During the Second World War the United States greatly benefited from its geostrategic position. The United States mainland and its private sector industrial capacity remained largely untouched throughout the conflict. Today it is difficult to imagine a similar scenario playing out in a war between great powers like the United States and China.

A situation where modern digital weapons turn cyberspace into battlespace is foremost in the minds of many defense experts. The hyperconnectivity propelling the United States into the twenty-first century doubles as a major vulnerability in a wartime setting. America must prepare to defend government networks as well as those of private industries working on potentially disruptive wartime technologies or managing critical infrastructure. Private-public cybersecurity partnerships are in their infancy, but so far fail to address one very disturbing question: What happens when war is all but certain and an important private sector actor is not only unprepared, but unwilling to take vital steps to secure its networks?

The potential answers to this question are uncomfortable, but clear: disruptive civilian technologies with wartime implications cannot be destroyed or stolen by the enemies of America or her allies. The domestic private sector—in the worst of situations—may need to be made legally liable for failure to partner with government network defense entities in a timely manner. America should act now to design such a statutory framework to provide the executive branch with the tools it needs to defend the country while also preventing constitutional overreach.

**Private Networks Already Under Attack**

Who wins the next modern conflict will depend largely on private sector technologies currently meant for ubiquitous civilian use. Artificial intelligence, 3D printing, hypersonics, quantum computing, 5G/6G networks, autonomous platforms, robotics, and even biotechnology will provide paths to victory for the nation using them effectively for military or infrastructure applications. The United States and China are locked in a race to dominate these technological fields, and it should come as no surprise that illegal Chinese acquisition of American intellectual property was on the rise throughout the last two decades.

The capacity for the Chinese Government to access and exploit American public and private industrial and infrastructure-related networks was laid bare by the Office of Personnel Management hack in 2015, the Microsoft Exchange breach in 2020, and recently the Pulse Secure VPN and Colonial Pipeline hacks of 2021. All of these hacks are disturbing, but the concerns regarding the Microsoft hack in particular are more alarming not only for the hack’s size and scope, but its sophistication. Experts are concerned China’s hacking and social media “data scraping” allowed the communist government to cross-reference stolen data and use it to breach
security manager protocols in some of Microsoft’s most critical systems. While any damage done to these systems appears minimal for now, the implications for wartime are ominous.

**Filling the Statutory Void**

There are myriad indicators of statutory weakness in light of the abovementioned hacks. The Cybersecurity & Infrastructure Security Agency (CISA), which is the Department of Homeland Security’s premiere cybersecurity risk-advising organization, is not statutorily-equipped to deal with breaches in vital private sector industries. The Pulse Secure hack emphasizes this fact.

CISA’s strongest statutory remedy for mitigating the effect of the Pulse Secure intrusion was to issue an emergency directive to government agencies asking them to take “lawful action ...for the purpose of protecting the information system from, or mitigating, an information security threat.” The power CISA possesses is more to advise (mostly federal) entities to take action to secure their systems, and/or partner with these agencies to close loopholes in their security software through information sharing. Often these measures are reactionary in nature coming after a major cyberattack already occurs.

But what of the domestic industries that are not currently partnered with the Federal Government, but will be in a future conflict? What if CISA or the Federal Government more broadly have the means to protect these industries with more than information sharing or cyber stress-tests, but the industry demurs? This scenario may seem hard to imagine, but we’ve already seen a reluctance by some major companies like Google to partner with the United States Government for defense purposes. Such refusals will likely be viewed as unacceptable when danger of a major war is imminent.

For these reasons, the United States needs to grant the power to the president to hold private sector companies developing disruptive technologies or managing critical infrastructure legally accountable. For instance, failure to work with the government, report attacks or vulnerabilities, or ensure the integrity of cyber systems critical to national survival would draw potential fines or punitive damages or remedies for harm done to the systems. Such authorities would be akin to the idea of the Defense Production Act, which allows the president to compel private industry to re-tool industrial capacity during national emergencies.

**Quelling Fears of Overreach, With Oversight**

Broad legislation granting the powers mentioned above will likely concern those who are worried about nationalization of private industry digital networks or government spying. But the question that should be asked is whether the imminent threat of a national cyber emergency or conflict would not invite that type of executive branch overreach anyway? Shouldn’t the rules be made clear now? Leaving the executive branch to act in unprecedented situations without congressional guidance will oftentimes invite it to create its own legal justifications and punishments with egregious constitutional consequences (think Korematsu or Youngstown Sheet & Tube). The solution proposed would constrain what the government can do on a private network by
defining the consequences beforehand, while still achieving the cooperation necessary to ensure that network’s security for national defense before an attack and without a forced takeover.

Congress need not look far for workable solutions as government organizations like CISA are already committed to formulating the relationships necessary to partner with private organizations. CISA works to advise private industry by placing cyber experts alongside those of the companies and agencies it helps rather than coercing them through a hostile takeover. Often this is done with those entities’ full cooperation and little constitutional or coercive concerns. As the Federal Government’s cyber defense capabilities continue to mature, the framework created by this legislation can require additional congressional oversight of CISA’s private industry activities to ensure it is achieving its cybersecurity objectives without unconstitutional overreach. Even if a private industry initially refused government help but was then compelled to act under the new liability law, this additional oversight should help mitigate vast government abuses inside a network. Even then, remedies through the courts would still be available to private companies and reviewable under law.

Conclusion

Cyber threats evolve with each passing day and the United States must develop the tools it needs at home to defend against them. A new era of great power competition means that preparation for wars in traditionally unconventional domains is paramount and, in the Cyber Domain, all of America is a battlespace. The National Defense Authorization Acts of 2018 and 2021 provided CISA with some of the “teeth” it needs to defend the nation’s critical infrastructure and governmental agencies. Congress should continue this trend by ensuring the executive branch has the tools it needs to partner with—and when necessary, hold legally accountable—private industry to secure its networks before the need arises. Not after.