Reform the Defense Supply Chain to Face the Realities of Conflict in the Digital Age

For centuries, we've operated under the principle that nations are sovereign within their own borders, with traditional rules of war clearly stating that combatants need to be identifiable military targets. Acting on this principle, a functioning government has traditionally had to raise a force more powerful than any potential rival, either internally or externally, when threatened with an act of war.

However, the rules of war are proving to be inadequate to the realities of cyber conflict in the digital age. The border-less nature of cyberspace presents a unique challenge, specifically for the defense sector, in dealing with the traditional governing principles of Law of Armed Conflict. In the digital age, the private sector may well be on the front line of cyber conflict with some asserting that, for national security purposes, the private sector may have to grow into traditional government roles of national defense.

The defense sector is fighting a two-front cyber war right now, with the challenges of fending off millions of attacks on defense networks and the slow burn of economic espionage. The President and Congress need to resolve fundamental issues already under discussion within the defense sector, such as what constitutes "war" in the digital age? What are the rules of engagement and retaliation? Are we really willing to start an armed conflict over a cyber-attack?

Several months ago, the Internet Security Alliance published *The Cybersecurity Social Contract*, a detailed analysis of cybersecurity challenges and solutions, with a chapter devoted solely to the defense sector, which could come in handy to Congress as they exercise their oversight in this area.

One such recommendation – small companies operating within the Defense Industrial Base supply chain need cybersecurity enhancements on a risk-based basis.

Among the most important findings of our work is that the Pentagon has evolved a two-tiered system within the DIB. In the first tier are prime contractors with developed, resilient systems. In the second tier, critical smaller players that make up the primes' supply chain with substantially less effective systems.

It is essential that a risk management framework be put in place for government systems. Risk management frameworks maximize effectiveness by deploying resources toward the most vulnerable elements of a system. An increased focus on the needs of smaller suppliers in the DIB supply chain, for example, would very much be in keeping with risk management directives.

Threats have expanded to attack the defense supply chain. Not only are weapons subject to cyber manipulation, but the developers and innovators who keep the US military on the cutting edge are at risk of having intellectual property stolen through cyber means. The militaristic implications are clear: second level nations skip generations of research and development and become competitive with US weaponry. The economic losses via

intellectual property theft warn of negative downstream effects on future investments and innovation.

A particularly effective way to address supply chain risks would be to modify current military procurement decisions to using a cyber-risk maturity model, as opposed to the binary model currently in use. This approach would incentivize small- to medium-sized businesses to improve their security. The current binary model is burdensome – in terms of both cost and resources – and fails to recognize incremental improvements, as it demands companies fulfill every requirement or be rejected as a prospective contractor.

The maturity proposal developed by our defense industrial base members would allow government and/or prime contractors the ability to tailor contract requirements to a level of security proportionate to the criticality of the information being protected, which would incentivize suppliers to move to the next level to increase eligibility for more important or lucrative contracts.

A tiered model should include a maturity component for each control to reflect a company's progress in taking advantage of each defensive control, which would go a long way toward incorporating the operational aspects of security that differentiate a compliant organization from a secure organization. Fundamentally, a tiered maturity model transforms the cyber environment from one of compliance to one of risk management and competition. A maturity model is inherently a measurement along a sliding scale, introducing the concept of increasing security rather than the binary pass/fail security.

Additionally, government reporting and information-sharing requirements are confusing and divert resources away from security to compliance. New regulations significantly increase costs of doing business with government and shift focus away from risk management to compliance with standards. These increased costs dwarf information technology budgets for small businesses without adding any real enhanced security. Imposing overlapping and redundant cyber requirements drives small companies away from doing business with the government.

Current close-hold information-sharing methods are designed for companies with the infrastructure and resources capable of manually receiving complex threat data, evaluating such data, and applying it to any number of defensive systems. Small companies simply cannot do this. Rather, sharing with small companies requires a passive model in which companies can accept threat data into an automated system and have that data applied to their network defense, creating a broader information-sharing environment that is affordable and passive. Allowing large system integrators to share DoD-provided, unclassified threat indicators with their supply chains could result in a high security payoff at a low cost.

We can achieve these goals with a set of modest tax incentives or a special fund for small companies in the DIB supply chain that provide for targeted deployment of mitigations top level techniques, such as advanced email filtering, multi-factor authentication

(MFA) on remote access, MFA for administrators and externally facing systems, and removal of end-of-life operating systems.

In fact, Executive Order 13636 specifically calls for the deployment of incentives to promote participation in the NIST Framework, as does the House GOP Task Force for Cybersecurity's final report. Yet, we have not seen the development of effective, market-driven incentives. A modest list of incentives could motivate small- and medium-sized businesses who might otherwise not be able to securely serve the DIB supply chain to employ defenses that truly move the cybersecurity needle.

The tiered maturity model discussed above would become another sort of incentive for defense contractors, one in which they could highlight their security postures through branding and market-place competition. The marketing possibilities for small- to medium-sized businesses would be significant, making it attractive for participation.

More – much more – can be discussed as it relates to the defense community and the current cybersecurity environment. But, we'll leave that to another post. For now, Congress – specifically Armed Services – has the opportunity to highlight the above obstacles and use the tools and resources at its disposal to suggest concrete steps to creating a sustainably secure cyber system.