The Cyber Pandemic that Could Redefine the Great Power Competition: Preparing the Defense Industrial Base

Adib Farhadi, PhD, Ian Galloway, and Ayman Bekdash

Abstract The Fourth Industrial Revolution (4IR) stands poised to transform the geopolitics and geoeconomics of the Great Power Competition (GPC) as digital and cyber worlds permeate societies, governments, and nation-states. The United States must reconceptualize its public–private approach to cybersecurity, starting with the Defense Industrial Base (DIB). As policymakers continue to grapple with the COVID-19 pandemic, the World Economic Forum (WEF) warns that "we should prepare for a COVID-like global cyber pandemic that will spread faster and further than a biological virus, with an equal or greater economic impact" (Davis & Pipkaite in What the COVID-19 pandemic teaches us about cybersecurity—And how to prepare for the inevitable global cyberattack. World Economic Forum, 2020, [3]). Despite this warning, the new cybersecurity regulations being rolled out under what is commonly known as Cybersecurity Maturity Model Certification (CMMC) are inadequate to protect the DIB from future cyber threats. Underpinned by the conceptual framework of stakeholder capitalism, this chapter posits that cybersecurity regulations must be reimagined to foster greater process and systems agility, transparency, and trust between the government and the private sector.

Keywords Great power competition · Cyber security · Defense industrial base

Introduction

Data and technology form the most critical foundations of today's digital era. Near-complete digitization of nearly every critical process and system means that cyber-disruptions can set off a chain of events that culminates in the failure of an entire system. The global community no longer enjoys the luxury of moving back to an analog era—we are too dependent on new technology, too dependent on data, and

A. Farhadi (✉)
University of South Florida, Tampa, FL 33620, USA
e-mail: farhadi@usf.edu

I. Galloway · A. Bekdash
DGC International, McLean, VA 22102, USA

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2022

A. Farhadi et al. (eds.), *The Great Power Competition Volume 3*,
https://doi.org/10.1007/978-3-031-04586-8_11

too dependent on the Internet of Things (IoT) driving the Fourth Industrial Revolution. Companies, specifically those in the Defense Industrial Base (DIB), that do not take their cybersecurity posture seriously will find themselves frozen out of trillions in government funding as well as struggle to compete with state-backed competitors in emerging revisionist nations. The result will profoundly impact geopolitics, geoeconomics, and the Great Power Competition (GPC).

Many businesses are racing into a global game of corporate and nation-state competition with outdated cyber-priorities, operating with partial cybersecurity solutions, traditional information security controls, and a slow-moving cyber-posture. Looking forward, entrepreneurs and other business leaders that seek to work with the Department of Defense (DOD) must ensure that cybersecurity is a core pillar of business operations. Businesses must change their approach to ensure that cybersecurity is not merely window dressing but a truly effective tool that improves the competitiveness of the DIB in the GPC. The threat landscape only grows larger, and most businesses remain unprepared for the multitude of threats.

Rapidly evolving cyber threats necessitate a timely shift in the U.S. national security paradigm—from a competitive state-oriented agenda to a cooperative public–private strategy that can better accommodate business and human security needs. A cyber-pandemic principally threatens U.S. national security in three key areas: (1) economic espionage (and tech transfer) of American corporations (business security), (2) the vulnerability and exploitation of personal data (human security), and (3) offensive cyberattacks on critical infrastructure (state security and business security, depending on whether the infrastructure is privately or publicly owned or both).

State-sponsored and state-aided cyberattacks definitively change the balance of power in favor of adversarial attackers over U.S. business' cyber-defenses. Chinese and Russian cyber-attacks were "targeting U.S. and military corporate networks as early as 2003….in a series of intrusions known as Titan Rain" [16]. Computer network exploitation endures as part of the Chinese and Russian intelligence toolkit, specifically targeting military technology developed by the United States at a high cost. This ability to "leap-frog" competitor businesses or militaries is the single biggest challenge facing the United States and key to understanding the future of the modern Great Power Competition.

Critically, any future solution to the cybersecurity challenge needs to be grounded in a framework that allows U.S. companies to defeat strategic state-capitalist actors by focusing on long-term, over-the-horizon threats. This chapter argues that significant policy changes will be needed to position the United States better to deter cyberattacks of a foreign state and non-state actors, including (1) greater cooperation with existing industry groups, (2) increased emphasis in identifying and investing in the non-traditional DIB, (3) changes to the CMMC Third-Party Assessor Organization, (C3PAO) auditing mechanism to make it more robust, (4) implementation of automated tools such as a cyber hygiene score, (5) public/private partnerships and forums for security and incident management, and (6) a cybersecurity infrastructure bill. Such reforms will result in better outcomes for both the federal government and businesses.

Underpinned by stakeholder capitalism, new fiduciary responsibilities must elevate cyber-governance requirements in both public and private institutions. A cybersecurity infrastructure bill, like the one passed for physical infrastructures such as roads and bridges, is not only necessary but critical to ensuring parity concerning cybersecurity posture for all DIB companies. Significant investments in the cyber-infrastructure of businesses, including hardware, software, and human talent, should be made in exchange for stronger fiduciary cyber-responsibilities and reporting requirements for public and private companies. A transformed corporate culture and private sector that emphasizes cyber-hygiene ensure that threats are taken seriously and build trust between consumers, corporations, and government. Public–private collaboration that invests in business cybersecurity first and foremost will position the United States uniquely within the modern GPC. As Robert Metzger noted: "Government and industry leaders must accept that the best of present defenses may only drive adversaries to aggression directed where defenses are weak or absent" [18]. "National Security" spending and defense budgets garner near-universal bi-partisan support, which makes the DIB a logical starting point for PPPs as a model for cyber-collaboration deployed within a framework of stakeholder capitalism.

Cybersecurity Maturity Model Certification (CMMC)

Cybersecurity breaches, including unauthorized access to networks, applications, and data, have caught the attention of governments worldwide and, as a result, are working on rolling out rules and standards intended to protect controlled unclassified information in public and classified procurements. Such rules and standards are being developed under the auspices of what is commonly known as CMMC, a unifying new certification model to ensure that cybersecurity contractors adequately protect sensitive information. This government-led approach will be insufficient and is too narrowly focused on meeting the needs of the DIB because the tools and certification processes will inhibit continuous system improvements, hinder agile development, and reduce transparency and trust between stakeholders.

Given the DIB's significant dependence on digital devices and information, inadequate cyber-posture is a significant threat to U.S. hegemony. Indeed, U.S. hegemony derives specifically through the interconnectedness of global markets and institutions that are most at risk from a future cyber-pandemic. After notable government breaches in 2015, most memorably, of the Office of Personnel Management and the Internal Revenue Service, which resulted in 21.5 million records stolen, the government issued mandates requiring cybersecurity contractors to protect CUI residing in non-Federal information systems and organizations [18]. Deadlines for CMMC rollout continue to be delayed or missed, with many businesses still non-compliant with the mandate [15]. This includes many companies that form the underlying foundation of the industrial innovation base, with foreign actors stealing large amounts of sensitive data, trade secrets, and intellectual property every day. Technology and data loss contribute to the erosion of the DIB and harm U.S. government interests with the GPC.

A unified framework is needed to combat adversarial attacks that would result in the eventual dethroning of the United States as a major contender in the GPC. To its credit, with CMMC 2.0, a revised and updated version of CMMC, the U.S. government is attempting to consolidate multiple cybersecurity and resilience frameworks proposed over the last several years to combat rising cyber insecurity. A recent study identified more than 25 research activities across 36 industries that attempted to clarify the disparate frameworks [23]. Furthermore, a simple search in Google Scholar brings up more than 10,000 results for the "cybersecurity maturity model" and around 12,000 hits for "cyber resilience maturity assessment" [23].

CMMC attempts to address the significant question of how to protect the business from cyberattacks; however, it does not achieve its aims (even the latest 2.0 version), because the framework fails to adequately promote transparency between the private and public sectors; it does not effectively incentivize continuous improvement in cyber hygiene practices; and because it will create further regulation that does not improve the U.S. security posture, particularly when compared to the speed and innovation of cyberattacks from adversarial state and non-state actors. This static framework creates significant issues for the DIB, especially when many small and medium-sized businesses that comprise it do not currently comply with the most basic Federal Acquisition Regulations (DFARS & FAR) and National Institutes of Standards and Technology (NIST) requirements that already exist.

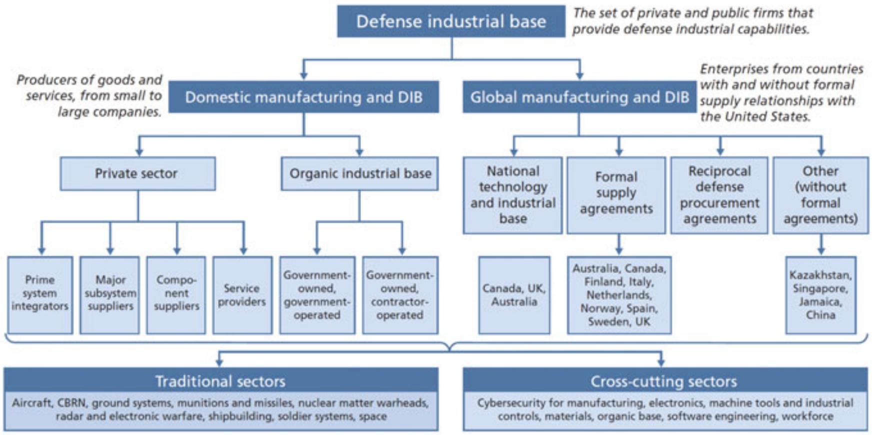
Even if the DIB can retroactively catch up and meet these requirements, and even if the current CMMC model is successful in getting them there, the industry will inevitably be caught off-guard once again if premeditated action and foresight are not built back into the model. For example, CMMC control SC.3.177 states that companies must use Federal Information Processing Standards (FIPS) Encryption to secure their data. However, traditional forms of encryption will be rendered useless by Quantum Computing. In the current model, businesses are expected to meet a level of cyber hygiene. Once they achieve that level, there is no incentive for them to seriously re-evaluate their protections until they are required to recertify, giving executives an excuse for complacency and leaving their information technology systems vulnerable to attack.

As a result, CMMC is ill-designed to counter foreign-state actors executing synchronized strategies to close innovation gaps. The DIB must assume that foreign state-sponsored tools perform magnitudes better than even the best open-source tools available to U.S. corporations. Foreign state and private actors involved in cybercrime and espionage target the DIB "to close [the] capability gaps" between them and the United States [10]. The results of such attacks from state actors are astonishing, totaling billions of dollars a year in net losses.

Understanding the Traditional DIB and Why It Matters in a Cyber-Pandemic

Despite a nearly universal agreement about the importance of shielding critical services and assets from digital harm, governments have thus far had difficulty in accurately assessing where the most significant vulnerabilities lie [8]. While the Federal Government identifies key cybersecurity contracts to enforce CMMC before others, the USG has yet to identify critical businesses and industries to support hardening immediately comprehensively. To achieve stakeholder collaboration and elevate cybersecurity within a national security policy, we must understand how CMMC impacts the DIB and how the DIB of approximately 300,000 companies is viewed in government. Cybersecurity defines its industrial base into two broad categories, as noted in the figure below:

DoD's Characterization of the Defense Industrial Base


Defense industrial base
The set of private and public firms that provide defense industrial capabilities.
Producers of goods and services, from small to large companies.
Domestic manufacturing and DIB
Global manufacturing and DIB
Enterprises from countries with and without formal supply relationships with the United States.
Private sector
Organic industrial base
National technology and industrial base
Formal supply agreements
Reciprocal defense procurement agreements
Other (without formal agreements)
Prime system integrators
Major subsystem suppliers
Component suppliers
Service providers
Government-owned, government-operated
Government-owned, contractor-operated
Canada, UK, Australia
Australia, Canada, Finland, Italy, Netherlands, Norway, Spain, Sweden, UK
Kazakhstan, Singapore, Jamaica, China
Traditional sectors
Aircraft, CBRN, ground systems, munitions and missiles, nuclear matter warheads, radar and electronic warfare, shipbuilding, soldier systems, space
Cross-cutting sectors
Cybersecurity for manufacturing, electronics, machine tools and industrial controls, materials, organic base, software engineering, workforce

SOURCE: Derived from U.S. Department of Defense, 2018.
NOTE: CBRN = chemical, biological, radiological, and nuclear.

Aerospace and defense sector leaders such Lockheed Martin and Raytheon remain dominant players but make up only a tiny percentage of the overall DIB. Supply chain sensitivities have traditionally limited the fidelity of comprehensive industry data by company size. Small companies that participate indirectly in cybersecurity supply chains are particularly difficult to quantify [7]. The composition of corporate supply chains is considered proprietary by many prime contractors. Data from the North American Industry Classification System (NAICS) codes shows that over 99% of U.S. firms have a revenue of <$100 million. For this chapter, they are considered small or medium-sized companies. Many of these companies sell commercial products and services, obfuscating which companies are classified as part of the "aerospace and defense" sector.

Imbalanced applications of cyber policy also occur in the government sector outside of the defense and intelligence communities [2]. DIB sector leaders have well-established operational cyber defense programs, while less well-resourced small and mid-sized companies lag behind these benchmarks. The frequency of outsourcing and subcontracting in modern manufacturing further challenges cyber policy application. Airbus has 1676 publicly disclosed "tier one" suppliers and has over 12,000 "tier two and below" suppliers. General Motors has 856 and over 18,000 of each, respectively [14]. The "lower tier" businesses are significantly more likely to lack critical cybersecurity infrastructure, including a security information and event management (SIEM) system and the in-house cyber expertise with which to operate it.

Notwithstanding the cybersecurity improvements needed for the "traditional" DIB and sector leaders, investments and programs that target "non-traditional" DIB and lower-tier suppliers are imperative. As noted in Farhadi and Galloway, the operating space of the future GPC will likely no longer be waged with conventional weapon systems built by corporations in the "Aerospace and Defense" sector, urgently warranting the identification and integration of non-traditional and commercial technology companies into the DIB (2022, In Press). The scope of non-traditional DIB could also be expanded to include innovative commercial technology companies, including those identified through initiatives of the Defense Innovation Unit (DIU) in Silicon Valley.

CMMC practitioners and cybersecurity policymakers could coordinate efforts with the DIU and venture capital groups such as In-Q-Tel to bring innovative companies into the DIB. Many of these innovative, lower-tier, non-traditional DIB companies may need increased cyber protection immediately despite not holding a government contract that requires them to do so. Startups at universities also fall into this category, many working on effective and innovative programs, yet fall outside the scope of CMMC. University programs and startups are often supported by foreign researchers and hungry for seed funding and venture capital investments. Identifying these "future companies" and setting conditions to thwart potentially adversarial venture capital funding also preemptively protects the DIB. Foreign venture capital flows to the DIB sector were roughly $6.5 billion in 2019, according to Preqin [4]. While discussing adversarial capital deployed into the DIB and non-traditional DIB is critical, it is better addressed outside this article. The non-traditional DIB, including thousands of small and medium-sized companies, is critical suppliers of products and services to the traditional DIB. The lack of focus on critical "non-traditional DIB," including innovative early-stage companies, poses a threat to U.S. competitiveness within the future GPC.

CMMC Gaps and Challenges to Private Industry

"The DIB is the target of increasingly frequent and complex cyberattacks by adversaries and non-state actors. Dynamically enhancing DIB cybersecurity to meet these evolving threats and safeguarding the information that supports and enables our warfighters, is a top priority for the Department. CMMC is a key component of the Department's expansive DIB cybersecurity effort.

The CMMC program includes cyber protection standards for companies in the defense industrial base (DIB). By incorporating cybersecurity standards into acquisition programs, CMMC provides the Department assurance that contractors and subcontractors are meeting cybersecurity's cybersecurity requirements" [24].

The CMMC programs are admirable but grounded in a framework that may stymie collaboration rather than enhance it. Cyber-hygiene best practices should constantly evolve to meet new threats never remain static. However, CMMC, as it is currently structured, may lead companies to "wait and see" how their proposed security solutions will be interpreted by internal or external cyber-teams and assessed by C3PAOs (independent assessors that are certified by the government). In addition, CMMC does not resolve the many significant cybersecurity gaps that plague most American businesses, including the use of the agile methodology in IT systems and the lack of cost-effective security information and event management systems.

Security Information and Event Management Systems (SIEMs)

Security Information and Event Management Systems (SIEMs) are tools that allow a company to monitor all log data that flows in and out of its network. While large defense and technology companies leverage SIEM solutions, many small and medium-sized companies lack a comprehensive SIEM solution. These businesses may monitor segments of their networks, like sign-in logs or firewall notifications, but few centralize their log data.

CMMC requires elements of a SIEM solution to be implemented but does not directly account for the ancillary experts in cybersecurity and process owners required to manage one effectively. According to a recent 2020 RAND study, which reviewed the costs associated with CMMC: "Most small DIB firms may not be able to afford the cyber-defenses that the CMMC could mandate, and many medium-sized DIB firms may face the same challenges, especially if held to the highest compliance levels of the CMMC" [7].

Defense contractors should already be enforcing some SIEM and cybersecurity regimes; however, according to the National Defense Magazine, most are not enforcing cyber standards defined by the CMMC [12]. Specifically, of the 300,000 companies that comprise the Pentagon's supply chain, "about 290,000 of those have no cybersecurity requirements whatsoever" [12]. Typically, these companies are subcontractors to large businesses performing work in the lower tiers of a supply chain and cannot afford to meet the department's increasingly demanding cybersecurity requirements [13]. The costs of a SIEM and in-house experts in cybersecurity can be prohibitively expensive for small and medium-sized businesses. Based on 2021 data, the average salary of a cybersecurity specialist is $83,516, and the average cost of a comprehensive SIEM solution is over $600,000 per year [6]. These costs do not include CMMC certification and other big-ticket items, such as cybersecurity insurance. The high costs may: (1) deter many companies from true implementation, or (2) cause a number of innovative companies to forego working with the cybersecurity altogether,or (3) create a quasi-monopoly of secure large businesses, reducing innovation and competition within the DIB.

The Agile Methodology, Patching and Addressing Vulnerabilities

The DIB and CMMC practitioners should re-evaluate the benefits and drawbacks of the agile methodology in the context of a cyber-pandemic. The agile methodology relies on trust and collaboration to develop, deploy, and iterate solutions quickly and incrementally. CMMC policy itself would be well-served by implementing this methodology to govern its protocols. However, agile methodology also creates vulnerabilities in cybersecurity for businesses and technology companies that CMMC is not built to address. Many companies deploy products and systems on a model of "field it fast, fix it later," resulting in unfixed vulnerabilities in their software [8]. In 2013, hackers accessed a Microsoft database that contained descriptions of critical and unfixed vulnerabilities in its software, including the Windows operating system [17]. The unfixed vulnerabilities allowed hackers to develop tools (or weapons) to target the American business part of the WannaCry and NotPetya attacks in 2017 [21]. To achieve a more robust level of security and reduce threats to businesses in the digital age, governments will need to step in and hold digital service providers and the manufacturers of ICT technology accountable for ensuring their products maintain adequate safety standards [8]. Ultimately, the paradigm of "field it fast, fix it later," which continues to hold sway in the technology industry, plays a determining role in this accountability. Traditionally, slow corrective actions for patches also plague many large businesses. Languid patch implementation following a vulnerability disclosure has led to multiple hacks and cyber-defense failures. While CMMC has controls that attempt to address this problem, specifically RM 2.143, CM 5.074, and MA 2.111, they may not solve the problem systematically for reasons discussed later in this chapter.

The United States maintains a National Vulnerability Database that incorporates data from hundreds of organizations and countries. Current measurements indicate that the NVD's data feed over 30,000 unique organizations using API and web tools over two weeks. The NVD sees requests originating from nearly all countries, with industrialized countries making up the vast majority of NVD's users. Within the United States, the NVD observes users from nearly all sectors of critical infrastructure. The U.S. Department of Homeland Security's Cyber and Infrastructure Security Agency discloses vulnerabilities reported to it to the public by way of the U. S. Computer and Emergency Readiness Team within 45 days of the initial reporting, regardless of the existence or availability of patches or workarounds from affected vendors [8].

China has a similar vulnerability database system, but it operates twice as fast as its American counterpart, averaging just 13 days from vulnerability identification to public disclosure [8]. China proactively scours the web and other sources of information, looking for vulnerability information. In contrast, the United States waits for reports from vendors to be processed through the Common Vulnerabilities and Exposures database [26]. A lack of resourcing for robust open-source databases often results in companies building their databases or outsourcing to a SIEM at considerable cost. CMMC assessors and implementing companies would be well served by more accessible access to cyber-threat information all too often siloed in various public and private forums and subject to impassable hurdles. In addition, the voluntary program for sharing information on threats to cybersecurity poses challenges, given that not all DIB firms can access the service because it requires a cybersecurity Common Access Card (CAC). Many DIB firms may lack informal ties to the Intelligence Community, making them privy to important cyber-threat information (Gonzales). Open-source solutions are not a panacea and pose security challenges. Open-source code that is publicly editable is susceptible to actors with malicious intent. A company that uses open-source software would have to prove to an auditor that updates and patches are tightly controlled and do not contain code written by anonymous contributors. Given the risks and vulnerabilities, open-source databases and solutions still present an effective, low-cost solution to small businesses if supported through public–private networks.

CMMC and Resilient Supply Chains

The current digital ecosystem is underpinned by many components, subcomponents, standards bodies, equipment providers, chip manufacturers, mobile device providers, users and employees, governments, and other third parties. The digital ecosystem is subsequently undermined when companies do not control their hardware, software, and assembly processes. Computer chips and other IoT components are frequently not made in the United States, nor are many engineers who design and program them. CMMC does not explicitly address supply-chain risk management (SCRM) related to verifiable trusted hardware. A requirement in CMMC RM 4.148 states: “Develop and update as required, a plan for managing supply chain risks associated with the IT supply chain”; however, there are no direct requirements stated as to what an organization needs to mitigate against specifically. Great power can erode if state actors quickly close technological and scientific gaps without paying a high cost to achieve those gains, which allows the exploiter to “leapfrog” and advance.

CMMC Third Party Assessor Organization (C3PAO)

C3PAO stands for CMMC Third-Party Assessor Organization. C3PAOs, as currently envisioned, is intended to audit DIB companies' cybersecurity posture to ensure compliance with new cybersecurity regulations. Many questions of assessor organizations' role in the CMMC certification process remain unanswered when posed by industry groups, including: "[H]ow the [cybersecurity] and its auditors will handle the immediate influx of contractors requiring certifications; the specific criteria for determining the certification level necessary to perform a contract; how the department and its accreditation body will ensure consistency of third-party audits; and how it will address the impact on the commercial item and small business contractors, which ordinarily do not obtain significant cost recovery under reimbursable contracts with the government" [1]. Cybersecurity officials admitted that they "are not set up or resourced to do these certifications and audits of 300,000 companies. As it is, our $750 billion budget [the total public cybersecurity budget] does not cover all that we need to do. Government outsourcing of this critical certification process needs to be re-evaluated. So we needed to look outside" [12].

Utilizing private for-profit contractors to certify DIB companies creates a perverse incentive within the audit process. C3PAO's will theoretically have to meet a high-standards and legally attest to the veracity of their audits or face prosecution; however, the profit motives remain strong in a shareholder-driven economy. C3PAO's could ensure companies "pass" audits to lock in future revenue [audits]. Furthermore, CMMC audit cost is "determined by assessment model scope (level of certification sought), organizational scope and size, and complexity… with small organizations…less costly than…large manufacturers, where multiple assessors may be required, and analysis could span several weeks.

Because of this, there can be no standard pricing for CMMC assessments" [24]. This could lead to C3PAO being less likely to support small businesses to make better margins from large corporations with more complex system requirements. Small and medium-sized companies, especially those with little expertise in cybersecurity, also face the risk of being easily manipulated by "certified" consultants to buy products or services they do not need. Conflicts of interest abound when C3PAO's offer certification support, including technical expertise and IT, support for their customers to meet CMMC requirements. If the same assessor companies provide technical consulting services, they also provide auditing services. Such assessor companies will ensure certification to protect their "product." The profit motive in this instance creates a perverse incentive for the auditors to protect their new revenue stream. The lack of a unified standard to enforce opens the door for C3PAOs to bend the rules to ensure their paying contractor meets the requirements, even if the technology and security solutions do not meet standards or are substandard compared to another similar product.

Conceptual Changes to the CMMC Framework

Resilience and vulnerability disclosure requirements, a cybersecurity hygiene score, mandatory incident disclosure requirements, increased federal funding to re-tool the cyber posture of businesses, and revisions to the C3PAO audit model will better position the DIB to meet the challenges of a future cyber-pandemic. An expansion of public–private partnerships will be a critical tool in supporting the DIB and help build trust between stakeholders to improve the U.S. cybersecurity posture within GPC.

Resilience and Vulnerability Disclosure

The path towards effective cybersecurity for the DIB is a "new vulnerability disclosure process (and operational requirements); a duty to warn of imminent danger, such as in the case of an emerging attack; and a duty to assist in the case of cyber-emergencies" [9]. The DIB has come to rely on ICT companies who can implement a "new communications and warning system for urgent patches, adding 'emergency' to their repertoire of categories (emergency, critical, important, moderate, and low)" [8]. A recent search at the U.S. Consumer Product Safety Commission (CPSC) noted zero IT recalls for potential data loss hazards. Greater industry collaboration with the CPSC can drive "accountability by eliminating or significantly reducing after-market repairs (patch Tuesday) to a market that drives accountability through product recalls. Vendors could be required to deliver well-engineered products and services and present buyers with a list of the underlying components, libraries, and dependencies—a 'software bill of materials'—to drive transparency and accountability" [8]. Industry groups and regulatory bodies could revise their existing vulnerability disclosure models to adapt to the future cyber domain.

Targeted investments in key cybersecurity and technology companies will have exponential benefits to the DIB. Large technology companies have an outsized impact on the vulnerabilities of the DIB because most U.S. businesses utilize their services. Well-known hacker Jeff Moss notes that "maybe 20 companies around the world are in a position to do something to increase security and resilience for all of us" [25, p. 44]. A special auditing body focusing on the most critical cybersecurity infrastructure companies could be created as a subset of the newly proposed C3PAO framework. Organizational conflicts of interest (OCI) that emerge between critical cybersecurity companies and C3PAOs add further utility to a special assessor auditing body.

DIB Cybersecurity-Hygiene Score

The Common Vulnerability Scoring System (CVSS) developed by NIST/NVD offers the DIB a practical model that can be expanded and applied to CMMC in the form of a cyber-hygiene score. Owned and operated by a U.S.-based non-profit, CVSS uses an open framework for communicating the characteristics and severity of software vulnerabilities to the industry [20]. A transparent cyber-hygiene score specifically tailored for CMMC requirements could help differentiate companies that institute best practices and create systems visibility among lower-tier suppliers even if they are not required to be CMMC-certified [19]. DIB companies could input, as part of their required disclosures on the System for Award Management (SAM.GOV—a website database profile required to do business with the U.S. Government), the systems and software they utilize based on a set of government questions (e.g., What cloud storage system do you use? Do you utilize a SIEM, if so, which one?). Tailored methodologies would integrate with the user-provided data. They could account for how DIB companies leverage their internal cyber-operations in conjunction with technology solutions to ensure that the "managed," "reviewed," and "optimized" aspects of CMMC factor into the score. Assigning process owners and written explanations to how each technology is tied back to an operational action would influence the cyber hygiene system.

A clear, understandable cyber-hygiene score could provide additional data points to small businesses when selecting and deploying information technology systems. Understanding the CMMC-specific cybersecurity attributes of Microsoft's Azure from Amazon's Web Services, or what differentiates Enveil versus Vera for data packet security, will help drive better decision-making across the DIB. A scoring system that ranks companies qualitatively (process and systems) and quantitatively adds more value. As automation increases, scores could help predict what parts of a company's cybersecurity posture are most at risk (like how a credit score helps individuals identify complex financial data).

A public–private working group of cybersecurity experts who collaborate on behalf of the U.S. Government to rate, assess, and evaluate the top technology companies such as Amazon, Microsoft, Symantec, Okta, and Google is a logical first step. Data aggregation compiled from multiple large businesses could help inform the cybersecurity score algorithmically. The working group would regularly update the top software cyber score automatically recalculate scoring for companies who use their software. Focusing on large business' software first alleviates the burden on many small businesses and allows the government to provide product or software security alerts similar to a credit score. Furthermore, building these scores into the SAM database can inform C3PAO's who are re-certifying companies.

A transparent cyber-hygiene score would empower stakeholders, including public and private sectors, and hold companies accountable for their potential to introduce risk into the DIB. Under such a system, companies would gravitate toward measures that reduce their exposure to cyber-risks, such as their reliance on foreign entities or adversary-controlled supply chains. To enforce such a system, an industry association, non-profit, or university might be more attuned to key predictors of risk than a more generalist adjudicating entity. Companies will appreciate the clarity of knowing what they need to improve to increase their score (or keep their current score). The proposed risk assessing agency can develop open scoring algorithms by processing data related to previous and ongoing problems in cybersecurity. Such incidents could train algorithms to assess risks and forecast damages more accurately. Over time, these algorithms could harness positive track records…as well as negative experiences…failures to improve risk detection [19].

Through a cyber-hygiene score system, businesses and customers (such as cybersecurity) would collaborate to ensure the system is fair, open-source, and inclusive by involving a combination of voices from cybersecurity experts and data scientists. By combining various sources of information, transparency will enhance competition and innovation while also minimizing the likelihood of regulatory capture by larger firms looking to influence cybersecurity rulemaking. Looking at aggregate scores over time will also allow the government to see who is actively monitoring the environment and making improvements to stay secure. As the cybersecurity score becomes more refined, insurance premium costs for cyber theft, damage, etc., would be lowered as risks become quantified, measurable, and transparent. This approach is not novel. Many systems utilize risk-based algorithms to “score” companies like NAVEX for regulatory and legal compliance. Further, an impartial scoring system, more widely employed, may incentivize greater cooperative efforts across vital sectors in the spirit of great power cooperation.

Improving C3PAOs

Universities, academia, and select cybersecurity non-profits can add substantial value as C3PAOs are authorized to provide CMMC certification. Universities offer a ready group of technical experts and have a significant population of U.S.-citizen masters and doctoral students who can perform such audits. Leveraging academia would also expand the pool of professionals with a security clearance if the United States were to engage in a cyberwar with our adversaries.

Mandatory Disclosure and Public–Private Collaboration

Reporting cybersecurity incidents and vulnerabilities is an essential element of effective cybersecurity. Cybersecurity relies upon businesses to self-disclose breaches but does not mandate them. Except for some “contractors cleared to do classified work, cybersecurity neither mandates nor facilitates the use of automated systems of event monitoring” [18]. An automated SIEM is widely accepted as a key means by which sophisticated companies respond and recover from attacks. Too little of the U.S.

DIB utilizes a SIEM, primarily due to a lack of financial resources or technical expertise. An open-source public–private SIEM would greatly improve information transfer between government and industry, thereby expediting responses to threats and attacks.

Implementing technology is not the only consideration when achieving CMMC compliance. Day-to-day operational cybersecurity burdens require knowledgeable staff members and process owners to manage and maintain these technologies. To ameliorate the cost burdens, subsidies could be provided to entities such as the NDIA and AFCEA to assist with the rollout, training, and implementation of complex cybersecurity systems.

All-Small Mentor Protégé Programs (currently designed for large businesses to assist smaller businesses to grow in the federal marketplace) can be expanded to include CMMC and cybersecurity requirements. Mentor companies could receive tax credits, performance incentive fees, and credits towards meeting their set-aside subcontracting and spending targets, a stated goal of the U.S. government.

A cybersecurity infrastructure bill passed separately from the omnibus cybersecurity spending bill would cover all of the proposed systems and frameworks mentioned above and emphasize the importance of cybersecurity outside the DIB. Tax credits and small business administration loans ultimately forgiven like the COVID Paycheck Protection Program loans could be provided to companies who implement a SIEM and hire or retrain staff in cybersecurity systems and CMMC.

Conclusion

To out-compete state-sponsored competitors, the U.S. government and the DIB must align resources within a framework of stakeholder capitalism to mutually reinforce defensive cyber-measures with U.S. government oversight. The alignment must focus on radical openness and transparency while decreasing the profit motives so entrenched in shareholder economies. Building trust with and between public and private sectors in defense of business stakeholders is the only sustainable long-term policy because cybersecurity relies on collaboration and shoring up of the weakest links in an interconnected system. Individual citizens, businesses, and communities can no longer disconnect from the IoT to protect themselves from those who are untrustworthy. Conversely, the wider the circle of trust with and between "cyber stakeholders," including foreign corporations, citizens, and suppliers, will expand the traditional DIB and enhance our collective security relative to our adversaries. With that noted, given the prohibitive costs for a SIEM or DCP2 for most small and medium-sized companies, the only way to ensure that cybersecurity can rely on even the weakest links in the DIB is if the U.S. government provides significant financial and technical support.

Securing data and ensuring the methodology for doing so should be the most critical facet of CMMC 2.0. With the proper framework grounded in stakeholder capitalism and mutually beneficial enforcement protocols, creators, administrators, and users of the cyber-domain as a technological construct can supervise and repair it. The U.S. government and the DIB can develop open-source, agile groups that respond quickly to adversaries. Dialogue can be improved between private companies and government by introducing public–private partnerships that encourage information sharing and cooperation rather than discouraging it. “Voluntary event sharing [is still limited as]... many companies refrain from sharing sensitive data about their information systems and their security experience” [18].

Achieving cyber-resilient critical infrastructure for businesses poses significant challenges. Society relies on infrastructure and services extending beyond a specific organizational entity; yet, existing cybersecurity maturity models typically aim to assess a single organization [11]. Shaked et al. note that the United States must reimagine critical infrastructure and services and explore cyber-resilience as a system property [22]. This can only be achieved by developing a system that encourages cooperation, develops clear and consistent frameworks for enforcement, and emphasizes transparency concerning the systems that underpin the digital ecosystem.

Without specific initiatives such as the cybersecurity infrastructure bill, C3PAO reforms, and a cyber-hygiene score, many small and even medium and large-sized companies may become ineligible for cybersecurity contracts, thus reducing the number of potential vendors that can support the DIB. Those companies that meet the criteria at the expense of bottom-line earnings will do so reluctantly, without looking to improve appreciably; meaning that competitors who look past profit will beat us with great urgency. Absent the necessary shifts in cybersecurity policy towards PPPs, more cooperative oversight, and the prioritization of human and business security, the United States risks losing not only its competitive edge in the modern GPC but its most vital national business resources.

***Special thanks to Joseph C Dorsey for his support and invaluable contributions to this article*.**

References

1. Burnette, R., Cassidy, S., & Clark, S. (2020). *Pentagon updating cybersecurity guidance, national defense*, 24 January, viewed 6 February 2020, https://www.nationaldefensemagazine.org/articles/2020/1/23/small-businesses-concerned-about-new-cybersecurity-certification.
2. Conti, G., & Fanelli, R. (2019). How could they not: Thinking like a state cyber threat actor. *The Cyber Defense Review,* 15 November, viewed 3 March 2020. https://cyberdefensereview.army.mil/Portals/6/Documents/CDR%20Journal%20Articles/Fall%202019/CDR%20V4N2-Fall%202019_CONTI-FANELLI.pdf?ver=2019-11-15-104103-203.
3. Davis, N., & Pipkaite, A. (2020). *What the COVID-19 pandemic teaches us about cybersecurity—And how to prepare for the inevitable global cyberattack*. World Economic Forum, 1 June, viewed 6 January 2021. https://www.weforum.org/agenda/2020/06/covid-19-pandemic-teaches-us-about-cybersecurity-cyberattack-cyber-pandemic-risk-virus/.
4. Fannin, R. (2020). *How the US-China trade war has starved some Silicon Valley start-ups*, CNBC, February, viewed 6 March 2022, https://www.cnbc.com/2020/01/31/chinese-venture-capitalists-draw-back-silicon-valley-investments.html.

5. Farhadi, A., & Galloway, I. (2022, In Press). Building trust and advancing U.S. Geoeconomic strength through public–private partnership stakeholder Capitalism. In *The great power competition volume 2: Contagion effect: Strategic competition in the COVID-19 Era.* Springer Press.
6. Foresight. (2021). *True cost of SIEM (Security Information and Event Management).* https://www.glassdoor.com/Salaries/cyber-security-specialist-salary-SRCH_KO0,25.htm, https://foresite.com/true-cost-siem-security-information-event-management/.
7. Gonzales, D., Harting, S., Adgie, M.K., Brackup, J., Polley, L., & Stanley, K. (2020). *A defense industrial base cyber protection program for unclassified defense networks,* Santa Monica, CA: RAND Corporation, viewed 3 January 2022, https://www.rand.org/pubs/research_reports/RR4227.html.
8. Hathaway, M. (2019). *Patching our digital future is unsustainable and dangerous.* Centre for International Governance Innovation, viewed 16 September 2021, https://www.cigionline.org/publications/patching-our-digital-future-unsustainable-and-dangerous/.
9. Hathaway, M., & Savage, J. (2012). Duties for Internet Service Providers. *Paper presented at Cyber Dialogue.* Canada Centre for Global Security Studies, Munk School of Global Affairs, University of Toronto, March.
10. Hallman, W. (2019). Cybersecurity: Front and center for industry. *National Defense Magazine Online,* 19 June, viewed 3 January 2021, https://www.nationaldefensemagazine.org/articles/2019/6/19/ndia-perspective-cybersecurity---front-and-center-for-industry.
11. Kott, A., & Linkov, I. (Eds.) (2019). *Cyber resilience of systems and networks.* Springer, Cham. https://doi.org/10.1007/978-3-319-77492-3
12. Lee, C. (2020). *Vital signs 2020: Small businesses concerned about new cybersecurity certification'.* National Defense, 23 January, viewed 6 March 2021, https://www.nationaldefensemagazine.org/articles/2020/1/23/small-businesses-concerned-about-new-cybersecurity-certification.
13. Lopez, T. (2019). DOD focuses on minimizing cyber threats to department, contractors. *DoD News*, December, viewed 9 July 2021, https://www.defense.gov/explore/story/Article/2034756/dod-will-help-small-companies-meet-cybersecurityrequirements/.
14. Lund, S., Manyika, J., Woetzel, J., Barriball, E., Krishnan, M., Alicke, K., Birshan, M., George, K., Smit, S., Swan, D., & Hutzler, K. (2020). *Risk, resilience, and rebalancing in global value chains*, McKinsey Global Institute, 6 August, viewed 27 April 2021, <https://www.mckinsey.com/business-functions/operations/our-insights/risk-resilienceand-rebalancing-in-global-value-chains.
15. Lynch, I. (2020). *Department of defense controlled unclassified information compliance: The impact on small business contractors.* Capitol Technology University, ProQuest Dissertations Publishing, 28000085.
16. Mattis, P., & Brazil, M. (2019). *Chinese communist espionage: An intelligence primer*. Naval Institute Press.
17. Menn, J. (2017). Exclusive: Microsoft responded quietly after detecting secret database hack in 2013. *Reuters,* 17 October, viewed 15 May 2020. www.reuters.com/article/us-microsoft-cyber-insight/exclusive-microsoft-responded-quietly-after-detecting-secret-database-hack-in-2013-idUSKBN1CM0D0.
18. Metzger, R. (2020). Cyber safety in the era of cyber warfare. *SciTech Lawyer, 16*(3), 8 February, viewed 15 March 2021. https://www.americanbar.org/groups/science_technology/publications/scitech_lawyer/2020/spring/cyber-safety-the-era-cyber-warfare/.
19. Norris, W., Balmain Rodgers, J., Blazek, C., Hewage, T., & Kobza, B. (2020). A market-oriented approach to supply chain security. *Security Challenges, 16*(4), 65–81. Institute for Regional Security. https://regionalsecurity.org.au/research-and-thought-leadership/security-challenges/.
20. National Vulnerability Database. (2021). *Vulnerability metrics*, viewed 3 March 2022, https://nvd.nist.gov/vuln-metrics/cvss.
21. Patel, A. (2017). Petya: "I Want To Believe". *F-Secure (blog)*, 29 June, viewed 8 December 2017, https://labsblog.f-secure.com/2017/06/29/petya-i-want-to-believe/.

22. Shaked, A., Tabansky, L., & Reich, Y. (2021). Incorporating systems thinking into a cyber resilience maturity model. *IEEE Engineering Management Review, 49*(2), 110–115, 1, Second quarter, June 2021, viewed 20 August 2021. https://doi.org/10.1109/EMR.2020.3046533.
23. Sharkov, G. (2020). Assessing the maturity of national cybersecurity and resilience. *Connections: The Quarterly Journal, 19*(4), pp. 5–24, viewed 5 January 2021, <https://www.researchgate.net/publication/348446458_Assessing_the_Maturity_of_National_Cybersecurity_and_Resilience>.
24. The Cybersecurity Maturity Model Certification Accreditation Body. (2021). CyberAB, viewed 8 November 2021, https://cmmcab.org/faq/.
25. Vos, A. (2020). Whose cyber is it anyways? A private perspective on a public good. *Atlantisch Perspectief, 44*(4), 41–45, viewed January 2021, https://www.jstor.org/stable/48600571.
26. Waterman, S. (2017). China's vulnerability disclosure system twice as fast as U.S. version. *CyberScoop*, 23 October, viewed 3 January 2021, www.cyberscoop.com/china-vulnerability-reporting-nvd-recorded-future/.

Dr. Adib Farhadi is Assistant Professor and Faculty Director of the Executive Education Program at the University of South Florida. His research focuses on the intersection of geoeconomics, geopolitics, and religion, particularly on the "Silk Road" Central and South Asia (CASA) Region. Dr. Farhadi also serves as the Editor-in-Chief of The Great Power Competition book series and previously served in senior positions for Afghanistan and extensively advised the U.S. government and various other international organizations.

Ian Galloway is a Principle and Management Executive in the Aerospace, Defense, and Energy sector with a keen interest in—and significant experience with—public affairs, international business, strategic consulting, and risk management.

At DGC International (DGCI), he specializes in developing highly innovative solutions that meet client needs in demanding, adverse, and contingency environments. Ian focuses on expanding current services; capturing new business in existing core mission areas; risk manage-ment; strategic communication; and corporate development. Recently, he helped to document and refine key supply chain, logistics and program man-agement processes and systems in support of government, military and international commercial markets. As a key member of DGCI's closely knit and highly collaborative Executive management Team, Mr. Galloway has contributed significantly to the achievements of DGCI.

He travels frequently to maintain his ties to international culture and politics—and his skills to promote the efforts of the Memorial Day Flowers Foundation and Zamani Foundation at home and abroad.

Ayman Bekdash serves as a board member of DGCI Corporation, a Virginia-based business that supports the U.S. Government. He was a significant contributor to the setup and expan-sion of DGCI operations in South America, Africa, the Middle East, and Central Asia. Prior to joining DGCI, he worked at Cardno Emerging Markets, an international development firm. Ayman proudly supports several charitable initiatives for military members and their families, as well as local and international charitable organizations supporting education. He has also published several articles and white papers on a variety of topics, both in the United States and abroad.

Mr. Bekdash holds a Bachelor of Science and two Bachelor of Arts degrees from the Univer-sity of Rochester. He is also a former Fulbright fellow.