ACC DOCKET
INFORMED. INDISPENSABLE. IN-HOUSE.

How Cyber Wargames Help Businesses and the US Government Protect National Security

Information Governance

Technology, Privacy, and eCommerce

Banner artwork by DC Studio / *Shutterstock.com*

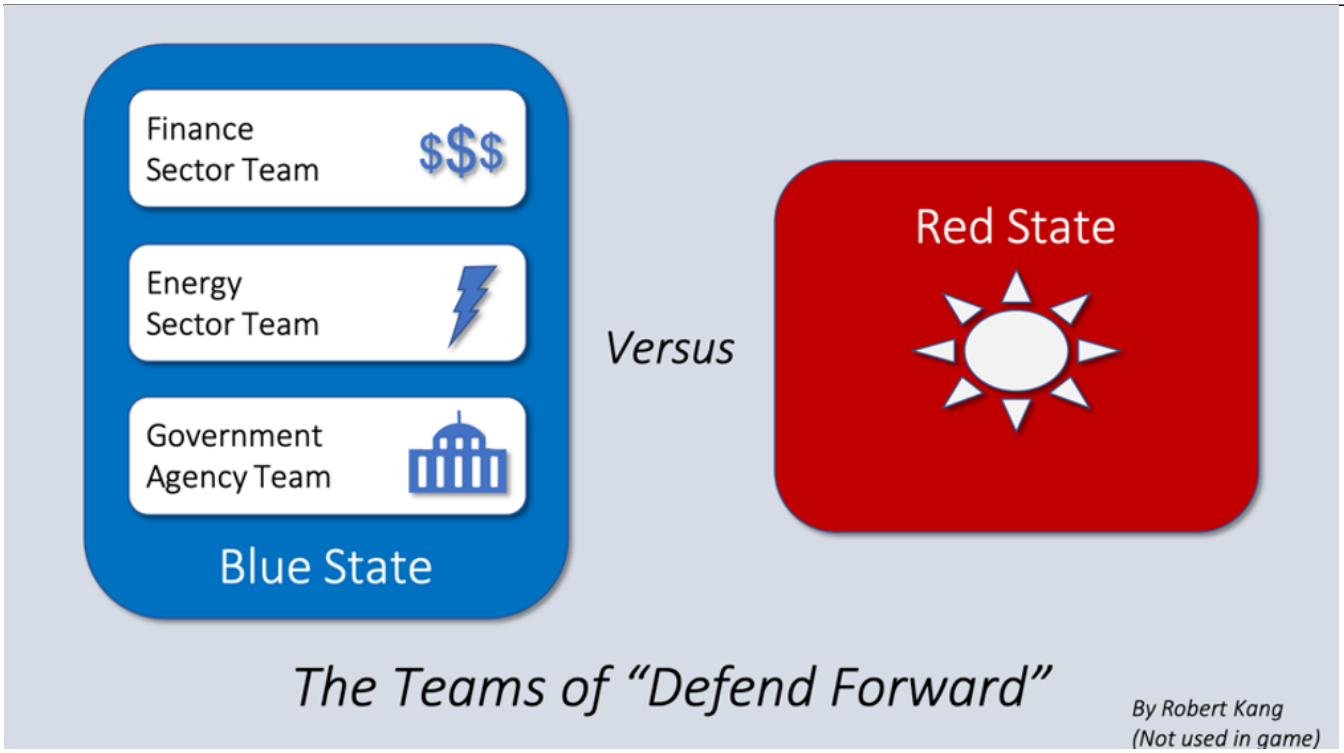
Part one of a two-part series about the public and private sectors' joint efforts to protect national security

Link to Part Two in the series here

Imagine you're the General Counsel or Vice President of Operations at a major US bank. A news alert flashes on your screen, reporting on failed diplomatic talks from the day before with a potentially hostile foreign nation. A few minutes later, your CISO calls, reporting on an explosion of intrusive cyber attempts against your company's mobile banking systems. If successful, they could result in millions of lost dollars and loss of consumer confidence. You wonder if there's a connection. The problems persist for days, leading your CEO to ask whether the company should temporarily take its mobile banking services offline. Now imagine the US Government gets wind of the attacks and determines there is, indeed, a connection between this attack, and that foreign nation. What are the ideal responses in each of these situations?

On July 25 and 26, 2019, leaders from the worlds of business, government and academia – over a hundred strong – gathered at the United States Naval War College in Newport, Rhode Island, to find answers to these questions and more. Welcome to "Defend Forward," the War College's wargame designed to help the public and private sectors prepare for national security cyber incidents. Want to know how? Let's take a look.

How was the game organized?



Cyber wargames come in many shapes and sizes. Jacquelyn Schneider, the War College professor in charge of the team that designed Defend Forward, crafted it to test strategic, executive-level decision making. "The Government and private sector each have their own response strategies, and we wanted to see how they would interact if something happened *today*. We're also looking for 'friction points' that might hinder the public and private sectors from working together."

Game organizers then divided the players into different teams, based on their role. Representing the private sector were leaders from finance and energy companies. That's where I played. Government interests were represented by officials from agencies like the FBI and Department of Defense. Together, we represented "Blue State," the game version of the United States. Arrayed against us were the players of "Red State," a fictional rival of Blue.

Using news reports, emails and other tools, game organizers sent us information from world events to attacks on our computer networks. We then took action based on that information. More on that later. Teams of judges analyzed our decisions to determine their impacts on the game.

What happened?

Imagine rooms of tense people making decisions with too-little-time and too-little-information. For example, Red State's government launched easy-to-spot cyberattacks early against Blue State's banks and electric utilities – the "explosion" of attacks described earlier. My private sector colleagues and I had to decide whether to treat them as one-offs, or as a prelude to something bigger. Considering the sheer scope of attacks – virtually every major bank and electric utility were hit – we took the safer route of significantly upping our defenses.

Blue State government players also faced tough choices: respond to the attacks diplomatically; launch a counterstrike; or do nothing. Considering the importance of the grid and banking systems to the nation, Blue launched a cyber counterstrike – one carefully calibrated to "send a message," but to also comply with international rules of war.

We then dealt with the aftermath of our choices. For example, Blue State's counterstrike startled Red State into stopping their attacks against civilians – a good thing – but it also roiled global financial markets and contributed to a simmering sense of international unease that infused the game. Think "Cold War on Cyber." And what about the private sector's decision to up our defenses? Due to rising geopolitical tensions, we kept them high for six months of simulated gameplay. That call protected our companies, but it wasn't cheap. At some point those decisions became public, causing our customers to worry whether the costs of our goods and services would drastically go up.

These are a small sample of the moves, countermoves and consequences peppering the game. Other moves dealt with issues from election hacking to supply chain cyber risks. Some moves might actually be used in real life; others we tried to see what would happen. Who won? That depends on how one defines "success." Every decision we made had elements of victory and loss. Longer play might have yielded a clear victor. For now, call it a draw.

What were the takeaways?

Defend Forward had two goals: (i) to help the US Government and private sector test our cyber strategies, and (ii) to look for friction points between the two, for real-world policymakers and operators to smooth out before an actual emergency. And though each player likely came away with a different set of takeaways, here are some of mine:

- **Private companies are defending the cyber front lines**
  In the 21st century a hostile power's first cyber target may not be a rival's military base, but rather its civilian infrastructure – finance, telecom, energy and more. In other words, the new front lines of cyber national security are being defended, not by the government, but by private companies. It's a tall order to expect civilian companies to repel sustained cyber assaults by malicious actors armed with the resources of entire nations behind them. The US government and private sector must work together to protect the country.
- **Assemble a diverse team**
  Teamwork is key to solving most problems, but only if the team enjoys a diversity of thought and skills. For example, a Blue State private sector CISO found a creative way to handle supply chain cyber risks with the government, but didn't know whether it would be legal. An attorney proposed using a certain national security law to handle that concern and government players jumped at the idea. Post-game analysis will determine if this idea will work, but it shows promise. "We need people who can cross-talk with each other to find solutions," said Professor Schneider.
- **Pre-planning works**
  Many companies and government agencies have existing protocols and incident response plans. Using them helped Blue State players respond quickly to certain Red State moves. But the game showed that even more pre-planning is needed to smooth out friction points – legal, policy-based and technical – that prevent the government and private sector from working together. Many companies and government agencies – including the Departments of Energy and Homeland Security – are proactively doing just that.

Conclusion

Meeting the national security threats of today is a tough job. In particular, the connected nature of cyberthreats to the public and private sectors, and their consequences, means that the two must cooperate to protect the nation and its people. Playing cyber wargames like Defend Forward together

is one way for these sectors to achieve that goal.

_____

Editor's Note: The Naval War College will later issue a comprehensive report on this wargame. Contact the War College or the author of this article for a copy.

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.