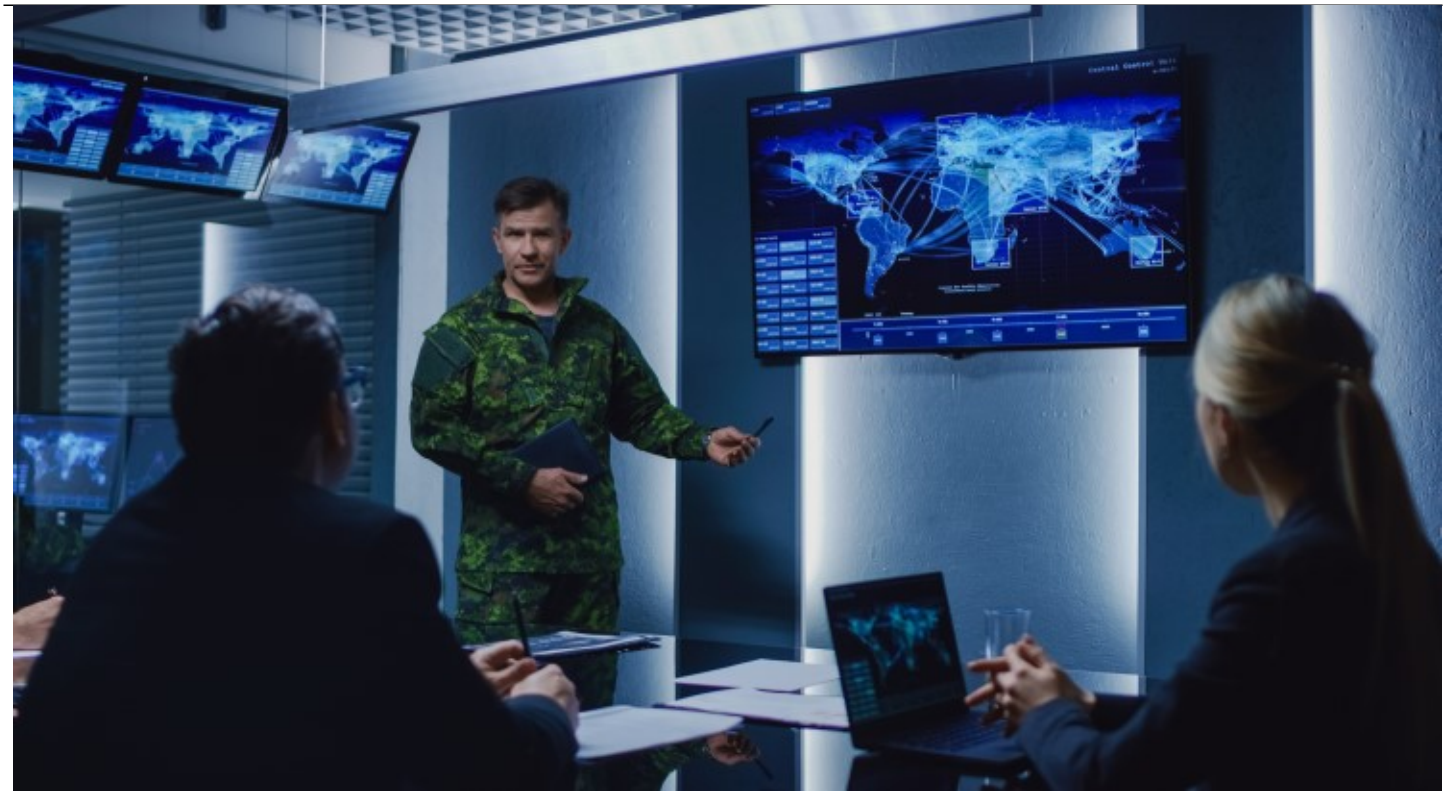
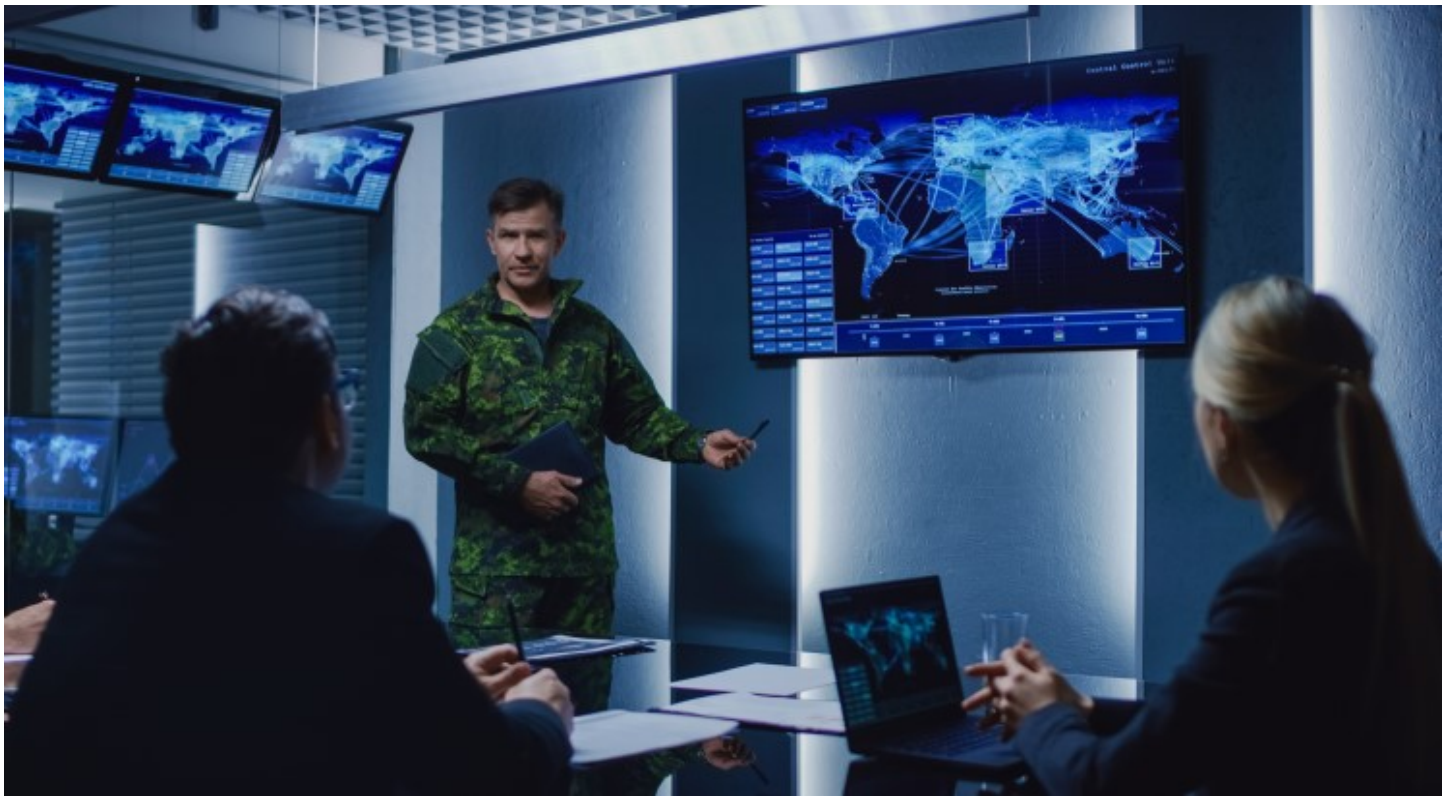
ACC DOCKET
INFORMED. INDISPENSABLE. IN-HOUSE.

How Businesses and the US Government Build Teams to Protect Cyber National Security

Technology, Privacy, and eCommerce





This is the second article in a two-part series about the public and private sectors' joint efforts to protect US national security.

Businesses and the US government must work together to protect national security in the 21st century. But why? Imagine you're the general counsel for a burgeoning startup telecom company that just went through its IPO. Forbes calls your company the "hottest new service provider in the United States." One day you get an invitation from the FBI and US Department of Homeland Security (DHS), offering you and your C-suite a one-day security clearance to participate in a classified cyber briefing at the FBI's Los Angeles office. Curious, you, your chief information security officer (CISO), and your CEO, accept.

A high-ranking FBI assistant director and her colleague from DHS lead the three of you into a silent, windowless room called a "SCIF" (Sensitive Compartmented Information Facility) for the briefing. Your eyes widen as they tell you the National Security Agency (NSA) intercepted communications from an antagonistic foreign power placing your company on its top 10 list of "preemptive strike" cyber targets should hostilities between the two nations increase.

The possibility of your customers suffering, maybe even dying, from a deliberately caused outage makes your fists clench. The assistant director further explains that a sufficiently heinous cyberattack on the US private sector — one causing "significant loss of life, injury, destruction of critical infrastructure, or serious economic impact" — could even lead to a shooting war.

As the briefing ends, the assistant director leans forward and makes her pitch. "Look," she says. "I know you never asked for it, but your company is now defending some of the new front lines of cyber national security. I think we need to work together to protect the country — share intel, develop joint strategies, and more." Her voice grows even more earnest. "We can hash out details later," she continues. "But for now, I just want to know if you're interested. Are you?" Thoughtfully, you lean back and confer with your colleagues. And then respond…

Introduction

The scene above may sound like the opening act of a spy thriller. But setting aside some artistic flair, meetings like this happen in real life, and for good reason. Collectively, the types and volume of threats facing companies providing essential services like telecom, internet, finance, or energy, go beyond the capabilities of any single organization — whether government or private — to repel. Instead, the two sectors must join forces to protect the country. "Think of national security as a puzzle," says Gabriel Taran, the deputy chief counsel for cybersecurity at DHS, when I ask why. He explains:

> *"The US government has information about threat landscapes that aren't available to private companies. But private companies know their systems and needs better than the government. We need to work together to put those pieces of the puzzle together."*

Here are some of the ways that both sectors work together to assemble the national security puzzle:

1. Promoting teamwork — the path to success

In the world of public/private sector national security projects, two sets of players come together to form one team. But for that team to function, one player can't simply dictate terms and expect the other to jump. Instead, both sets of players must have equal input in setting common goals and strategies. Many "critical infrastructure" industries, such as telecom, finance, and energy, have set

up “Coordinating Councils” — bodies comprised of senior industry leaders — to meet regularly with their government counterparts to collectively set those goals.

Below these councils (and other bodies like them) are working teams staffed by representatives from private sector companies and government agencies such as DHS, the US Department of Energy, the FBI, and more. Their mandate is to develop and implement initiatives pursuant to the shared strategic direction set by their leaders.

Though public/private initiatives focusing on cybersecurity have existed since at least 2008, recent years have seen surges of activity. One publicly touted program is Cybersecurity Risk Information Sharing Program (CRISP), which launched in 2014. This program is a national security initiative and jointly championed by the US Department of Energy (DOE) and the private electric sector.

Under CRISP, utilities install sensors on their IT networks to collect certain network traffic, which is then sent to certain DOE national laboratories for analysis using assets otherwise unavailable to the private sector. If that analysis identifies threats or other alarming activity, DOE shares the results with CRISP’s private sector participants, who can use the information to shore up defenses.

CRISP has already shown its mettle. In a 2018 interview with FCW, Rick Perry, the then-Secretary of DOE, credited CRISP with alerting the government and industry “to a really dramatic event […] of Russian intrusion.” According to Secretary Perry, “had we not had this working relationship with our private-sector partners, [that threat] would most likely have gone unfound [to our] great detriment.”

Photo: The FBI Los Angeles Field Office, where the fictional briefing described in the article took place. (By E. Song)

2. Assembling the right team — include lawyers

If cyber national security is a team sport, it's crucial for that team to have the right players. Some companies delegate all things cyber to IT staff, but exercises like Defend Forward, the cyber wargame reported in part one of this series, show that lawyers have roles to play. For example, in developing responses to novel wargame scenarios, questions like "Can we do this?" or "Is taking that action legal?" peppered the game. These questions fall into the lawyer's wheelhouse.

Defend Forward also showed how public and private sector lawyers can proactively solve problems before bad things happen. For example, during the game, several private sector companies requested DHS' help to find specific threats in their respective companies' cybersystems. But even when companies had equal need for that help, some got it more quickly than others.

How? Because, in real life, in-house counsel from a particular industry, and DHS realized that developing shared protocols for seeking and receiving help from each other could help their organizations respond more quickly to events. They then worked to develop those protocols, including legal ones. DHS' Taran, who was involved in that effort, said:

> *"We at DHS are stewards of taxpayer money. That's why we want to work on projects useful to the private sector as well as to us. Working with private sector legal counsel helps us find out what [those projects] are."*

From negotiating national security legal agreements and processes with the government, to helping create new programs from the ground up, the amount of legal work needed to push these public/private sector initiatives forward continues to grow. Still, does every company need to engage dedicated in-house cyber or national security counsel? Not every business needs such a specialist due to cost and other factors.

But companies with enough resources facing advanced technology risks should at least consider hiring an attorney capable of creating and running enterprise-wide technology legal risk management programs. For example, although this article focuses on the benefits of businesses collaborating with the government, there are still risks involved.

Taking any action may risk third party lawsuits if things go south – an argument Apple made when it pushed back against the FBI's request to help unlock an iPhone in 2016. Collaborating may trigger reputational concerns, as Google discovered after employees began protesting the company's involvement in artificial intelligence (AI) research with the US Department of Defense.

Finally, counsel must determine if laws such as the Freedom of Information Act may require the government to disclose sensitive business information shared with the government. These examples represent the tip of the iceberg when the worlds of business, technology, and national security connect. Experienced counsel can help your company successfully navigate these murky waters.

"I'm seeing more companies realizing they need a dedicated cyber or national security legal advisor," says Taran. "The IT people, in particular, need someone who understands what they're doing."

3. Looking ahead — meeting the national security needs of tomorrow

Digital threats to national security evolve at blinding speed. For example, new technologies such as AI, deep fakes, unmanned drones, and more, all trigger national security concerns. Even smart cars

and social media platforms can be weaponized. In order to meet such threats, the public and private sectors must also evolve.

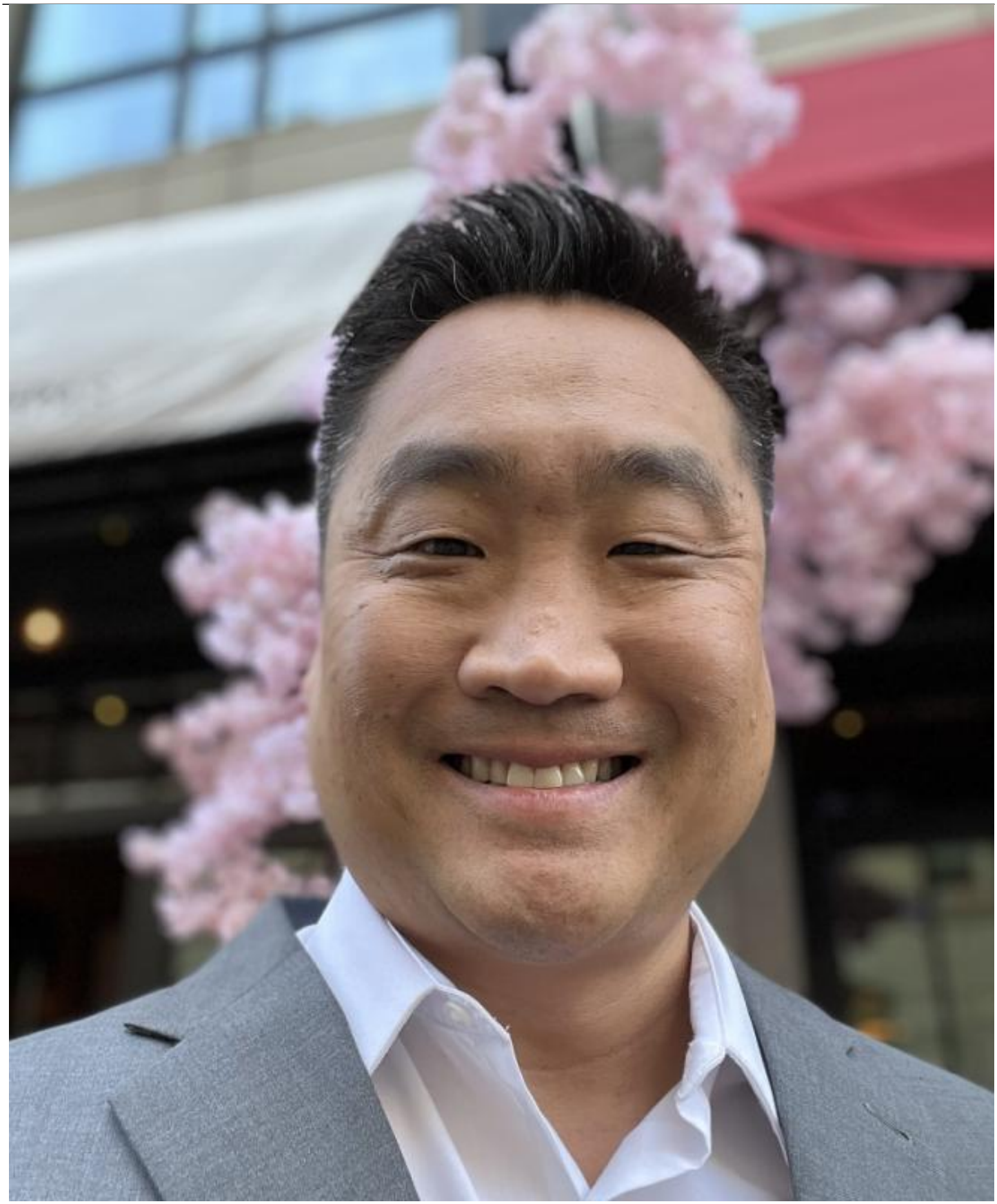
On the legislative policy front, the US Congress authorized a major new commission earlier this year — the "Cyberspace Solarium" — to determine whether Congress should change analog era laws to meet digital era threats (my opinion: yes!). The Solarium's report is due in early 2020 and is expected to be sweeping in nature.

More recently, the GC for the NSA proposed wide-ranging, almost existential, changes to the ways the United States protects national security. Many of those changes would significantly increase the private sector's involvement, costs, and risk, but some may be essential to the United States' survival. On a practical level, I urge public and private sector organizations to cultivate forward-thinking in-house talent capable of innovating solutions to the threats of today, and those forming over the horizon.

Conclusion

Cyber national security represents a vast array of ever-evolving threats. No private company or government agency working alone can repel them all. Instead, the public and private sectors must team up to create unified goals and strategies to meet those threats. Legal counsel should also be included. In the wise words of Leslie Knope from *Parks and Recreation*, it's time to "go find your team and get to work."

Robert Kang



Adjunct Professor

Loyola Law School, Los Angeles & USC Viterbi School of Engineering

Professor Robert Kang serves as adjunct faculty at the foregoing institutions. His role includes training the next generation of attorneys, CISOs and business leaders in meeting emerging technology and national security needs. He also provides corporate training. He is also a former in-house legal executive focusing on technology, cybersecurity and national security. Robert serves as a member of the ACC Foundation's Cybersecurity Advisory Board.

Visit his LinkedIn page.