orbit satellites working in constellations operated by SpaceX, relies on satellite receivers no larger than a backpack that are easily installed and transported. Because Russian targeting of cellular towers made communications coverage unreliable, . . . the government 'made a decision to use satellite communication for such emergencies' from American companies like SpaceX. Starlink has proven more resilient than any other alternatives throughout the war. Due to the low orbit of Starlink satellites, they can broadcast to their receivers at relatively higher power than satellites in higher orbits. There has been little reporting on successful Russian efforts to jam Starlink transmissions.[25]

Starlink is not, however, the only satellite company involved in the war:

> Companies both small and large, private and public, have supported Ukraine's military operations. Planet, Capella Space, and Maxar technologies—all satellite companies—have supplied imagery helpful to the Ukrainian government. . . . The imagery has done everything from inform ground operations to mobilize global opinion . . . Primer.AI, a Silicon Valley startup, quickly modified its suite of tools to analyze news and social media, as well as to capture, translate, and analyze unencrypted Russian military leaders' voice communications.[26]

The role of space assets presents a specific example of the systemic overlap among different capabilities operated by the private sector—and the need to coordinate with and protect them during wartime. As Levite indicates, the fusion of space and cyberspace as well as land- and space-based digital infrastructure is evident in the Ukraine conflict:

> Digital information, telecommunication, navigation, and mass communication assets are vital for modern warfare, and many now operate in or through space. In the Ukraine conflict we can detect early signs that attacking (and defending) space assets is not only deeply integrated with warfare in the air, sea, and land but is also heavily intertwined with digital confrontation in other domains. Control (or conversely disruption or disablement) of digital assets in space is thus becoming indispensable to gaining the upper hand on the battlefield and in the overall war effort.[27]

D. Artificial Intelligence

Artificial intelligence is another capability utilized in the Ukraine-Russia war that has been heavily supported by the private sector. Robin Fontes and Jorrit Kamminga underscore the voluntary role and impact of companies, primarily American ones, to heighten Ukraine's wartime capacity:

> What makes this conflict unique is the unprecedented willingness of foreign geospatial intelligence companies to assist Ukraine by using AI-enhanced systems to convert satellite imagery into intelligence, surveillance, and reconnaissance advantages. U.S. companies play a leading role in this. The company Palantir Technologies, for one, has provided its AI software to analyze how the war has been unfolding, to understand troop movements and conduct battlefield damage assessments. Other companies such as Planet Labs, BlackSky Technology and Maxar Technologies are also constantly producing satellite imagery about the conflict. Based on requests by Ukraine, some of this data is shared almost instantly with the Ukrainian government and defense forces.[28]

In providing such assistance, the private sector has often integrated its artificial intelligence capabilities with open-source information, combining them for military-effective results. Fontes and Kamminga also provide some granular examples of this and discuss how open-source data also bolster battlefield intelligence:

> In general, AI is heavily used in systems that integrate target and object recognition with satellite imagery. In fact, AI's most widespread use in the Ukraine war is in geospatial intelligence. AI is used to analyze satellite images, but also to geolocate and analyze open-source data such as social media photos in geopolitically sensitive locations. Neural networks are used, for example, to combine ground-level photos, drone video footage and satellite imagery to enhance intelligence in unique ways to produce strategic and tactical intelligence advantages.
>
> This represents a broader trend in the recruitment of AI for data analytics on the battlefield. It is increasingly and structurally used in the conflict to analyze vast amounts of data to produce battlefield intelligence regarding the strategy and tactics of parties to the conflict. This trend is enhanced by the convergence of other developments, including the growing availability of low-Earth orbit satellites and the unprecedented availability of big data from open sources.[29]

E. Communications

Maintaining functional information technology networks has been a critical requirement of Ukraine's defense. As Levite has pointed out, that has been accomplished despite massive Russian attacks essentially because of the inherent resilience of the underlying private-sector technologies including space and cloud capabilities (as described above):

> One especially novel insight to emerge from the Ukraine conflict is the relative agility of digital infrastructure (telecommunications, computers, and data) compared to physical infrastructure. Physical, electromagnetic, and cyber attacks can undoubtedly disrupt and even destroy key digital assets and undermine or diminish the efficacy of the missions they serve. But Ukrainian digital infrastructure (especially its cell towers and data servers) has been able to absorb fairly massive Russian missile as well as cyber attacks and continue to function, notwithstanding some temporary setbacks. . . . It appears that modern digital technology networks (such as those based on mobile and satellite communications and cloud computing infrastructure) are more robust and resilient than older infrastructure, allowing relatively quick reconstitution, preservation, and repurposing of key assets and functions.[30]

III. THE US HOMELAND SECURITY FRAMEWORK DOES NOT INCLUDE WARTIME REQUIREMENTS FOR THE PRIVATE SECTOR

The current US framework for private-sector engagement with the government is not focused on wartime. Rather, as set forth in PPD-21, the scope is limited by the definition of the term "all hazards," which stops short of armed conflict:

> The term 'all hazards' means a threat or an incident, natural or man-made, that warrants action to protect life, property, the environment, and public health or safety, and to minimize disruptions of government, social, or economic activities. It includes natural disasters, cyber incidents, industrial accidents, pandemics, acts of terrorism, sabotage, and destructive criminal activity targeting critical infrastructure.[31]

A recent report by the Government Accountability Office (GAO) similarly notes that, while the US Department of Homeland Security (DHS) was initially established in the wake of the 9/11 terrorist attacks and correspondingly had a counterterror focus, PPD-21 "shifted the focus from protecting critical infrastructure against terrorism toward protecting and securing critical infrastructure and increasing its resilience against all hazards, including natural disasters, terrorism, and cyber incidents."[32]

While wartime planning and operations are not covered, it is nonetheless important to recognize that the United States does undertake multiple efforts under the National Plan that are focused on the resilience of critical infrastructures and that the National Plan has been enhanced by each administration and the Congress since its inception. The National Plan is briefly reviewed below, as it provides the context and a valuable starting point for the recommendations made by this report with respect to the role of the private sector in wartime.

The GAO has described the National Plan as providing both a foundation for critical infrastructure protection and an "overarching approach" to make the work of protection and resilience an integrated national effort:

> The National Plan details federal roles and responsibilities in protecting the nation's critical infrastructures and how sector stakeholders should use risk management principles to prioritize protection activities within and across sectors. It emphasizes the importance of collaboration, partnering, and voluntary information sharing among DHS and industry owners and operators, and state, local, and tribal governments.[33]

DHS has the overall coordination responsibility under the National Plan and, within DHS, the Cybersecurity and Infrastructure Security Agency has been established as the "national coordinator for critical infrastructure protection,"[34] partnering with federal, state, and municipal agencies as well as territorial and tribal authorities and the private sector.

In conjunction with the National Plan, PPD-21 designated sixteen critical infrastructure sectors. In each sector, a lead agency or department—dubbed a sector risk management agency (SRMA)—coordinates with CISA; collaborates with critical infrastructure owners and operators; coordinates with the varying levels of governments, authorities, and territorial partners; and participates in a government coordinating council as well as a sector coordinating council with owners-operators of critical assets and relevant trade association representatives.[35]

Pursuant to PPD-21, including through actions taken by CISA, a host of coordination mechanisms exist to enhance the resilience of critical infrastructures, including the Federal Senior Leadership Council, the Critical Infrastructure Partnership Advisory Council, government coordinating councils, and sector coordinating councils.[36] Congress also established the Office of the National Cyber Director (ONCD), whose mandate includes working with "all levels of government, America's international allies and partners, non-profits, academia, and the private sector, to shape and coordinate federal cybersecurity policy."[37] ONCD's mandate includes coordinating the recently issued *National Cybersecurity Strategy Implementation Plan,* whose multiple initiatives include defending critical infrastructures, disrupting threat actors, shaping market forces for security and resilience, undertaking investment, and forging international partnerships.[38]

In addition to the substantial efforts at coordination, CISA and the SRMAs have undertaken a number of other worthwhile steps to enhance the US capability to respond to attacks on critical infrastructures. Regulatory authority has been utilized to require or propose cybersecurity requirements including for air, rail, pipelines, and water.[39] Utilizing the authority and resources provided by Congress, cybersecurity assistance is being provided to SLTT entities.[40] A Joint Cyber Defense Collaborative has been established to effectuate "operational collaboration and cybersecurity information fusion between public and private sectors, for the benefit of the broader ecosystem, [and for] producing and disseminating cyber defense guidance across all stakeholder communities."[41] CISA additionally conducts exercises and training with the private sector, ranging from a ta-

bletop exercise to the large-scale Cyber Storm exercise, which simulates a cyberattack.[42]

CISA also has set forth a "planning agenda" seeking to "combin[e] the capabilities of key industry partners with the unique insights of government agencies . . . [in order to] create common shoulder-to-shoulder approaches to confront malicious actors and significant cyber risks."[43] The agenda includes "efforts to address risk areas" such as open-source software, and the energy and water sectors, while recognizing that "our plans and doctrine have not kept up" with the requirements of cybersecurity.[44] Similarly, CISA has recognized the value of effective cybersecurity firms supporting less-capable companies, specifically seeking to "advance cybersecurity and reduce supply chain risk for small and medium critical infrastructure entities through collaboration with remote monitoring and management (RMM), managed service providers (MSPs), and managed security service providers (MSSPs)."[45]

CISA's efforts are complemented by the National Cyber Investigative Joint Task Force, led by the Federal Bureau of Investigation and by the Cybersecurity Collaborative Center (CCC) led by the National Security Agency (NSA). Under the recent *National Cybersecurity Strategy Implementation Plan,* the FBI is to "expand its capacity to coordinate takedown and disruption campaigns with greater speed, scale, and frequency."[46] The NSA's CCC provides support to the private sector including cost-free protection for DIB companies through a "filter which blocks users from connecting to malicious or suspicious [Internet] domains" as well as "bi-directional cyber threat intelligence sharing with major IT and cybersecurity companies who are best positioned to scale defensive impacts [and which has] hardened billions of endpoints across the globe against foreign malicious cyber activity."[47]

To sum up, while the National Plan is focused on significant threats and there is much to commend in the actions taken and planned, those efforts have not yet taken account of the significant disruptive potential of wartime threats. Neither CISA (through the Joint Cyber Defense Collaborative or otherwise) nor the SRMAs nor the ONCD have yet established the type of coordination mechanisms necessary for effective private-sector operations in wartime along the lines as have been undertaken in the Ukraine-Russia war. Similarly, while the FBI and the NSA undertake certain operational activities, in their current format those actions do not reach the level of effort required for effectiveness in wartime.

IV. RECOMMENDATIONS

The discussion above demonstrates both the ongoing engagement of the private sector in the Ukraine-Russia war and the potential for important private-sector future roles if the United States and its allies were involved in a future conflict. Maximizing that potential for the United States and its allies will require collaborative initiatives that engage the private sector as an operational partner. The discussion below sets forth ten such initiatives focusing largely on actions to be taken in the United States, though as previously noted, comparable actions should be undertaken by allies and key partners.

A. Congress and the Biden Administration Should Expand the Existing National Framework to Provide for Effective Engagement with the Private Sector in Wartime

Congress and successive administrations have regularly focused on the need to upgrade homeland security and each branch of government has undertaken to assure an effective national defense. However, neither Congress nor the executive branch has yet brought the two together in a comprehensive approach, and neither has provided a framework for the inclusion of the private sector as part of operational wartime defense activities.

The importance of establishing such a framework has recently been made clear by the lessons drawn from the Ukraine-Russia war, as discussed above. Broadly, the administration should issue an executive order under existing authorities to begin the establishment of such a framework, and Congress should work with the administration to establish the necessary full-fledged approach, including the provision of the requisite authorities and resources. The specific actions are discussed at length in the recommendations below.

Initially, the administration should establish a Critical Infrastructure Wartime Planning and Operations Council with government and private-sector membership (including, as requested, SLTTs); establish regional resilience collaboratives; and help facilitate the establishment of sector-specific coordinating mechanisms. Congress and the administration should work together to establish an Integrated Cybersecurity Providers Corps; authorize the establishment of a national Cybersecurity Civilian Reserve Corps and an expansion of National Guard cybersecurity capabilities; authorize Cyber Command in wartime to support key critical infrastructures; establish an international Undersea Infrastructure Protection Corps; expand the use of private-sector space capabilities; and enact the required authorities and provide the necessary resources to accomplish each of the foregoing.

B. Establish a Critical Infrastructure Wartime Planning and Operations Council with Government and Private-Sector Membership

In the United States (and in most other allied countries), there is no comprehensive mechanism to engage the private sector in warfare. While there are worthwhile efforts—such as by CISA and the SRMAs, as described above—they are focused on prewar resilience. By contrast, Finland, NATO's newest member, has long had a comprehensive approach to national security that fully engages the private sector, including in the event of an "emergency," which is defined to include "an armed or equally serious attack against Finland and its immediate aftermath [or] a serious threat of an armed or equally serious attack against Finland."[48]

In such an event, the Finland model of "comprehensive security" provides that the "vital functions of society are jointly safeguarded by the authorities, business operators, organisations

and citizens."[49] The *Security Strategy for Society* describes a "cooperation model in which actors share and analy[z]e security information, prepare joint plans, as well as train and work together." Participants include the central government, authorities, business operators, regions and municipalities, universities, and research and other organizations.[50] Quite importantly, "[b]usiness operators are playing an increasingly important role in the preparedness process . . . [and in] ensuring the functioning of the economy and the infrastructure."[51]

Finland has a small population, so the precise mechanisms it utilizes for its comprehensive approach would need to be modified for other countries, including the United States. But the key point is that there needs to be such an overarching cooperation model involving this range of actors and activities.

To accomplish such a coordinated effort—and to focus on the United States—a CIWPOC with government and private-sector membership should be established through the issuance of an executive order as part of the overall White House national security structures.

At the governmental level, it is important to recognize that neither the existing Federal Senior Leadership Council, which includes CISA and the SMRAs, nor any of the other councils and coordinating efforts described above are operationally oriented for wartime activities, nor are they designed to undertake the necessary actions required to "analyze security information, prepare joint plans, as well as train and work together" in the context of conflict or imminent threat of conflict.[52] Accordingly, a better mechanism to guide actions in wartime would be to establish a CIWPOC along the lines of a joint interagency task force (JIATF) with appropriate personnel from relevant agencies plus private-sector subject matter experts, each of whom would have the background and capabilities to plan for and, if required, act in a wartime context.[53]

Such a CIWPOC could be headed by CISA prior to a wartime-related emergency, with the Defense Department acting as the deputy and organizing the necessary planning and training. In the event of a conflict or if a threat is imminent, the Defense Department would take command to integrate the CIWPOC into the full context of responding to the conflict, with CISA then in the deputy role. The dual-hatting of CISA and the Defense Department is key to ensuring a smooth transition in the event of conflict as that will allow for coordination mechanisms to be established prior to conflict. The planning and training led by the Defense Department prior to conflict will also establish lines of coordination as well as the necessary familiarity with tasks required in wartime, both for DOD and CISA as well as for the other government departments and private sector entities that are engaged with the CIWPOC.

Initially, at least, the CIWPOC membership should be limited to departments with responsibility for sectors most relevant to wartime military efforts as well as to continuity of government and to key elements of the economy. Utilizing that criterion, a first set of members would include defense, homeland security, energy, finance, information and communications technology, transportation, SLTTs, food, and water.

Private-sector representation on the CIWPOC should come from the key critical infrastructures, noted above, most relevant to planning and operations in a conflict. As discussed below, that would include representatives from the proposed Integrated Cybersecurity Providers Corps and the Undersea Infrastructure Protection Corps, as well as from the regional resilience collaboratives and the private-sector systemic risk analysis and response centers, established as recommended below. As would be true for governmental departments, private-sector membership will not necessarily include all critical infrastructures, as the focus for the CIWPOC is on the operational capabilities that the private sector can provide in the event of a conflict. There would be costs to the private-sector entities associated with the planning and training efforts described, and, inasmuch as those costs are associated with providing national defense, Congress should undertake to include them in the national defense budget.

As part of organizing the proposed CIWPOC, DOD would have to determine which military command would have the lead and what resources would be required. In order to achieve the full degree of effectiveness required, the administration should undertake a thorough review of command arrangements and resources required for homeland defense, as the current arrangements are not sufficient.[54]

- Northern Command's current mission is to provide "command and control of . . . DOD homeland defense efforts and to coordinate defense support of civil authorities."[55] While it is analytically the appropriate command to lead in the context of the CIWPOC, in reality, Northern Command would need substantial additional resources and expanded authorities to undertake the requisite actions. By way of example, its mission would need to expand beyond "defense support to civil authorities" to include planning for wartime and operational control as required in the event of conflict.
- Transportation Command, Cyber Command, Space Command, and the Coast Guard each would have important roles in generating the necessary plans, training, and (if required) operations. They likely should be supporting commands in undertaking those missions in the United States in order to maintain unity of command at the DOD level and unity of effort both at the interagency and private-sector levels. However, the arrangements within DOD and with interagency participants are not yet established.
- The review recommended above should be undertaken promptly, and the results presented to the president and then to the Congress for such actions as may be required—but that process should not be a bar to the initial establishment of the CIWPOC, including DOD's engagement.

C. Establish Regional Resilience Collaboratives

In addition to the central Critical Infrastructure Wartime Planning and Operations Council discussed above, it will be important to coordinate government and private-sector activities in key geo-

graphical locations with a focus on support to national defense wartime efforts.

Not everything can best be done centrally in the context of a conflict. By way of example, the Finnish model of collective security underscores the importance of regional efforts:

> There should be cooperation forums of security actors (such as preparedness forums) . . . in each region . . . [which] would form the basis for the preparedness plan that would also include the lines of authority, continuity management, use of resources, [and] crisis communications plan[s] . . . The workability of the preparedness plans and the competence of the security actors would be ensured by training and joint exercises.[56]

CISA does have established mechanisms to reach out to private sector companies and to SLTTs, including through its regional offices and its SLTT grant program.[57] However, in accord with its overall approach, those efforts are not focused on wartime activities. One way to generate the necessary regional efforts for wartime would be to establish regional resilience collaboratives for key geographic areas with an initial focus on those areas that provide critical support to military operations such as key US ports on the East, Gulf, and West coasts. To increase the attractiveness for the private sector, the regional resilience cooperatives should focus on both wartime and other high-consequence risks, such as cascading impacts in circumstances short of war.

The Senate version of the FY2024 National Defense Authorization Act includes a provision focused on regional resilience. The bill provides for a pilot program to evaluate "how to prioritize restoration of power, water, and telecommunications for a military installation in the event of a significant cyberattack on regional critical infrastructure that has similar impacts on State and local infrastructure."[58] The bill requires that the pilot program should be "coordinated with . . . private entities that operate power, water, and telecommunications" for the military installations included in the pilot program.[59]

It should be apparent that the Defense Department will not be able of itself to create the necessary cyber resilience against an attack nor the necessary restoration processes (though, as discussed below, DOD can provide important support). Those actions will have to be undertaken by the private sector (or, in some cases, by SLTTs that operate critical infrastructure).

Accordingly, the FY2024 NDAA when enacted should include provisions to establish regional resilience collaboratives, initially to operate to generate sustained engagement among public and private entities designed to respond to wartime attacks and high-consequence cybersecurity risks in peacetime through collaboration among key private, SLTT, and federal entities. As a first step (and consistent with the Senate bill calling for mapping dependencies)[60], a regional resilience collaborative should build a regional risk registry focused on regional dependency models, including cascading risks.

As with the case of the CIWPOC discussed above, CISA would lead in peacetime and DOD in wartime. Support would also come from the integrated cybersecurity protection corps described below. Regional resilience collaboratives would undertake operational planning led by the Department of Defense that would utilize both private and public capabilities. Continuous planning (including updated threat reviews and net assessments) and implementing actions would enhance resilience and allow for effective responses, if required. While the benefits from a regional resilience collaborative would be made widely available, the actual participants would be selectively included as relevant to the risks identified by the regional risk registry.

A regional risk collaborative effort would have costs associated with its activities. As would be the case regarding the CIWPOC as well as the integrated corps of cybersecurity providers, and since those costs are associated with providing national defense, Congress should undertake to include them in the national defense budget.

D. Establish Private-Sector Systemic Risk Analysis and Response Centers

Certain sectors of the economy are sufficiently critical that undertaking enhanced efforts to reduce risk in wartime would be important to the national defense. To be sure, all critical infrastructures already undertake a variety of coordination efforts, including those noted above, as well as through Information Sharing and Analysis Centers (ISACs) and Information Sharing and Analysis Organizations.[61] However, particularly in the context of wartime, it will be important to go beyond information sharing and to undertake coordinated risk-reduction efforts.

A model for this in the United States is the Analysis and Resilience Center for Systemic Risk (ARC), which is a "coalition that is identifying, prioritizing, and mitigating risks to their infrastructure and the points of connection to other critical infrastructure sectors."[62] The ARC brings together "small groups of industry experts [who] identify risks and find solutions that benefit the larger critical infrastructure community."[63] The activities of the ARC go well beyond the information sharing currently undertaken by the ISACs, seeking to respond to systemic risk in a coordinated way. While the existing ARC members come from leading financial and energy firms, the concept should be extended to key functional areas including transportation, food, water, and healthcare.

Newly established private-sector systemic risk analysis and response centers will also benefit from close coordination with key providers of network infrastructure and services, as is currently being accomplished for the financial industry through the Critical Providers Program of the financial services ISAC (FS-ISAC).[64] That program "enables critical providers to use FS-ISAC channels to communicate during large-scale security upgrades, technical outages, cyber-based vulnerabilities, software and hardware misconfigurations, and/or changes that could impact multiple FS-ISAC members"[65] As the foregoing suggests, there is already a certain amount of coordination being undertaken

in the information and communications technology (ICT) arena, and a determination can be undertaken as to the value of establishing an ICT systemic risk analysis and response center.

E. Establish an Integrated Cybersecurity Providers Corps

As discussed above, one of the key roles that the private sector has played in the Ukraine-Russia war is to provide highly effective cybersecurity for critical infrastructures despite significant and continuing Russian cyberattacks. In the event of a conflict with either Russia or China, US cybersecurity firms could be expected to undertake similar actions, including based on service-level agreements they have with critical infrastructures in the United States and efforts like the Critical Providers Program noted above. However, also as noted above, the actions being taken in Ukraine are part of a larger operational collaborative effort that includes firms working together and with governments (including the United States, the UK, and Ukraine). Accordingly, for private-sector cybersecurity support to be most effective in the United States in wartime, a similar approach to coordinated support should be organized in advance of the need, in conjunction with the government, including appropriate information sharing, planning, and exercises relevant to wartime operations.

To begin such an effort, an Integrated Cybersecurity Providers Corps (ICPC) should be established and focused on providing effective cybersecurity for those critical infrastructures most relevant to military activities, continuity of government, and maintaining the performance of the economy. One of the fundamental recommendations of the *National Cybersecurity Strategy* is to "ask more of the most capable and best-positioned actors to make our digital ecosystem secure and resilient," and that should certainly apply to wartime.[66]

The ICPC should operate under the general ambit of the Critical Infrastructure Wartime Planning and Operations Council, described above. Membership should consist of highly capable cybersecurity firms and major cloud providers, with CISA and DOD jointly determining whether a cybersecurity provider met the requirements for membership in the corps. Broadly speaking, an integrated cybersecurity provider should be able to provide high-end cybersecurity services including authentication, authorization, segmentation, encryption, continuous monitoring, and protection against DDoS attacks. Cloud providers should have the ability to protect the cloud itself and to offer other expert security providers the opportunity to provide cybersecurity as a service on the cloud. The intent would be to ensure that key critical infrastructures have the support of effective integrated cybersecurity providers in wartime.[67]

Concomitant with the establishment of the ICPC, DHS/CISA and DOD, who will work closely with the ICPC members, should undertake to assure the engagement of the key critical infrastructures most relevant in wartime to military activities, continuity of government, and maintaining the performance of the economy. Usefully, DHS/CISA already is required to identify infrastructures of critical importance to the United States:

> The Department of Homeland Security (DHS), in coordination with relevant Sector Specific Agencies (SSAs), annually identifies and maintains a list of critical infrastructure entities that meet the criteria specified in Executive Order (EO) 13636, *Improving Critical Infrastructure Cybersecurity*, Section 9(a)('Section 9 entities') utilizing a risk-based approach. Section 9 entities are defined as 'critical infrastructure where a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security.'[68]

The Section 9 list could provide the basis—or at a minimum, a starting point—for identifying the infrastructures most critical in the context of wartime. Additionally, however, since one key objective in wartime will be continuity of government, at least some SLTT governments will need to be included on the list—though there will have to be some very significant prioritization since there are approximately ninety thousand local governments in the United States.[69] Initial inclusion of SLTTs might be for those related to areas for which regional resilience collaboratives are established.

A third step will be to create a process to provide assured linkages between the designated key critical infrastructures (including the key SLTTs) and integrated cybersecurity providers. Congress should enact legislation authorizing regulations requiring such support in wartime for designated critical infrastructures and should establish a voluntary program for key SLTTs. A regulatory approach is particularly necessary as, for the most part, critical infrastructure companies are far less capable at cybersecurity than are the expert cybersecurity providers—and that would certainly be true in wartime, when the threat would be more substantial. Under the regulations, designated critical infrastructures should be required to plan and train with integrated cybersecurity providers prior to conflict so that the requisite cybersecurity resilience could be achieved in wartime. SLTTs should likewise be provided the opportunity for cybersecurity support, including planning and training on a voluntary basis, for reasons of federalism. As noted above, there will be costs associated with such activities which, since they would be undertaken in support of national defense, should be included by Congress in the Defense Department budget.

F. Create a Wartime Surge Capability of Cybersecurity Personnel by Establishing a Cybersecurity Civilian Reserve Corps and Expanding National Guard Cyber Capabilities

The need for the federal government to overcome the currently existing shortage of qualified cybersecurity personnel is well understood, and the importance of having sufficient cybersecurity personnel would be even greater in wartime. At the time of this writing, both the House and Senate versions of the fiscal year (FY) 2024 National Defense Authorization Act (NDAA) have provisions intended to help ameliorate that shortage, but more substantial improvements are warranted.

In the House, Representative Mark Green had proposed requiring a report on the "feasibility of establishing a cyber unit in

every National Guard of a State."[70] That recommendation was not included in the House version of the NDAA but there is a provision authorizing Cyber Command to "accept voluntary and uncompensated services from cybersecurity experts."[71] By contrast, in the Senate, Senators Jacky Rosen and Marsha Blackburn had proposed establishing a pilot program for a cyber reserve for DOD and DHS.[72] That proposal also was not included in its entirety in the Senate version of the NDAA but there is a provision for the Secretary of the Army to "carry out a pilot project to establish a Civilian Cybersecurity Reserve."[73] Each of the proposed provisions is a step forward and enacting both the House and Senate provisions would be worthwhile, but the final version of the NDAA should go further than the existing proposals and move promptly to full-fledged cyber civilian reserve and augmented National Guard cyber capabilities.

Establishing a "surge capability" able to add significant numbers of personnel from the private sector for cybersecurity activities in the event of a conflict should be a high priority for the United States. The value of such a capability has been underscored in the context of the conflict in Ukraine, in which:

> [i]mmediately after the invasion, Ukraine also began to elicit support from the private sector to supplement its own cyber capabilities. One aspect of this effort was to call on national private-sector experts. Requests for volunteers to help protect [critical infrastructures] were reportedly circulated through communities at the request of a senior Ukrainian defence ministry official. These volunteers were requested to help defend infrastructure, identify critical vulnerabilities and carry out other defensive tasks.[74]

In the United States, such a reserve capability could be established by a combination of the proposed measures now in the House and Senate versions of the NDAA as well as Representative Green's proposal for expanding National Guard cyber capabilities.

- A cybersecurity civilian reserve corps would provide for the United States access to personnel beyond those seeking to be part of the military. Such an approach is being utilized by US allies with very substantial cyber capabilities. The UK has already established its Joint Cyber Reserve Force with a "mantra of high-end cyber talent first," so that the "Reserves 'conventional' physical entry standards (physical ability, fitness, etc.) are not our immediate concern. This ensures that we can select untapped talented individuals who would not normally see reserve service as an option or possibility."[75] Other countries such as Estonia have also developed reserve models to "bring together competent IT experts who can solve significant and long-term cyber incidents."[76]
- The National Guard currently includes both Army and Air Force cyber units.[77] However, expanding their numbers and better integrating them into the force would have high value. Given the substantial demand for additional cyber personnel, and as previously recommended, "the number of National Guard personnel directed toward the cyber mission should be significantly increased. . . . [and] a reasonable initial step would be to increase Guard end strength in order to increase the number of cyber personnel to approximately double the current levels."[78] In accomplishing that increase, the "Department of Defense [should] bolster its operational capacity in cyberspace through improved utilization of the National Guard," as Congress has previously called for: "Despite [Congressional] calls for change, the Department of Defense and the military services appear not to have made any meaningful change in how the expertise resident within the National Guard and the Reserve Component can be better leveraged."[79]

In sum, combining the current versions of the House and Senate NDAA legislation and additionally establishing an expanded National Guard cyber capability would result in significant benefits to the United States in the event of a conflict.

G. Expansion of Cyber Command's "Hunt Forward" Model to Support Key Critical Infrastructures in Wartime in the United States

US Cyber Command regularly works with allied and partner nations at their request to enhance the cybersecurity of their critical infrastructures.[80] Testimony from Cyber Command has described that "since 2018, [it] has deployed hunt forward teams 40 times to 21 countries to work on 59 networks."[81] Cyber Command has described its Hunt Forward operations (HFOs) as follows:

> strictly defensive cyber operations conducted by U.S. Cyber Command (USCYBERCOM) at the request of partner nations. Upon invitation, USCYBERCOM Hunt Forward Teams deploy to partner nations to observe and detect malicious cyber activity on host nation networks. The operations generate insights that bolster homeland defense and increase the resiliency of shared networks from cyber threats.[82]

A Hunt Forward operation is a joint effort, as the Cyber Command operators "sit side-by-side with partners and hunt for vulnerabilities, malware, and adversary presence on the host nation's networks."[83]

As a matter of policy, Cyber Command does not currently undertake operations in the United States. In wartime, however, Cyber Command should have an expanded mission to support key critical infrastructures most relevant to national defense. As described above, such governmental efforts have been instrumental—along with the actions of the private sector—in supporting Ukraine, and a similar collaborative approach should be undertaken for wartime in the United States.

In the United States in wartime, Cyber Command hunting capabilities should be coordinated with the relevant critical infrastructures and with the proposed Integrated Cybersecurity Providers Corps. Undertaking prior training and exercises would, of course, make any actual operations more effective. Additionally, to accomplish such a mission without diverting resources from Cyber Command's core mission set (i.e., global cyber opera-

tions and defense of DOD networks), Cyber Command would likely require a substantial increase in personnel for wartime operations.[84] As discussed in the prior section, there are good reasons to establish a wartime cyber civilian reserve and to increase National Guard cybersecurity capabilities—and supporting Cyber Command wartime operations would be one of the most important.

In expanding the mission as recommended above, Cyber Command would be subject to the same constitutional requirements as other federal departments and agencies, including the Fourth Amendment's limits on intrusion into private activities. While searches based on enemy actions in wartime would likely be deemed reasonable and warrants could be obtained, a much better approach—both as a matter of constitutional law and appropriate policy—would be for the federal government to work with the key critical infrastructures to establish a consensual wartime set of arrangements and for Congress to undertake a review of the agreed activities.[85]

H. Establish an Undersea Infrastructure Protection Corps

The United States and its allies have long recognized the vulnerability of undersea pipelines and cables.[86] Attacks on the Nord Stream 1 and 2 pipelines in September 2022 have underscored those vulnerabilities and raised the visibility of the security issue at the highest levels of government.[87] At the May 2023 G7 summit, the group determined, "[w]e are committed to deepen our cooperation within the G7 and with like-minded partners to support and enhance network resilience by measures such as extending secure routes of submarine cables."[88] Relatedly, the Quad grouping of countries (i.e., Australia, India, Japan, United States) agreed to establish "the Quad Partnership for Cable Connectivity and Resilience [which] will bring together public and private sector actors to address gaps in the infrastructure and coordinate on future builds."[89]

The G7 and Quad actions are future-oriented, but pipelines and undersea cables are currently subject to more immediate vulnerabilities, with Russia being a particularly concerning threat.[90] As NATO Secretary General Jens Stoltenberg has stated:

> So we know that Russia has the capacity to map, but also potentially to conduct actions against critical infrastructure. And that's also the reason why we have, for many years, addressed the vulnerability of critical undersea infrastructure. This is about gas pipelines, oil pipelines, but not least thousands of kilometres of internet cables, which is so critical for our modern societies—for financial transaction, for communications, and this is in the North Sea, in the Baltic Sea, but across the whole Atlantic, the Mediterranean Sea.[91]

A report to the European Parliament similarly highlighted the issues, noting the Russian Navy has a "special focus" on the Yantar class intelligence ships and auxiliary submarines, which have the capacity to disrupt undersea cable infrastructure. Also of note are "new abilities to deploy mini-submarines" to explore underwater sea cables by stealth, according to the report.[92]

As a consequence of those concerns, NATO has established a NATO Maritime Centre for the Security of Critical Undersea Infrastructure as a partnership with the private sector.[93] Per Secretary General Stoltenberg, the purpose is to strengthen the protection of undersea infrastructure:

> And of course, there's no way that we can have NATO presence alone [surveilling] all these thousands of kilometres of undersea, offshore infrastructure, but we can be better at collecting information, intelligence, sharing information, connecting the dots, because also in the private sector is a lot of information. And actually, there's a lot of ongoing monitoring of traffic at sea and to connect all those flows of information will increase our ability to see when there is something abnormal and then react dependent on that.[94]

Secretary General Stoltenberg highlighted the importance of collaborating with the private sector:

> And then most of it is owned and operated by the private sector and they also have a lot of capabilities, to protect, to do repair and so on. So the purpose of this Centre . . . is to bring together different Allies to share information, share best practices, and to be able to react if something abnormal happens and then also to ensure that the private sector and the government, the nations are working together.[95]

As the new NATO effort underscores, resilience of undersea infrastructure will be of high consequence in the event of armed conflict. However, NATO itself does not generally provide the capabilities that the organization utilizes, but rather relies on the capabilities provided by its member nations. Accordingly, the United States should work with allies and those elements of the private sector that have relevant undersea capabilities to establish an international Undersea Infrastructure Protection Corps, both to support NATO activity and because security for undersea infrastructures is inherently international. This corps should include both the private-sector builders/maintainers and the owners of undersea cables and pipelines. That group would organize the actions required to enhance the resilience that would be necessary in wartime.

The countries and companies connected by cables and pipelines involve substantial numbers of US allies. According to one industry analysis, the top five undersea cable vendors are Alcatel-Lucent Enterprise (France), SubCom LLC (United States), NEC Corporation (Japan), Nexans (France), and Prysmian Group (Italy).[96] In terms of ownership, US companies are significantly involved with Google, Facebook, Microsoft, and Amazon being significant investors in cables.[97] With respect to undersea pipelines, there are multiple such pipelines in the North Sea, Baltic Sea, Mediterranean Sea, and the Gulf of Mexico, all, of course, involving US allies and/or the United States.[98] Accordingly, there should be sufficient geopolitical alignment with respect to establishing an Undersea Infrastructure Protection Corps, and while the precise arrangements will have to be negotiated, it is

notable that several countries have already taken steps. The UK, Norway, and Italy are each organizing security efforts to enhance pipeline security, and the United States, the UK, and France have well-established undersea capabilities.[99]

An international Undersea Infrastructure Protection Corps should have three areas of focus. First, as is true with respect to other information and communication technology networks, undersea cables will need the same type of effective cybersecurity. As noted above, several significant undersea cable owners are also companies that have been extensively involved in the defense of Ukraine's ICT networks, including working with the United States and the UK. That operational experience and real-time experience with public-private coordination should provide a basis for extending such an approach to undersea cables.[100]

Second, all undersea cables eventually come out of the sea to on-ground "landing points." John Arquila has indicated that "concerns about the vulnerability of landing points, where the cables come ashore . . . has led to the idea of having many branch points near landfall."[101] Arquila also describes efforts "to improve landing-point security through concealment and hardening—including, in the latter case, the shielding with armor of the cable segments in shallower waters near landing points. . . . [and also use of] both surveillance technologies and increased on-site security."[102] An Undersea Infrastructure Protection Corps can build on such approaches.[103]

Third, undersea infrastructures can be repaired, with cable repairs regularly undertaken for commercial reasons.[104] However, as a report to the European Parliament describes, the availability of cable repair capabilities deserves review:

> A key and often neglected vulnerability of the cable infrastructure is the capabilities . . . for repair. The capabilities within Europe are very limited . . . The repair infrastructure is often not featured in risk analyses, although it is in larger-scale coordinated attack scenarios.[105]

The proposed international Undersea Infrastructure Protection Corps should evaluate whether sufficient repair capability exists under the conditions that might occur if there were an active conflict and recommend such remediation steps as should be undertaken in the face of any deficiencies.

I. Expand Usage of Commercial Space-Based Capabilities

In the Ukraine-Russia war, commercial space capabilities have been critical to Ukraine's defense (as described above), as well as to maintaining governmental and economic functioning. The United States is already undertaking significant activities with the commercial space sector in the defense arena. The discussion below summarizes key elements of that effort and further proposes additional actions for the use of private-sector space capabilities that would enhance resilience in wartime for defense, government continuity, and the economy.

First, in the defense arena, commercial capabilities are being increasingly relied upon to meet the military's space launch requirements. Private-sector SpaceX Falcon 9 reusable rockets, which regularly put commercial satellites in place, have recently been used, for example, to launch "the first 10 of the planned 28 satellites [for defense] low-latency communications [and] missile warning/missile tracking."[106] That space architecture is planned to expand to 163 satellites.[107] Similarly, other companies such as Rocket Lab have commercial launch capabilities.[108] Continuing the use of commercial launch capabilities to generate military constellations as well assuring their availability in wartime will be critical to effective defense operations.

Second, and as the foregoing suggests, the proliferation of satellites that the DOD can rely on in wartime significantly adds to the resilience of the space enterprise. As one report describes:

> The use of small, inexpensive satellites in a pLEO [proliferated low-earth orbit] constellation also improves deterrence because of its increased cost imposition potential. The cost of a direct-ascent KE ASAT [kinetic antisatellite] is now greater than the target satellite, and because of the sheer number of assets an enemy must attack, proliferation reduces the effectiveness and impact of these weapons and other coorbital threats.[109]

Third, commercial sensing capabilities can complement the military's more exquisite sensing. Satellite companies such as Planet, Capella Space, and Maxar Technologies have supplied imagery upon Ukraine's request, as noted above.[110] The Defense Department has likewise been utilizing such commercial space-based, ground-sensing capabilities having, for example, recognized a "critical need for improved, large scale, situational awareness satisfied by less expensive, day/night, all-weather imaging satellites capable of filling gaps in space-based reconnaissance."[111] For example, Planet was awarded a National Reconnaissance Office (NRO) contract in October 2019 for "an unclassified, multi-year subscription service contract for daily, large-area, 3-5 meter resolution commercial imagery collection. . . . [for] access to new daily unclassified imagery over multiple areas of interest to military planners, warfighters, and the national security community."[112]

Moreover, commercial sensing is becoming increasingly capable, going beyond optical capabilities, with Umbra having launched commercial "radar-imaging" microsatellites whose capabilities can be used for "remote wildlife habitat protection, pollution and plastic waste tracking, oil spill detection, *military intelligence gathering* [italics added], live flooding estimation during storms, and more.[113]

The Defense Department also has been seeking to expand its "space domain awareness" through collaboration with the private sector. Maxar Technologies, for example, recently signed a contract with the NRO which "includes a provision to experiment with using its satellites to provide 'non-Earth' data, which includes high-resolution imagery of the space environment."[114] That effort would complement ongoing actions by Space Force, whose "fleet of radars, known as the Space Surveillance Network, observe space from the ground and feed data into com-

mand and control systems that catalog space objects" to deal both with issues of "congestion and debris in low Earth orbit . . . and aggression from adversaries like Russia and China."[115]

Fourth, the information and communications technology networks being established by commercial providers can themselves be utilized for wartime operations, again as has been demonstrated by the use of Starlink in Ukraine. But Starlink would not be the only provider. Currently, another constellation consisting "of small, low-cost satellites under 100 kilograms capable of multiple rapid-launch" is under development, based "on an orbital mesh network of . . . commercial and military microsatellites," which will be "capable of providing low-latency internet connectivity between sensors and weapons for military mission."[116] Future capabilities include the establishment of "free space optical networks" which will potentially have "immense benefits including high security, better data rates [and] fast installations, no requirement of licensed spectrum, best costs [and] simplicity of design," and will be challenging to detect and to intercept "in view of small divergence of the laser beams."[117]

Governments plan to develop position, navigation, and timing capabilities—now generally done in medium-Earth orbit by the Global Positioning System or equivalent satellites—with a variety of capabilities including but not limited to low-Earth orbit capabilities.[118] In the United States, Xona Space Systems is "developing PULSAR—a high-performance positioning, navigation, and timing (PNT) service enabled by a commercial constellation of dedicated [low-Earth orbit] satellites."[119]

Another application of commercial capabilities for defense space support is the use of the cloud for development of space-related software:

> The Space Development Agency awarded a $64 million contract to Science Applications International Corp. (SAIC) to develop a software applications factory for the agency's low Earth orbit constellation [but] . . not [by] build[ing] an actual factory but [rather] a cloud-based development process to design, test and update software applications using a repeatable path.[120]

In light of the very substantial ongoing interactions between the Department of Defense and the commercial space sector, as discussed above, the key issue for wartime is simply to ensure that the existing (and future) capabilities are available for use as required. That can be accomplished in the first instance by contractual arrangements along the lines of those utilized by DOD for support from the airline and maritime industries. By way of example, the Civil Reserve Air Fleet (CRAF) provides "selected aircraft from US airlines [which are] contractually committed to CRAF [to] augment Department of Defense airlift requirements in emergencies when the need for airlift exceeds the capability of military aircraft."[121]

The US Space Force is in process of developing the Commercial Augmentation Space Reserve (CASR) program. As with CRAF, CASR would seek to establish "voluntary pre-negotiated contractual arrangements" that would provide support to the military by ensuring that "services like satellite communication and remote sensing are prioritized for U.S. government use during national security emergencies."[122] Among the issues that Space Force presumably is discussing with the private sector in connection with CASR would be determining which services and in what amounts could reliably be provided in a wartime environment, whether such services could be based on existing (or planned) private-sector constellations or whether those would need to be expanded, what provisions would need to be made for satellite and/or ground station replacement in the event of adversary attacks, what provisions for indemnification need to be agreed upon, and what level of funding would be appropriate both to incentivize the private sector and to accomplish the requisite wartime tasks as well as to undertake planning and training prior to conflict.

Relatedly, it is worth noting that the Defense Production Act authorizes the government to require the prioritized provision of services—which would include services from space companies—and exempts any company receiving such an order from liabilities such as inability to support other customers.[123] However, it would be much more desirable—and much more effective—if the necessary arrangements were established in advance through a voluntary arrangement as the CASR program is seeking.

J. Authorities and Resources

Undertaking the actions recommended above will require some important changes to governmental authorities as well as the provision of additional resources necessary to accomplish the recommended outcomes.

Regarding authorities, the administration currently has the authority to establish a Critical Infrastructure Wartime Planning and Operations Council with government and private-sector membership (including, as requested, SLTTs); establish regional resilience collaboratives; and help facilitate the establishment of sector-specific coordinating mechanisms. The administration and the Congress should work together to establish the authorities necessary to:

- Create an Integrated Cybersecurity Providers Corps.
- Establish a national Cybersecurity Civilian Reserve Corps and expand National Guard cybersecurity capabilities.
- Authorize Cyber Command to support key critical infrastructures in wartime.
- Establish an international Undersea Infrastructure Protection Corps.
- Expand the use of private-sector space capabilities.

In undertaking such enactments as required, Congress should also evaluate whether any antitrust or other safe harbor exemptions would be necessary to allow for the desired level of collaboration.

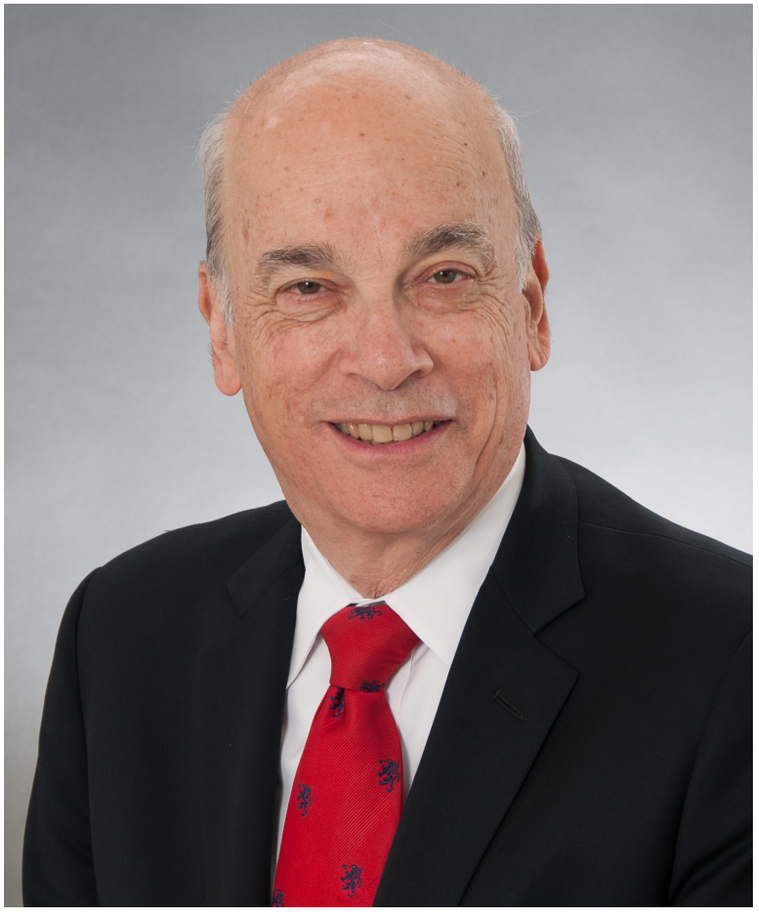
In terms of resources, funding, as noted above, will be required for each of the recommended activities. Including such costs as line items in the Defense Department budget would be appropriate to support each of the proposed activities as the activities are all to be undertaken in support of national defense in a wartime context. As a complement to line-item budgeting, Congress might also consider authorizing the use of transferable tax credits, which could be utilized as payment in order to offset the costs of the provision of capabilities and services prior to or in wartime.[124] The precise nature of the funding arrangement might differ among the different activities. Space Force's CASR initiative is a useful model but whatever the precise mechanism, it is important to recognize that the private sector would incur potentially significant costs including pre-conflict planning and training activities, and that those are being undertaken to support national defense.

Conclusion

The United States has made significant efforts in enhancing the resilience of critical infrastructures, but has not yet focused on how to support those infrastructures in wartime. The recommendations in this report provide a basis for such an effort. That effort should start now. Indeed, one of the lessons from Ukraine's wartime experience is the importance of beginning as soon as possible. As one analysis states:

> others seeking to replicate Ukraine's model of success should recognise that building an effective cyber-defence posture is a marathon, not a sprint. Ukraine's capacity to withstand Russia's offensive stems from incremental improvements in its cyber defences over years of painstaking effort and investment. The specific plans and contingencies developed for the war would not have been possible without modernising national cyber-defence systems and raising the maturity levels of public and private critical infrastructure providers in the years leading up to the invasion. Take for example the unprecedented levels of threat intelligence sharing from external partners—undeniably a significant boon to Ukrainian situational awareness and ability to detect emerging threats. Without prior efforts to close visibility gaps, train defenders and adopt a more active cyber-defence posture, the ability to integrate and exploit this intelligence at scale would have been severely limited.[125]

The private sector will have important roles in any future conflict in which the United States engages. To maximize that potential, there needs to be active development of the sixth domain, with the private sector being fully included in wartime constructs, plans, preparations, and actions, as recommended in this report.



ABOUT THE AUTHOR

Franklin D. Kramer is a distinguished fellow and board director at the Atlantic Council. Kramer has served as a senior political appointee in two administrations, including as assistant secretary of defense for international security affairs. At the Department of Defense, Kramer was in charge of the formulation and implementation of international defense and political-military policy, with worldwide responsibilities including NATO and Europe, the Middle East, Asia, Africa, and Latin America.

In the nonprofit world, Kramer has been a senior fellow at CNA; chairman of the board of the World Affairs Council of Washington, DC; a distinguished research fellow at the Center for Technology and National Security Policy of the National Defense University; and an adjunct professor at the Elliott School of International Affairs of The George Washington University. Kramer's areas of focus include defense, both conventional and hybrid; NATO and Russia; China, including managing competition, military power, economics and security, and China-Taiwan-US relations; cyber, including resilience and international issues; innovation and national security; and irregular conflict and counterinsurgency.

Kramer has written extensively. In addition to the current report, recent publications include *China and the New Globalization; Free but Secure Trade; NATO Deterrence and Defense: Military Priorities for the Vilnius Summit; NATO Priorities: Initial Lessons from the Russia-Ukraine War;* "Here's the 'Concrete' Path for Ukraine to Join NATO"; and *Providing Long-Term Security for Ukraine: NATO Membership and Other Security Options.*

Endnotes

1. "Multi-Domains Operations Conference—What We Are Learning," Allied Command Transformation, April 8, 2022, https://www.act.nato.int/articles/multi-domains-operations-lessons-learned.
2. Christine H. Fox and Emelia S. Probasco, "Big Tech Goes to War," *Foreign Affairs,* October 19, 2022, https://www.foreignaffairs.com/ukraine/big-tech-goes-war.
3. Department of Defense (DOD), *2022 National Defense Strategy*, 7, https://media.defense.gov/2022/Oct/27/2003103845/-1/-1/1/2022-NATIONAL-DEFENSE-STRATEGY-NPR-MDR.PDF.
4. The report elaborates on the discussion of the private sector and the sixth domain in Franklin D. Kramer, *NATO Deterrence and Defense: Military Priorities for the Vilnius Summit, Atlantic Council,* April 18, 2023, https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/nato-summit-military-priorities/.
5. PPD-21 is in process of being updated. Tim Starks, "A Presidential Critical Infrastructure Protection Order Is Getting a Badly Needed Update, Officials Say," *Washington Post,* May 11, 2023, https://www.washingtonpost.com/politics/2023/05/11/presidential-critical-infrastructure-protection-order-is-getting-badly-needed-update-officials-say/.
6. White House, "Presidential Policy Directive—Critical Infrastructure Security and Resilience," February 12, 2013, https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil; William M. (Mac) Thornberry National Defense Authorization Act For Fiscal Year 2021, Pub. L. No. 116–283, 134 Stat. 3388 (2021), https://www.congress.gov/116/plaws/publ283/PLAW-116publ283.pdf; Cybersecurity and Infrastructure Security Agency (CISA), *National Infrastructure Protection Plan and Resources,* accessed July 6, 2023, https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/national-infrastructure-protection-plan-and-resources; CISA, "About CISA," accessed July 6, 2023, https://www.cisa.gov/about.
7. DOD, *National Defense Strategy 2022,* 5.
8. "Statement of General Glen D. VanHerck, Commander, United States Northern Command and North American Aerospace Defense Command Before the Senate Armed Services Committee," March 23, 2023, 8-9, https://www.armed-services.senate.gov/imo/media/doc/NNC_FY23%20Posture%20Statement%2023%20March%20SASC%20FINAL.pdf.
9. CISA, "The Attack on Colonial Pipeline: What We've Learned & What We've Done Over the Past Two Years," May 7, 2023, https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years; Saheed Oladimeji and Sean Michael Kerner, "SolarWinds Hack Explained: Everything You Need to Know," Tech Target, June 27, 2023, https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know; and "Stop Ransomware," CISA (website), accessed July 6, 2023, https://www.cisa.gov/stopransomware/resources.
10. Office of the Director of National Intelligence (ODNI), *Annual Threat Assessment of the U.S. Intelligence Community,* February 6, 2023, 12, https://www.dni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf.
11. ODNI, *Annual Threat Assessment,* 14.
12. ODNI, *Annual Threat Assessment,* 10.
13. David E. Sanger and Julian E. Barnes, "U.S. Hunts Chinese Malware That Could Disrupt American Military Operations," *New York Times,* July 29, 2023, https://www.nytimes.com/2023/07/29/us/politics/china-malware-us-military-bases-taiwan.html.
14. Cyber Peace Institute, "Case Study, Viasat," June 2022, https://cyberconflicts.cyberpeaceinstitute.org/law-and-policy/cases/viasat. The case study describes the breath of the impact: "The attack on Viasat also impacted a major German energy company who lost remote monitoring access to over 5,800 wind turbines, and in France nearly 9,000 subscribers of a satellite internet service provider experienced an internet outage. In addition, around a third of 40,000 subscribers of another satellite internet service provider in Europe (Germany, France, Hungary, Greece, Italy, Poland) were affected. Overall, this attack impacted several thousand customers located in Ukraine and tens of thousands of other fixed broadband customers across Europe."
15. Microsoft Threat Intelligence, "A Year of Russian Hybrid Warfare in Ukraine," March 15, 2023, 19, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW10mGC.
16. DOD, *Military and Security Developments Involving the People's Republic of China 2022,* 127, https://media.defense.gov/2022/Nov/29/2003122279/-1/-1/1/2022-military-and-security-developments-involving-the-peoples-republic-of-china.pdf.
17. Irene Sánchez Cózar and José Ignacio Torreblanca, "Ukraine One Year On: When Tech Companies Go to War," European Council on Foreign Relations, March 7, 2023, https://ecfr.eu/article/ukraine-one-year-on-when-tech-companies-go-to-war/.

18. Ariel E. Levite, *Integrating Cyber Into Warfighting: Some Early Takeaways from the Ukraine Conflict,* Working Paper, Carnegie Endowment for International Peace, April 2023, 14, https://carnegieendowment.org/files/Levite_Ukraine_Cyber_War.pdf.

19. Elias Groll and Aj Vicens, "A Year After Russia's Invasion, the Scope of Cyberwar in Ukraine Comes into Focus," *CyberScoop,* February 24, 2023, https://cyberscoop.com/ukraine-russia-cyberwar-anniversary/.

20. Groll and Vicens, "A Year After Russia's Invasion."

21. Groll and Vicens, "A Year After Russia's Invasion." A report from Google, *Fog of War: How the Ukraine Conflict Transformed the Cyber Threat Landscape,* underscores the "unprecedented" nature of the efforts including "expanded eligibility for Project Shield, our free protection against distributed denial of service attacks (DDoS), so that Ukrainian government websites and embassies worldwide could stay online and continue to offer critical services" as well as "rapid Air Raid Alerts system for Android phones in the region; support for refugees, businesses, and entrepreneurs . . . and "compromise assessments, incident response services, shared cyber threat intelligence, and security transformation services—to help detect, mitigate and defend against cyber attacks." See Threat Analysis Group, *Fog of War,* Google, February 2023, 2, https://services.google.com/fh/files/blogs/google_fog_of_war_research_report.pdf.

22. Dan Black, *Russia's War in Ukraine: Examining the Success of Ukrainian Cyber Defences,* International Institute for Strategic Studies, March 2023, 14, https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/2023/03/russias-war-in-ukraine-examining-the-success-of-ukrainian-cyber-defences.pdf.

23. Emma Schroeder and Sean Dack, *A Parallel Terrain: Public-Private Defense of the Ukrainian Information Environment,* Atlantic Council, February 2023, 14, https://www.atlanticcouncil.org/wp-content/uploads/2023/02/A-Parallel-Terrain.pdf.

24. Black, *Russia's War in Ukraine,* 17-18.

25. Schroeder and Dack, *A Parallel Terrain,* 16.

26. Fox and Probasco, *"Big Tech Goes to War,"* 4.

27. Levite, *Integrating Cyber Into Warfighting,* 17-18.

28. Robin Fontes and Jorrit Kamminga, "Ukraine: A Living Lab for AI Warfare," *National Defense,* March 24, 2023, https://www.nationaldefensemagazine.org/articles/2023/3/24/ukraine-a-living-lab-for-ai-warfare; their report notes that "the Russia-Ukraine war can also be considered the first conflict where AI-enhanced facial recognition software has been used on a substantial scale. In March 2022, Ukraine's defense ministry started using facial recognition software produced by the U.S. company Clearview AI. This allows Ukraine to identify dead soldiers and to uncover Russian assailants and combat misinformation. What's more, AI is playing an important role in electronic warfare and encryption. For example, the U.S. company Primer has deployed its AI tools to analyze unencrypted Russian radio communications. This illustrates how AI systems were constantly retrained and adapted, for example, to deal with idiosyncrasies in customized ways, such as colloquial terms for weaponry."

29. Fontes and Kamminga, "Ukraine: A Living Lab"; they also note that AI has also been used for the "spread of misinformation and the use of deep fakes as part of information warfare. AI has, for example, been used to create face images for fake social media accounts used in propaganda campaigns. While the spread of disinformation is not new, AI offers unprecedented opportunities for scaling and targeting such campaigns, especially in combination with the broad range of social media platforms."

30. Levite, *Integrating Cyber Into Warfighting,* 17.

31. White House, "Presidential Policy Directive—Critical Infrastructure Security and Resilience, Definitions," February 12, 2013, https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

32. Government Accountability Office (GAO), *Critical Infrastructure Protection: Time Frames to Complete DHS Efforts Would Help Sector Risk Management Agencies Implement Statutory Responsibilities,* February 2023, 7, https://www.gao.gov/assets/gao-23-105806.pdf.

33. GAO, *Critical Infrastructure Protection.*

34. GAO, *Critical Infrastructure Protection,* 11.

35. GAO, *Critical Infrastructure Protection,* 8.

36. CISA, "FSLC Charter and Membership," accessed July 6, 2023, https://www.cisa.gov/fslc-charter-and-membership; CISA, "Critical Infrastructure Partnership Advisory Council (CIPAC)," accessed July 6, 2023, https://www.cisa.gov/resources-tools/groups/critical-infrastructure-partnership-advisory-council-cipac; CISA, "Government Coordinating Councils," accessed July 6, 2023), https://www.cisa.gov/resources-tools/groups/government-coordinating-councils; and CISA, "Sector Coordinating Councils," accessed July 6, 2023, https://www.cisa.gov/resources-tools/groups/sector-coordinating-councils.

37. White House, "Office of National Cyber Director," accessed July 6, 2023, https://www.whitehouse.gov/oncd/.

38. White House, *National Cybersecurity Strategy Implementation Plan,* July 2023, https://www.whitehouse.gov/wp-content/uploads/2023/07/National-Cybersecurity-Strategy-Implementation-Plan-WH.gov_.pdf.

39. Transportation Security Administration (TSA), "TSA Issues New Cybersecurity Requirements for Airport and Aircraft Operators," March 7, 2023, https://www.tsa.gov/news/press/releases/2023/03/07/tsa-issues-new-cybersecurity-requirements-airport-and-aircraft; TSA, "TSA Issues New Cybersecurity Requirements for Passenger and Freight Railroad Carriers," October 18, 2022, https://www.tsa.gov/news/press/releases/2022/10/18/tsa-issues-new-cybersecurity-requirements-passenger-and-freight; TSA, "TSA Revises and Reissues Cybersecurity Requirements for Pipeline Owners and Operators, July 21, 2022, https://www.tsa.gov/news/press/releases/2022/07/21/tsa-revises-and-reissues-cybersecurity-requirements-pipeline-owners; and Environmental Protection Agency, "EPA Cybersecurity for the Water Sector," accessed July 6, 2023, https://www.epa.gov/waterriskassessment/epa-cybersecurity-water-sector.

40. CISA, "State and Local Cybersecurity Grant Program," accessed July 4, 2023, https://www.cisa.gov/state-and-local-cybersecurity-grant-program.

41. CISA, "JCDC FAQs, What Are JCDC's Core Functions," accessed June 24, 2023, https://www.cisa.gov/topics/partnerships-and-collaboration/joint-cyber-defense-collaborative/jcdc-faqs.

42. CISA, "Cybersecurity Training and Exercises," accessed July 4, 2023, https://www.cisa.gov/cybersecurity-training-exercises.

43. CISA, "JCDC 2023 Planning Agenda," accessed June 24, 2023, https://www.cisa.gov/topics/partnerships-and-collaboration/joint-cyber-defense-collaborative/2023-jcdc-planning-agenda.

44. CISA, "JCDC 2023 Planning Agenda."

45. CISA, "JCDC 2023 Planning Agenda."

46. "National Cyber Investigative Joint Task Force," Federal Bureau of Investigation, accessed July 18, 2023, https://www.fbi.gov/investigate/cyber/national-cyber-investigative-joint-task-force; White House, *National Cybersecurity Strategy Implementation Plan,* July 2023, 21, https://www.whitehouse.gov/wp-content/uploads/2023/07/National-Cybersecurity-Strategy-Implementation-Plan-WH.gov_.pdf.

47. National Security Agency, NSA Cybersecurity Collaboration Center, accessed September 7, 2023, https://www.nsa.gov/About/Cybersecurity-Collaboration-Center/.

48. Government of Finland, Ministry of Defense, Security Committee, *Security Strategy for Society,* November 2, 2017, 98, https://turvallisuuskomitea.fi/wp-content/uploads/2018/04/YTS_2017_english.pdf.

49. Government of Finland, *Security Strategy for Society,* 5.

50. Government of Finland, *Security Strategy for Society,* 5.

51. Government of Finland, *Security Strategy for Society,* 7.

52. Government of Finland, *Security Strategy for Society,* 7-8.

53. CISA, *Federal Senior Leadership Council Charter,* accessed July 4, 2023, https://www.cisa.gov/sites/default/files/publications/fslc-charter-2021-508.pdf.

54. The FBI-led National Cybersecurity Investigative Joint Task Force is, of course, a joint task force, but it is not oriented to wartime activities.

55. The *National Cybersecurity Implementation Plan* requires DOD to issue an "updated DOD cyber strategy," and while the full scope of homeland defense goes beyond cyber, the two efforts might be undertaken in a coordinated fashion. White House, *National Cybersecurity Strategy Implementation Plan,* July 2023, 21, https://www.whitehouse.gov/wp-content/uploads/2023/07/National-Cybersecurity-Strategy-Implementation-Plan-WH.gov_.pdf.

56. Northern Command, "Defending the Homeland," accessed July 6, 2023, https://www.northcom.mil/HomelandDefense.

57. Government of Finland, *Security Strategy for Society,* 10.

58. CISA, "CISA Regional Office Fact Sheets," August 4, 2021, https://www.cisa.gov/resources-tools/resources/cisa-regional-office-fact-sheets; and CISA, "State and Local Cybersecurity Grant Program."

59. Section 331(c)(1)(a), Senate Armed Services Committee, National Defense Authorization Act for Fiscal Year 2024, accessed September 2, 2023, https://www.armed-services.senate.gov/imo/media/doc/fy24_ndaa_bill_text.pdf.

60. Section 331(d), Senate Armed Services Committee, National Defense Authorization Act for Fiscal Year 2024, accessed September 2, 2023, https://www.armed-services.senate.gov/imo/media/doc/fy24_ndaa_bill_text.pdf.

61. Section 331(c)(2), Senate Armed Services Committee, National Defense Authorization Act for Fiscal Year 2024, accessed September 2, 2023,

https://www.armed-services.senate.gov/imo/media/doc/fy24_ndaa_bill_text.pdf.

62. CISA, "Information Sharing: A Vital Resource," accessed July 2, 2023, https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/information-sharing-vital-resource.

63. Analysis and Resilience Center for Systemic Risk, "Who We Are," https://systemicrisk.org/.

64. Analysis and Resilience Center for Systemic Risk, "What We Do," https://systemicrisk.org/.

65. FS-ISAC, "Critical Providers Program FAQ," accessed July 2, 2023, https://www.fsisac.com/faq-criticalproviders.

66. FS-ISAC, "Critical Providers."

67. White House, *National Cybersecurity Strategy,* March 2023, 4, https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.

68. The *National Cybersecurity Strategy Implementation Plan* takes a step in this direction by requiring the Department of Commerce to publish a "Notice of Proposed rulemaking on requirements, standards, and procedures for Infrastructure-as-a-Service (IaaS) providers and resellers." White House, *National Cybersecurity Strategy Implementation Plan,* July 2023, 25, https://www.whitehouse.gov/wp-content/uploads/2023/07/National-Cybersecurity-Strategy-Implementation-Plan-WH.gov_.pdf.

69. CISA, "Support to Critical Infrastructure at Greatest Risk, ('Section 9 Report') Summary," February 8, 2021, https://www.cisa.gov/resources-tools/resources/support-critical-infrastructure-greatest-risk-section-9-report-summary.

70. "Census Bureau Reports There Are 89,004 Local Governments in the United States," US Census Bureau, August 30, 2012, https://www.census.gov/newsroom/releases/archives/governments/cb12-161.html.

71. "Amendment to Rules Comm. Print 118–10 Offered by Mr. Green of Tennessee," June 27, 2023, https://amendments-rules.house.gov/amendments/Cyber%20in%20National%20Guard%20Amendment230630140357934.pdf.

72. Section 1521, Rules Committee Print 118–10 Text of H.r. 2670, The National Defense Authorization Act for Fiscal Year 2024, June 23, 2023, https://rules.house.gov/sites/republicans.rules118.house.gov/files/RCP_xml_1.pdf.

73. Office of Senator Jacky Rosen, "Rosen, Blackburn Introduce Bipartisan Bills to Strengthen Federal Response to Cyberattacks," March 21, 2023, https://www.rosen.senate.gov/2023/03/21/rosen-blackburn-introduce-bipartisan-bills-to-strengthen-federal-response-to-cyberattacks/.

74. Section 1116, Senate Armed Services Committee, National Defense Authorization Act for Fiscal Year 2024, accessed September 2, 2023, https://www.armed-services.senate.gov/imo/media/doc/fy24_ndaa_bill_text.pdf.

75. Black, *Russia's War in Ukraine,* 14.

76. "Joint Cyber Reserve Force," Gov.UK, accessed June 3, 2023, https://www.gov.uk/government/groups/joint-cyber-reserve-force.

77. Republic of Estonia, Information System Authority, "Cyber Security in Estonia 2023," 51, https://www.ria.ee/media/2702/download.

78. National Guard, National Guard Cyber Defense Team, accessed September 2, 2023, https://www.nationalguard.mil/Portals/31/Resources/Fact%20Sheets/Cyber%20Defense%20Team%202022.pdf.

79. Franklin D. Kramer and Robert J. Butler, "Expanding the Role of the National Guard for Effective Cybersecurity," *The Hill*, April 21, 2021, https://thehill.com/opinion/cybersecurity/550740-expanding-the-role-of-the-national-guard-for-effective-cybersecurity/.

80. Mark Pomerleau, "Lawmakers Pushing for More Integration of National Guard, Reserve Personnel into DOD Cyber Forces," Defensescoop, June 12, 2023, https://defensescoop.com/2023/06/12/lawmakers-pushing-for-more-integration-of-national-guard-reserve-personnel-into-dod-cyber-forces/.

81. Cyber Command, "Hunt Forward Operations," November 15, 2022, https://www.cybercom.mil/Media/News/Article/3218642/cyber-101-hunt-forward-operations/.

82. "2023 Posture Statement of General Paul M. Nakasone," US Cyber Command, March 7, 2023, https://www.cybercom.mil/Media/News/Article/3320195/2023-posture-statement-of-general-paul-m-nakasone/.

83. Cyber Command, "Hunt Forward Operations."

84. Cyber Command, "Hunt Forward Operations."

85. This is a nontrivial requirement, as there is a significant shortage of highly skilled cyber talent, and retaining such talent has been a challenge for US Cyber Command. As Gen. Nakasone recently observed, "someone that has this type of training is very, very attractive to those on the outside." Jim Garamone, "Cyber Command, NSA Successes Point Way to Future," DOD News, March 8, 2023, https://www.defense.gov/News/

News-Stories/Article/Article/3322765/cyber-command-nsa-successes-point-way-to-future/.

86. There are important legal issues regarding the interface between the Fourth Amendment and constitutional wartime powers, but establishing a consensual regime—which should be in the self-interest of critical infrastructures—would avoid those questions.

87. There are approximately 550 existing and planned undersea cables; see TeleGeography, "Submarine Cable Frequently Asked Questions," accessed July 2, 2023, https://www2.telegeography.com/submarine-cable-faqs-frequently-asked-questions. There are far fewer undersea pipelines, but for Europe, important pipelines include those in the North, Baltic, and Mediterranean seas with "about 8,000 kilometers (5,000 miles) of oil and gas pipelines crisscross[ing] the North Sea alone." Lorne Cook, "NATO Moves to Protect Undersea Pipelines, Cables as Concern Mounts over Russian Sabotage Threat," Associated Press, June 16, 2023, https://apnews.com/article/nato-russia-sabotage-pipelines-cables-infrastructure-507929033b05b5651475c8738179ba5c.

88. There is at least some indication that Ukraine undertook those Nord Stream actions. See Julian E. Barnes and Michael Schwirtz, "C.I.A. Told Ukraine Last Summer It Should Not Attack Nord Stream Pipelines," *New York Times,* June 13, 2023, https://www.nytimes.com/2023/06/13/us/politics/nord-stream-pipeline-ukraine-cia.html.

89. White House, "G7 Hiroshima Leaders' Communiqué," May 20, 2023, paragraph 39, https://www.whitehouse.gov/briefing-room/statements-releases/2023/05/20/g7-hiroshima-leaders-communique/.

90. White House, "Quad Leaders' Summit Fact Sheet," May 20, 2023, https://www.whitehouse.gov/briefing-room/statements-releases/2023/05/20/quad-leaders-summit-fact-sheet/.

91. Though there is at least some indication that Ukraine undertook the Nord Stream actions. Barnes and Schwirtz, "C.I.A. Told Ukraine Last Summer It Should Not Attack Nord Stream Pipelines."

92. Jens Stoltenberg, "Press Conference by NATO Secretary General Jens Stoltenberg Following the Meeting of NATO Ministers of Defense in Brussels," Remarks (as delivered), NATO, June 16, 2023, https://www.nato.int/cps/en/natohq/opinions_215694.htm?selectedLocale=en.

93. Christian Bueger, Tobias Liebetrau, and Jonas Franken, *Security Threats to Undersea Communications Cables and Infrastructure–Consequences for the EU,* In-Depth Analysis Requested by the SEDE Sub-committee, European Parliament, June 2022, 31, https://www.europarl.europa.eu/RegData/etudes/IDAN/2022/702557/EXPO_IDA(2022)702557_EN.pdf.

94. The Maritime Centre for the Security of Critical Undersea Infrastructure will be based in Northwood near London. NATO had earlier set up a coordination cell in Brussels to better monitor pipelines and subsea cables that are deemed especially endangered by underwater drones and submarines. See "NATO to Set Up New Unit to Monitor Pipelines/Other Critical Infrastructure," *Pipeline Technology Journal,* June 19, 2023, https://www.pipeline-journal.net/news/nato-set-new-unit-monitor-pipelines-other-critical-infrastructure.

95. Stoltenberg, "Press Conference."

96. Stoltenberg, "Press Conference."

97. "Frequently Asked Questions, Submarine Cable Systems Market," MarketsandMarkets, accessed July 1, 2023, https://www.marketsandmarkets.com/Market-Reports/submarine-cable-system-market-184625.html.

98. "Submarine Cable Frequently Asked Questions," TeleGeography, accessed July 1, 2023.

99. "Underwater Arteries—the World's Longest Offshore Pipelines," Offshore Technology, September 9, 2014, https://www.offshore-technology.com/features/featureunderwater-arteries-the-worlds-longest-offshore-pipelines-4365616/; "After Nord Stream Attack, Europe Scrambles to Secure Subsea Pipelines," *Maritime Executive,* October 2, 2022, https://maritime-executive.com/article/after-nord-stream-attack-europe-scrambles-to-secure-subsea-pipelines; "Gulf of Mexico Data Atlas," National Centers for Environmental Information ("There are over 26,000 miles of oil and gas pipeline on the Gulf of Mexico seafloor,"), accessed July 1, 2023, https://www.ncei.noaa.gov/maps/gulf-data-atlas/atlas.htm?plate=Gas%20and%20Oil%20Pipelines.

100. "After Nord Stream Attack," *Maritime Executive*; and Christiana Gallardo, "UK and Norway Team Up to Protect Undersea Cables, Gas Pipes in Wake of Nord Stream Attacks," *Politico,* June 28, 2023, https://www.politico.eu/article/uk-norway-team-up-protect-undersea-cables-gas-pipelines/.

101. For a series of specific recommendations, see Sherman, *Cyber Defense Across the Ocean Floor.*

102. John Arquila, "Securing the Undersea Cable Network," Hoover Institution, 2023, 4, https://www.hoover.org/sites/default/files/research/docs/Arquilla_SecuringUnderseaCable_FINAL_0.pdf.

103. Arquila, "Securing the Undersea Cable Network," 8, 9.

104. For recommendations on enhancing the cybersecurity of undersea cables, see also Justin Sherman, *Cyber Defenses Across the Ocean Floor,* Atlantic Council, September 2021, https://www.atlanticcouncil.org/in-depth-research-reports/report/cyber-defense-across-the-ocean-floor-the-

geopolitics-of-submarine-cable-security/.

105. Mick Green et al., "Submarine Cable Network Security," Slide Deck, International Cable Protection Committee, April 13, 2009, https://www.iscpc.org/publications/.

106. Bueger, Liebetrau, and Franken, "Security Threats to Undersea Communications Cables," 53.

107. DOD, "Space Development Agency Successfully Launches Tranche 0 Satellites," April 2, 2023, https://www.defense.gov/News/Releases/Release/Article/3348974/space-development-agency-successfully-launches-tranche-0-satellites/.

108. DOD, "Space Development Agency."

109. Rocket Lab, "About Us," accessed July 5, 2023, https://www.rocketlabusa.com/about/about-us/.

110. Charles S. Galbreath, "Building U.S. Space Force Counterspace Capabilities: An Imperative for America's Defense," Mitchell Institute, June 2023, 16, https://mitchellaerospacepower.org/wp-content/uploads/2023/06/Building-US-Space-Force-Counterspace-Capabilities-FINAL2.pdf.

111. Fontes and Kamminga, "Ukraine: A Living Lab."

112. "Planet Labs, Inc.—Peacetime Indications & Warning," Defense Innovation Unit (DIU), 2019, https://www.diu.mil/solutions/portfolio/catalog/a0Tt0000009En0yEAC-a0ht000000AYgyYAAT.

113. "Planet Labs," DIU.

114. "Umbra Launches World's Most Capable Commercial Radar-Imaging Satellite," Umbra, June 25, 2021, https://umbra.space/blog/umbra-launches-worlds-most-capable-commercial-radar-imaging-satellite.

115. Courtney Albon, "Maxar Explores New Uses for Earth Observation Satellites," *C4ISRNET,* May 30, 2023, https://www.c4isrnet.com/battlefield-tech/space/2023/05/30/maxar-explores-new-uses-for-earth-observation-satellites/.

116. Albon, "Maxar Explores New Uses."

117. *Offset-X: Closing the Deterrence Gap and Building the Future Joint Force,* Special Competitive Studies Project (a bipartisan, nonprofit effort), May 2023, 51, https://www.scsp.ai/wp-content/uploads/2023/05/Offset-X-Closing-the-Detterence-Gap-and-Building-the-Future-Joint-Force.pdf.

118. Suresh Kumar and Nishant Sharma, "Emerging Military Applications of Free Space Optical Communication Technology: A Detailed Review," *2022 Journal of Physics Conference Series* (2022), 1, https://iopscience.iop.org/article/10.1088/1742-6596/2161/1/012011/pdf.

119. The European Commission has undertaken an evaluation of seven different systems that it found to have met technical requirements. See L. Bonenberg, B. Motella, and J. Fortuny Guasch, *Assessing Alternative Positioning, Navigation and Timing Technologies for Potential Deployment in the EU*, JRC Science for Policy Report, EUR 31450 EN (Luxembourg: Publications Office of the European Union, 2023), https://doi.org/10.2760/596229.

120. "Safran to Provide GNSS Simulation Solutions for Xona Space System's Low-Earth-Orbit Constellation and Navigation Signal," *Electronic Engineering Journal,* April 6, 2023, https://www.eejournal.com/industry_news/safran-to-provide-gnss-simulation-solutions-for-xona-space-systems-low-earth-orbit-constellation-and-navigation-signals/.

121. Sandra Erwin, "SAIC to Develop 'Software Factory' for Space Development Agency," *SpaceNews,* June 8, 2023, https://spacenews.com/saic-to-develop-software-factory-for-space-development-agency/.

122. US Air Force, "Civil Reserve Air Fleet," accessed July 4, 2023, https://www.af.mil/About-Us/Fact-Sheets/Display/Article/104583/civil-reserve-air-fleet/.

123. Sandra Erwin, "Space Force to Further Define Details of a 'Commercial Space Reserve'", *Space News,* July 25, 2023, https://spacenews.com/space-force-to-further-define-details-of-a-commercial-space-reserve/.

124. 50 US Code, §§ 4511 and 4557.

125. See Franklin D. Kramer, Melanie J. Teplinsky, and Robert J. Butler, "We Need a Cybersecurity Paradigm Change," *The Hill,* February 15, 2022, https://thehill.com/opinion/cybersecurity/594296-we-need-a-cybersecurity-paradigm-change/.

126. Black, *Russia's War in Ukraine,* 39.

Atlantic Council

Board of Directors

CHAIRMAN
*John F.W. Rogers

EXECUTIVE CHAIRMAN EMERITUS
*James L. Jones

PRESIDENT AND CEO
*Frederick Kempe

EXECUTIVE VICE CHAIRS
*Adrienne Arsht
*Stephen J. Hadley

VICE CHAIRS
*Robert J. Abernethy
*Alexander V. Mirtchev

TREASURER
*George Lund

DIRECTORS
Stephen Achilles
Gina F. Adams
Timothy D. Adams
*Michael Andersson
Barbara Barrett
Colleen Bell
Sarah E. Beshar
Stephen Biegun
Linden P. Blue
Adam Boehler
John Bonsell
Philip M. Breedlove
Richard R. Burt
*Teresa Carlson
*James E. Cartwright
John E. Chapoton
Ahmed Charai
Melanie Chen
Michael Chertoff
*George Chopivsky
Wesley K. Clark
*Helima Croft
*Ankit N. Desai
Dario Deste
Lawrence Di Rita
*Paula J. Dobriansky
Joseph F. Dunford, Jr.
Richard Edelman
Thomas J. Egan, Jr.
Stuart E. Eizenstat
Mark T. Esper
*Michael Fisch
Alan H. Fleischmann
Jendayi E. Frazer
Meg Gentle
Thomas H. Glocer
John B. Goodman
*Sherri W. Goodman
Marcel Grisnigt
Jarosław Grzesiak
Murathan Günal
Michael V. Hayden
Tim Holt
*Karl V. Hopkins
Kay Bailey Hutchison
Ian Ihnatowycz
Mark Isakowitz
Wolfgang F. Ischinger
Deborah Lee James
*Joia M. Johnson
*Safi Kalo
Andre Kelleners
Brian L. Kelly
Henry A. Kissinger
John E. Klein
*C. Jeffrey Knittel
Joseph Konzelmann
Keith Krach
Franklin D. Kramer
Laura Lane
Almar Latour
Yann Le Pallec
Jan M. Lodal
Douglas Lute
Jane Holl Lute
William J. Lynn
Mark Machin
Marco Margheri
Michael Margolis
Chris Marlin
William Marron
Gerardo Mato
Erin McGrain
John M. McHugh
*Judith A. Miller
Dariusz Mioduski
*Richard Morningstar
Georgette Mosbacher
Majida Mourad
Virginia A. Mulberger
Mary Claire Murphy
Julia Nesheiwat
Edward J. Newberry
Franco Nuschese
Joseph S. Nye
Ahmet M. Ören
Sally A. Painter
Ana I. Palacio
*Kostas Pantazopoulos
Alan Pellegrini
David H. Petraeus
*Lisa Pollina
Daniel B. Poneman
*Dina H. Powell McCormick
Michael Punke
Ashraf Qazi
Thomas J. Ridge
Gary Rieschel
Michael J. Rogers
Charles O. Rossotti
Harry Sachinis
C. Michael Scaparrotti
Ivan A. Schlager
Rajiv Shah
Gregg Sherrill
Jeff Shockey
Ali Jehangir Siddiqui
Kris Singh
Varun Sivaram
Walter Slocombe
Christopher Smith
Clifford M. Sobel
Michael S. Steele
Richard J.A. Steele
Mary Streett
Nader Tavakoli
*Gil Tenzer
*Frances F. Townsend
Clyde C. Tuggle
Melanne Verveer
Charles F. Wald
Michael F. Walsh
Ronald Weiser
*Al Williams
Ben Wilson
Maciej Witucki
Neal S. Wolin
*Jenny Wood
Guang Yang
Mary C. Yates
Dov S. Zakheim

HONORARY DIRECTORS
James A. Baker, III
Robert M. Gates
James N. Mattis
Michael G. Mullen
Leon E. Panetta
William J. Perry
Condoleezza Rice
Horst Teltschik
William H. Webster

**Executive Committee Members*

List as of July 5, 2023

The Atlantic Council is a nonpartisan organization that promotes constructive US leadership and engagement in international affairs based on the central role of the Atlantic community in meeting today's global challenges.

Atlantic Council

1030 15th Street, NW, 12th Floor,
Washington, DC 20005

(202) 463-7226, www.AtlanticCouncil.org