The Rogers-Ruppersberger Cybersecurity Bill

The Cyber Threat: Every day U.S. businesses are targeted by nation-state actors like China, Iran and Russia for cyber exploitation and theft, resulting in huge losses of valuable trade secrets and sensitive customer information. This rampant industrial espionage costs American jobs.

- When these hackers steal these trade secrets, they take new, high-paying jobs right along with it. Estimates of loss from cyber economic espionage are hard to make, but range up to $400 billion a year. **Just as important, many of the same vulnerabilities used to steal trade secrets can be used to attack the critical infrastructure we depend on every day.**

- China is the world's most active and persistent perpetrator of cyber economic espionage. U.S. companies have reported an onslaught of Chinese cyber intrusions that steal sensitive information like client lists, merger and acquisition data, pricing information, and the results of research and development efforts. This illegally-acquired information gives Chinese companies an unfair competitive advantage against the American companies from which it was stolen.

Intelligence Sharing to Help the Private Sector Protect Itself: Most elements of the private sector are already working hard to make their networks more secure. They are too often hindered, however, by a lack of information about what attacks other American companies are experiencing and how they are coping with those attacks.

- Too often, companies that would like to share cyber threat information with other parts of the private sector are prevented or deterred from doing so by a range of policy and legal barriers.

- Just as importantly, the U.S. Intelligence Community collects classified information overseas about advanced foreign cyber hackers and their plans to attack the networks of American companies. Unfortunately, a lack of positive legal authority to share such information hinders the government's ability to distribute it, and the vast majority of the private sector doesn't get the benefit of it. If Congress could provide that positive authority to share its classified threat information in a timely and operationally useful form, the private sector would be able to better defend itself against nation-state actors in cyberspace.

    - An innovative program developed by the Defense Department proves that this can work. The Defense Industrial Base Enhanced Cybersecurity Services program (DECS) provides classified cyber threat intelligence to communications service providers who use it protect defense contractors who voluntarily participate in the program. DECS demonstrates how sharing intelligence can enhance private cybersecurity without any direct government involvement or monitoring.

- In April 2012, the full House of Representatives approved the Cyber Intelligence Sharing and Protection Act (CISPA), which builds on the DECS model, by a strong bipartisan vote of 248-168. The Senate failed to act on cybersecurity legislation in the last Congress, but CISPA will be reintroduced today in the House.

- Previously, in December 2011, the House Permanent Select Committee on Intelligence (HPSCI) passed CISPA out of committee on a strong bipartisan vote of 17 to 1, and when it was considered on the House floor, the bill had 112 bipartisan cosponsors.

- This important legislation enables cyber threat sharing within the private sector and, on a purely voluntary basis, with the government, all while providing strong protections for privacy and civil liberties.

  - Voluntary information sharing with the federal government helps improve the government's ability to protect against foreign cyber threats and gives our intelligence agencies tips and leads to help them find advanced foreign cyber hackers overseas. This in turn allows the government to provide better cyber threat intelligence back to the private sector to help it protect itself.

- This bipartisan legislation was developed in close consultation with a broad range of private sector companies, trade groups, privacy and civil liberties advocates, and the Executive Branch.

  - Based on helpful input from the privacy and civil liberties community, the HPSCI adopted an amendment offered by the Chairman and Ranking member during committee markup in December 2011 that significantly limited the government's use of information voluntarily shared by the private sector.

  - In April 2011, the Chairman and Ranking Member announced additional changes to the legislation to further enhance protections for the privacy and civil liberties of Americans, including a package of five amendments on the House floor.

- These provisions of the legislation, along with others, serve to strongly protect privacy and civil liberties.

  - First, the bill permits only the voluntary sharing by the private sector of a very limited category of information—cyber threat information—and permits only the sharing of such information for cybersecurity purposes, a similarly limited term.

  - The bill protects privacy by prohibiting the government from forcing private sector entities to provide information to the government, by encouraging the private sector to "anonymize" or "minimize" the information it voluntarily shares with the government, and by explicitly authorizing and encouraging the government to create procedures to protect privacy and civil liberties.

  - The bill also puts in place strict restrictions on the use, retention, and searching of any data voluntarily shared by the private sector with the government.

  - The bill enforces these strong privacy and civil liberties protections by permitting individuals to sue the federal government for damages, costs, and attorney's fees in federal court, and provides for strong public and Congressional oversight by requiring the independent Inspector General of Intelligence Community to conduct a detailed review of

the government's use of any information voluntarily shared by the private sector, and by requiring the Inspector General to provide recommendations to Congress—in an unclassified report—to better protect privacy and civil liberties.

- The bill also carefully limits the information that private sector entities may search for and share on a voluntary basis with others, including the government. The definitions contained in the statute which set these limitations were narrowed to clarify that the bill is focused on helping the private sector to defend against attempts by advanced cyber hackers, from countries like China, to gain unauthorized access to networks and exfiltrate sensitive information.

- The legislation also makes clear that no new authorities are granted to the Defense Department, National Security Agency, or any other element of the Intelligence Community to direct private or public cybersecurity efforts and further that nothing in the bill authorizes any entity to deploy government-owned or controlled equipment on private sector systems or networks to protect such systems or networks.

- Finally, the bill will sunset in five years, permitting Congress to carefully review the use of the authorities provided under the legislation and determine whether they should be extended or modified.

- By allowing the private sector to expand its own cybersecurity efforts and to employ classified information to protect systems and networks, this bill will harness private sector drive and innovation while also keeping the government out of the business of monitoring and guarding private sector networks.

  - This bill will not require additional federal spending or the creation of a vast new government bureaucracy. It will impose no new regulations or unfunded mandates.

  - This legislation is a critical, bipartisan first step toward enabling America's private sector to do what it does best: create, innovate, and sell cybersecurity solutions.