The Collaboration Imperative for Cyberspace Stakeholders

Author: Mr. Riley Repko, HQE to the Air Force Deputy Chief of Staff for Operations, Plans & Requirements

Executive Summary

I. Challenge

Cyberspace is a core enabler for our nation's critical infrastructures and our military's battle-space. It is also a fundamental underpinning for the nation's economy; our continued prosperity and security are increasingly reliant on the sensors, computers, devices, networks, information and communications commonly referred to as cyberspace. Therefore, protecting our national and military interests in cyberspace is essential to our economic and national security. To be successful, that protection increasingly demands a .com, .gov, .mil collaborative partnership. Securing cyberspace is a difficult problem because it is threatened by challenges both similar to and different from traditional national security threats. The digital battlefield is a daunting mix of local, regional, and global adversaries, who target both public and private interests for widely varying objectives, operate outside of existing legal or diplomatic frameworks, and possess enormous collective destructive potential.

II. Issues

The bureaucratic constraints and ponderous processes inherent in most public and military institutions have not been able to adapt as quickly compared to the myriad of adversaries that operate outside of constraining rules and legal proscriptions. Cumbersome government acquisition and budgetary processes contribute to an inability to coordinate the necessary public/private collaboration. There are many factors which combine to impede effective collaboration: outmoded laws and policies related to permissible actions; the difficulty in exchanging business intelligence and military intelligence; the fact that much of the relevant infrastructure is privately-owned and operated; and, the private sector's sensitivity to releasing proprietary information or revealing sensitive data on cyber losses or vulnerabilities. As a result, all issues are not open for discussion at the same time. Even if such candor was possible, the expertise necessary to consider the issues thoroughly would be difficult to convene and empower to make decisions.

The severity and prevalence of the threat along with the low barriers to entry by malefactors demand that the public and private sectors work together in a coordinated fashion. Rapid threat identification, information exchange, increased awareness of innovative technologies and shared solutions are essential to mitigate or avoid potentially destructive outcomes. Importantly, this is not merely a U.S problem; ***U.S. and Coalition militaries must vigorously and collectively establish a partnership framework for global exchange between government and the private sector.***

III. Recommended Path Forward

An effective way to deal collectively with threats from cyberspace is through public-private collaboration and investment. Almost everyone endorses this idea; the challenge is how to accomplish that goal. HQ USAF believes the first step is to define and build an initial framework for both organizing and prioritizing efforts toward public-private partnerships. Building upon previous or existing public/private collaborative projects/models in other domains is important as this framework would

require fundamentally different approaches to broker connections among cyberspace-users with urgent requirements, the investors, and capability providers. HQ USAF (SAF/AQX sponsored) made an initial 'seed-capital' investment specifically focused on creating some substance for this collaborative framework, including convening a group to address the key issues over a 45-day period. Specifically, this group focused on how to leverage the rapid identification of innovative solutions for both public and private urgent mission requirements.

The highlights and defining characteristics of the proposed public/private endeavor are:

- Agreed upon "Rules of the Road," defining acceptable parameters for operating in cyberspace. We can ill-afford to continue accepting asymmetrical warfare attacks on our nation enabled by our own vulnerabilities.

- A collaborative environment and integrated network that enables rapid reach-back into a broad and diverse array of cyber experts throughout the nation, giving the warfighter access to cutting-edge technology and expertise that otherwise would be unavailable to the military.
- A process to discover world-class cyber experts, who may be either unaware of the military cyberspace requirements or over-looked because they work for smaller, less well-known firms.
- A senior advisory board providing strategic oversight and visionary leadership for the private and public sector's respected activities.
- Public and private "front line needs detachments" that will facilitate relationships, connections and exchange between primary stakeholders and their respective communities.
- A not-for-profit collaboration management center (CMC)providing administrative oversight for placing public/private resources to cyber-entrepreneurs in a "DARPA-like" effort; tracking program status & deliverables; and, managing a "best practices" repository of revolutionary technologies to remain ahead of adversaries.

The Cyber Challenge

The cyber domain poses new and constantly evolving security challenges to both the private and public sector that require a non-traditional mitigation strategy. The adversary has leveraged: (1) low barriers to entry (limited capital investment, manpower, and other resources); (2) nearly unfettered access to target-sets across geographies; and (3) fast execution that employs stealth and surprise. Perhaps most importantly, cyber attacks effectively exploit both the uncertain and tangled morass of international and domestic privacy, trade, and cyber law. In addition, a private-public coordination gap offers considerable immunity to the attacker, because the victim's relies on conventional processes and toolsets. The shared private-public vulnerability is a primary characteristic of cyber operations, which distinguishes it from traditional national security challenges. To meet this non-traditional threat, we must review and update our legal framework, develop a common operational picture and shared intelligence process, and establish collaborative bonds across the .mil, .gov, and .com domains. The public and private sectors share domain attributes such as risks, vulnerabilities, and operational responsibilities to such an extent that delineating boundaries frequently blur. The public sector's commitment for securing, protecting, and responding to cyber threats on its organizational networks intersects and frequently overlaps **the** private sector's responsibilities. Much of the public sector cyber capability rides on private sector infrastructure, yet the public sector, including the military, does not

control all infrastructure upon which essential national security capabilities are delivered. Due to the shared risk and mutual vulnerability for both the private and public sectors in cyberspace, the private sector must be an integral partner in any response. Some questions arise: "Is it possible to cooperate and share investment, and how would this be structured to be acceptable and value-added to both sectors?" This large scale public/private collaboration focusing initially on shared vulnerabilities requires a forum and a framework for both information and solution exchange; it must operate and consider solutions frequently in advance of an actual attack.

Current Approach to Cyber Threat is Inadequate

There is recognition that the national and military responses to cyberspace threats and opportunities are inadequate. This view is underscored by the initiatives and investments of past and current Administrations. There are urgent calls for a viable government and military response to build a sustainable capacity to protect our interests and access to the cyberspace "global commons." An unprecedented window of opportunity is open now, fueled by senior leadership advocacy to address these cyberspace challenges as reflected in efforts like the U.S. Comprehensive National Cyber-Security Initiative (CNCI). There is active interest from both the public/private sectors to bridge these gaps in situational awareness of the threat, requirements, capabilities, and investment opportunities (See Diagram 1 below). However, bridging the cyberspace gaps will require a sustainable framework that effectively "brokers" these connections between the public and private sectors stakeholders.

Materially significant investments worldwide in information technology security solutions provide a degree of tactical situational awareness on the threat to protect information and systems in cyberspace. However, many stakeholders are unaware either of the full spectrum of operational capabilities available, or of the equally material strategic investments being made in creating response options. Establishing and maintaining situational awareness (tactical and strategic future technologies) of emerging cyber security requirements, coupled with tracking previous and current cyber security capital investment, offers benefits, including:

- Lessons learned;
- Rapid identification of emerging technology developments; and
- Timely identification of new threats and potential counters;

The proposed collaboration framework provides stakeholders with the situational awareness of past, present and future needs and investments so that each may make more informed budget and organizational decisions.

Large bureaucratic departments found within federal agencies or companies represented within the Defense Industrial Base (DIB) have lost the agility and flexibility required to rapidly respond and defeat a cyber threat. Cyber threats challenge longstanding conventional approaches in both the private and public sectors and subsequently highlight the inadequacy of organizational cyber safeguards spanning the spectrum of policies, requirements, and resources. This inadequacy enables the clever adversary to maneuver within our acquisition cycle, which hasn't been aligned to bring current capabilities to the

fight. These strategies cut across a broad swath of operational roles and responsibilities, ranging from establishing requirements to acquisition, deliberative planning, and operations execution. Cyber assets are decentralized and cross disparate disciplines and organizational boundaries limiting visibility between cyberspace component contracts, requirements and program information. This proposed cyberspace framework attempts to: 1) streamline and facilitate the delivery of capabilities (technology, processes, ideas, people etc.) from the provider to the consumer or user (e.g., the warfighter); and 2) move awareness of warfighter needs out into a trusted community capable of meeting them in a timely fashion.

The Private Sector's Primacy in Cyberspace

The private sector influences the composition and operation of cyberspace more than it influences any other warfighting domain. The military and federal mission in cyberspace is inextricably linked to private and commercial technology stakeholders. These stakeholders range from the international open standards organizations**,** which shape core network specifications, to the global operating centers of international telecommunications companies, which transport large portions of military data.

It has been demonstrated repeatedly that the private/commercial sector often has first awareness of new challenges and opportunities in cyberspace. The same cyber-threats that directly challenge the survival and prosperity of a nation also threaten the survival and prosperity of private and commercial entities. For example, the security and integrity of an international bank's client information requires a level of protection similar to the strategic, operational, and tactical mission details of a military operation.

While established DIB partners provide essential capabilities, the innovation required in a rapidly changing domain will also require close collaboration with the small business community. The broad and deep marketplace of young technology companies collectively brings an innovative breadth and depth that cannot be matched by any one company. Venture-backed companies bring unique solutions through their essential skills and intellectual property and are able to respond to an agile cyberspace adversary. Companies such as In-Q-Tel's Palantir Systems Corp, Okena Inc. (bought by Cisco for $154m), IronPort Systems Inc. (bought buy Cisco for $830m), Network Intelligence Corp (bought by EMC for $175m), and others are purposely created by investors to focus on the market opportunity created by cyber threats. Conversely, the DIB, with its traditional focus on large weapons systems and equipment and a concomitant cultural alignment, is ill-equipped structurally and philosophically to identify dynamic cyber solutions. Lockheed, General Dynamics, Northrop Grumman and the other large aerospace and defense contractors are eager to move into the cyberspace arena, but are challenged by their own corporate cultures, resources and processes more attuned to their primary government customers. Emerging companies are resource constrained and are constantly competing with others in their market-space, both large and small in size and resources. Consequently, they typically avoid slow bureaucratic environments and tend to ignore potential government business. As a result, decades of history and experience have taught innovative firms to avoid tackling the onerous and time-consuming prerequisites required to serve the U.S. public sector. A collaboration framework that facilitates a two-way dialogue across public/private sector boundaries, while simultaneously attracting and/or

incentivizing the attraction of cyberspace talent from the entire technical base, will be essential to leveraging the private sector's full range of technological capability.

The Collaboration Imperative

U.S. and Coalition militaries are beginning to appreciate that the necessary cyberspace infrastructure and talent often lies with the private sector. The skills required to respond to cyberspace challenges are as diverse as cyberspace itself. Each new technology introduced brings new opportunities as well as new vulnerabilities. The ability to respond quickly to these vulnerabilities is a core survival competency for private-sector firms and represents a uniquely critical capability of the cyber mission that distinguishes it from other weapons systems. Additionally, the private sector has a collective diversity and depth in cyberspace expertise that could never be replicated fully in the military (or public-sector). The military must therefore leverage the technological diversity and depth that only the private sector can offer. This can only be achieved through a collaboration optimized for cyberspace solutions.

The speed and agility of the cyber-threat demands a requirements-to-solutions arrangement that is both timely and flexible. The venture capital community is highly effective at matching opportunities with talent in the commercial sector. Venture capital can also rapidly pool and mobilize financial and human resources. In order to be successful, U.S. and coalition militaries must collectively leverage the private/public sector's ability to respond to threats at the tempo demanded in cyberspace based on their awareness and capability to respond to requirements.

To address this collaboration imperative, a pilot development effort is currently underway. This effort is being facilitated by the Headquarters US Air Force Current Operations Directorate and funded by the HQ USAF Acquisition Directorate. The goal of this effort is to establish a viable and sustainable public/private collaboration framework for cyberspace collaboration. The initial cadre is a diverse mix of thought-leaders whose varied backgrounds bring new, innovative thought that speeds the requirements-to-solutions loop. Ensuring inclusiveness amongst the key stakeholders within the Air Force operational, requirements/planning and acquisition communities will be paramount to this success.

The Proposed Collaborative Framework

The primary objective of the collaboration framework must be to deliver critical cyber capabilities to the warfighter (see Figure 1). Delivery of these capabilities requires situational awareness for both public and private sector, and timely access to people, products and processes. To achieve this objective, the initial planning effort established the following charter statement: "Develop a public-private brokerage to advance current and game-changing technologies and processes, proactively addressing emerging cyber-threats through collaboration that ensures mission assurance for the decision maker (warfighter)." This "brokerage" is meant to intersect both the public and private sectors by 1) "matching" those that need a cyberspace capability with those that can provide it, and 2)"facilitating the exchange" of capabilities or services. Once mature, this brokerage should independently

operate in the space between the public and private arenas. However, in its incubation stage, the Air Force will need to carefully consider its organizational location in order to nurture, shape and adjust along a growth trajectory toward maturity.

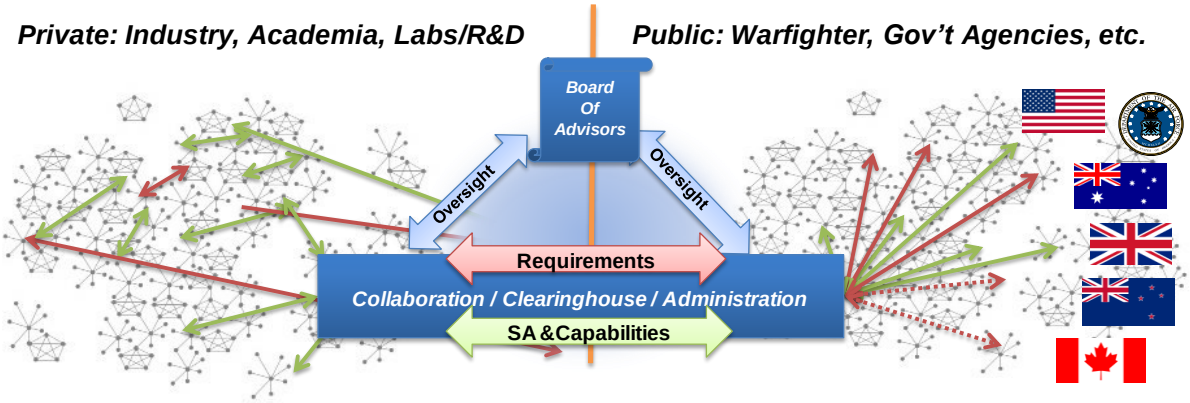

Figure 1: The Proposed Collaborative Framework – Macro View. A senior board of advisors will provide oversight between the private and public sectors, respectively. They would be primarily responsible for overseeing the exchange of cyber-situational awareness (SA), communicating requirements and capabilities pertaining to both sector's operational needs and at both the tactical and strategic levels.

Guided by the lessons-learned from existing and previously attempted public/private collaboration efforts, and coached by a seasoned professional facilitator, this initial planning cadre recognized that a fundamentally different approach and organizational structure are necessary for the cyberspace collaboration framework to operate effectively. Innovation in the funding, the collaboration governance, the membership and the brokering concepts needs examination. Furthermore, a senior advisory board was recommended to provide oversight for the members representing their private and public entities, respectively. These appointed management advisors would be primarily responsible for exchanging cyber-situational awareness (SA), communicating public/private requirements and needs, and matching those requirements to each other's respective needs or capabilities.

The goals for the pilot effort emerged from the first development workshop held in August 2009 in Washington D.C. with the early objectives of: 1) building a tactical plan that identifies and engages the key stakeholders in a collaboration framework; 2) establishing a concept for the governance and organization of the framework, and 3) establishing the advocacy and support from senior leaders who are the decision authorities for policy and resources. To shape a viable collaborative structure, it is essential for key stakeholders to remain actively involved throughout its development effort to include, if necessary, adding various additional stakeholders outside ones organization for the purpose of stimulating and leveraging new ideas.

There are several guiding principles that the initial planning cadre of framework builders intend to follow:

- It is not necessary to "reinvent the wheel"; efforts will include reviewing established legal and policy precedents that support collaboration. Leverage and inclusiveness will be key precepts in

order to garner support within the cyber domain. Capabilities and lessons learned from other similar initiatives must be leveraged to the fullest extent possible

- "Think big – start small – scale fast." Do not try to 'boil the ocean' by developing a way-ahead that cannot have measureable results or gain traction early.
- Establish clear value propositions for both the private sector and military to ensure participants are incentivized to participate
- Collaboration can "build pathways" for information and cooperation (see Fig. 1). A working group of advisors can form a "hub" for collaboration, with these pathways and frameworks functioning as "spokes."

This initial working group will benchmark past and existing public/private sector business models to identify and adopt best practices. The group will also take advantage of the experience and counsel of senior public and private mentors whose past experience will help to guide and lead the pilot effort through the intricacies of the cyber-security environment. Collectively this team has identified a number of expected "barriers" to public-private cooperation, which will be separately reviewed to determine the criticality of each. These barriers include:

- ***Cultural barriers***: There are significant differences between the military mission of attack/defend/exploit, and operate and the commercial mission of survive/grow/profit. Similarly there are domains and cultural divides that range across all manner of organizational constructs and preferences (flat vs. hierarchical, risk averse vs. experimental, "rice bowl" or "not-invented-here" mentalities). All of these differences create potential barriers to collaboration and potential conspiracy theories, privacy concerns, and competitive edge worries.
- ***Temporal barriers***: There is a mismatch between the tempo of cyberspace operations, production and deployment times (measured in months), whereas DoD acquisition and deployment cycles are measure in years. In contrast, cyber-threats can develop and deploy in days. Most notably, the current acquisition process lacks the responsiveness and agility required to serve the military with capabilities to meet the immediate and ever-changing cyber-threats.
- ***Entry barriers****:* Venture–backed, emerging technology companies are often overwhelmed by the government acquisition systems and security clearance requirements. For small firms with key capabilities, there is no viable path to market entry and few entities are willing to guide organizations through the maze. **(**In fact, the government acquisition maze has spawned a number of companies that do nothing more than guide other companies through the maze!) Additionally, venture-backed companies require means of beta-testing products in a fashion that government customers are typically unable or unwilling to accept. Lack of such a process inhibits the government's ability to be an early adopter of critical technologies. Finally, emerging technology companies are often hesitant to work with larger contractors, which provide a path to the government, even when binding non-disclosure agreements (NDAs) are in place.
- ***Jurisdictional barriers:*** The question of exactly who should be in charge of cyberspace and in what form is still open. Current jurisdictional requirements regarding state, federal,

international, law enforcement, intelligence, and active attacks through cyber are convoluted and at best open to interpretation. Little work has been done on compatibility standards, performance standards, or product and personal liability standards when it comes to cyberspace.

- ***Funding barriers:*** (Government and military budgeting processes) Innovation requires money up front and, therefore, cannot be part of the five-year budgeting process. Even when innovation funds are set aside, they are often usurped at the last minute to cover unanticipated needs or emergency funding requirements perceived at the time as more urgent.
- ***Human capital barriers****:* The U.S. lags the international community in the number of US students pursuing technical undergraduate and advanced graduate studies in cyber-related fields. And foreign graduate students are leaving the U.S. after finishing their studies. Consequently, the Air Force's capability to staff cyber operations with appropriately trained and experienced professionals is severely constrained.
- ***Perception barriers:*** The technical jargon of "cyberspace" can seem ill-defined or incomprehensible to decision makers. Typically, if they get their email (and when do they not?) cyber is working fine for them. Additionally, many years of "alarms" about potential cyber-security disasters have dulled sensitivities to the point that some people question whether a significant impact attack is even possible. Those perceptions work against large budget shares for vaguely explained systems and "software tools."

These barriers will need to be reduced if the collaboration framework is to be effective. The initial pilot development team believes that they can be overcome. National security and financial security depends on creative thinking from those willing non-traditional participants, who can visualize the goal and can see past these barriers. Further, it will require stakeholders at the top to actually become stakeholders, taking the time to understand the cyber domain and be willing to lead the change in policy, regulation, and law. Subsequently, all of their organizational stakeholders can embrace more effective and responsive operational, acquisition, and budgetary paradigms to overcome these challenges.

Summary

The cyberspace domain is a rapidly evolving, contested environment, where the stakes are security, prosperity and, potentially, national sovereignty. The entry requirements are low for adversaries, but their destructive potential is enormous. We cannot cede this to adversaries as an asymmetrical threat environment. We must see first, understand first, and act first to beat the adversaries at their own game—and in doing so, eliminate the asymmetry. Because the risks are shared by everyone who utilizes the "global commons" of cyberspace, there is tremendous value in collaborating on challenges and solutions. No organization has the breadth and depth of talent or money to respond fully to the cyberspace threats. Effective collaboration between the public and private sector will be essential to operational success in cyberspace. The first step to success is to develop a framework for effective collaboration between the public and private sectors.

The charter established by the initial working group is: “To develop a public-private brokerage to advance current and game-changing technologies and processes, proactively addressing emerging cyber-threats through collaboration that ensures mission assurance for the decision maker (warfighter).” Though this working group focused initially on the framework, the value is in establishing an institutionalized, persistent process for addressing the cyber threat.

In an environment where an attack can be delivered at light speed, an effective collaboration framework must leverage a pre-existing collective defense and response partnership to assist warfighters in identifying, analyzing, and responding to cyber threats in an agile and timely manner. For the public/military sector to respond at the speeds demanded in cyberspace, the collaboration pathways between the public and private sectors must be established before the need; and in many cases the responses must be “pre-decided”.

Fueled by an initial investment by Headquarters Air Force’s acquisition leadership and with a mandate to think beyond the current constructs for requirements management, funding and acquisition, an initial group of carefully selected thought-leaders was assembled from highly diverse public/private backgrounds. This very small group (8-10 members) includes government and military leaders, public/private technologists, venture capitalists, science & technology researchers and successful innovators. The development effort is being led by a highly experienced facilitator. Collectively this team is creating actionable plans and deliverables to achieve the vision. In the near term, the initial meeting yielded near-term objectives to establish a governance plan, identifying key stakeholders, building and submitting a business plan for Air Force Operations and Requirements to use as a baseline for follow-on support and finally, creating a pilot effort to demonstrate the collaboration framework capabilities. Although there are numerous issues and elements identified in this framework, which need careful scrutiny and will need to be addressed, private-sector participants must be integral partners in order to achieve our warfighting objectives.

This initiative is resonating with leaders throughout the public/private sector. This team is actively shaping, streamlining and enabling a more effective public/private collaboration mechanism that will be essential to the Air Force’s success in cyberspace.