



## Executive Order Marks Progress in Battle Against Cyberattacks

In the wake of the spring 2017 [“WannaCry”](#) cyberattacks on governments and businesses worldwide, cybersecurity is back in the spotlight and as complex and high-stakes as ever. A few hours before the attack launched, the White House issued its long-awaited [Cybersecurity Executive Order](#), a new tool in securing the nation and its economy in a global era.

It has been six years since the Pentagon first [declared](#) cyberspace “an operational domain,” and far from the political fray, a partnership of leading public and private “cyber warriors” are leading this mission-critical defense. Here are five ways the recent executive order helps:

- **International Cooperation.** WannaCry wreaked havoc around the world. Whether attacks come from nation-states or unaffiliated criminal or terrorist hacker networks, more international cooperation is a must. The order calls for new strategies to work across borders to deter these attacks, work that should be prioritized in the weeks and months to come.
- **Battling Botnets.** In tackling the thorny global issue of botnets—robot networks that infect connected devices with malware and use them to launch attacks—the focus has rightly extending beyond an overly narrow focus on core communications infrastructure to also include the broader internet ecosystem. Device manufacturers, software developers, ecommerce platforms, search engines and social media sites all need to share responsibility to deploy a cohesive and effective national cyber-defense.
- **Collaborating on Critical Infrastructure.** The order embraces the public-private collaborative framework that has defined the nation’s cybersecurity efforts from day one. This helps ensure government cyber leaders continue to work closely with their private sector counterparts to help support the security of our financial systems, power grid, broadband networks and other essential infrastructure to help ensure it is both well-defended and resilient.
- **Tearing Down the Silos.** The order recognizes it’s time to push past today’s patchwork of often- clashing information technology architectures across the vast maze of federal bureaucracy. Taking a page from the discipline of innovators and industry, the order calls for an “enterprise architecture” approach, where departments and agencies essentially act as divisions of one company all working together toward common systems and security practices.
- **Modernizing Government Technology.** In a world where cyberwarfare—both overt and covert—is a daily reality, the order recognizes that government systems must be built

on modern, state-of-the-art technology. This is an essential component of our nation's defense. The price tag won't be cheap, and Congress will need to engage to see this through.

This latest executive order serves as a useful reminder that government can get it right on priorities that matter most, particularly when working with—not against—American businesses and other stakeholders to present a united front to the world.