Cyber Naïveté

First Washington ignored the al Qaeda threat. Now they're doing the same with the cyber threat. It's time to wake up.

BY FRANK R. WOLF

My colleague, Representative Mike Rogers, the chairman of the House Intelligence Committee, often says that there only two types of companies in America: those who have been attacked by Chinese cyberattacks and know it, and those who have been attacked but don't yet know it.

Chairman Rogers' comments are particularly prescient, given the enormous costs this cyber espionage is having on Western companies and their competitiveness with state-owned or state-connected Chinese companies, which appear to the be the beneficiaries of this stolen data.

By now, most everyone is aware of the pervasive threat from Chinese cyber espionage and cyber attacks—targeting both government and private business networks. These attacks are no longer just probing for national security information; they are seeking private firms' intellectual property, trade secrets, and any other information that could be used to provide Chinese companies with an unfair advantage over their Western counterparts. It's

Frank R. Wolf (R) represents Virginia's 10th congressional district in the U.S. House of Representatives, serving since 1981. Congressman Wolf sits on the House Appropriations Committee, where he is the Chairman of the Commerce-Justice-Science Subcommittee.

THE INTERNATIONAL ECONOMY
THE MAGAZINE OF INTERNATIONAL ECONOMIC POLICY
220 I Street, N.E., Suite 200
Washington, D.C. 20002
Phone: 202-861-0791 • Fax: 202-861-0790
www.international-economy.com
editor@international-economy.com

ultimately undermining job creation in the United States and impacting the economic recovery.

Cyber espionage is having a real and corrosive effect on job creation in the United States and other western countries. Last year, the *Washington Post* reported that "[t]he head of the military's U.S. Cyber Command, General Keith Alexander, said that one U.S. company recently lost $1 billion worth of intellectual property over the course of a couple of days—'technology that they'd worked on for twenty-plus years—stolen by one of the adversaries.'"

And should there be any confusion about who is responsible for these cyber attacks: Chairman Rogers remarked in an October 2011 *Washington Post* article that "When you talk to these companies behind closed doors, they describe attacks that originate in China and have a level of sophistication and are clearly supported by a level of resources that can only be a nation-state entity."

Yet despite the constant, pervasive attacks and the enormous associated costs to business and government, the U.S. public and private sectors remain unprepared to adequately defend against, and unwilling to articulate, a response to these Chinese actors.

This is particularly frustrating to me, as an early target of Chinese cyber espionage. In August 2006, my congressional office's computers were attacked by "entities within China," very likely connected to the Chinese government. The computers were targeted and stripped of information about dissidents in China that I had been working to assist.

The computers in the offices of sixteen other members were similarly compromised, as well as those of the House Foreign Affairs Committee.

In subsequent meetings with FBI officials, it was revealed that the outside sources responsible for this attack came from within the People's Republic of China. My suspicion is that I was targeted by Chinese sources because of my long history of speaking out about the Chinese government's abysmal human rights record.

The fact that the Congress was attacked in such a brazen manner outraged me, and I wanted to share this incident with the public as a "cautionary tale" for other government offices and private firms. Yet the FBI and other federal officials urged me to remain silent, lest I "let the perpetrators know that we knew" what they had done.

After two years, I nonetheless took to the House floor in June 2008 to inform my colleagues—and the public and business community—about the incident and warn of the growing threat to the U.S. government and businesses.

I believed it was important for the public to better understand this threat and what the attackers wanted—not national security secrets, but information about all of

Representative Mike Rogers (R-MI): *The chairman of the House Intelligence Committee often says that there only two types of companies in America: Those who have been attacked by Chinese cyberattacks and know it, and those who have been attacked but don't yet know it.*

The economic and security costs of failing to prevent a "cyber Pearl Harbor" are too great to anticipate.

Cyber espionage is having a real and corrosive effect on job creation.

the casework I had done on behalf of political dissidents and human rights activists around the world.

It's almost stunning how much has changed since I spoke out on the House floor in 2008. Over the last four years, there has been a "sea change" in how senior defense and intelligence officials publicly discuss the cyber threat.

Four years ago, some of these same leaders who were warning against even publicly acknowledging cyber attacks—much less the source of the threat—are now publicly warning of the Chinese threat in very stark terms.

Last year, the usually reticent Office of the National Counterintelligence Executive issued a warning that "Chinese actors are the world's most active and persistent perpetrators of economic espionage." The counterintelligence office took this rare step of singling out the Chinese due to the severity of the threat to U.S. national and economic security.

During an appearance before the Senate Select Committee on Intelligence earlier this year, FBI Director Robert Mueller said that while terrorism is the greatest threat today, "down the road, the cyber threat will be the number one threat to the country."

Additionally, a 2010 Pentagon report highlighted China's cyber espionage efforts. The U.S. intelligence community notes that China's attempts to penetrate U.S. agencies are the most aggressive of all foreign intelligence organizations.

Defense Intelligence Agency chief General Ron Burgess also recently testified that "China has used its intelligence services to gather information via a significant network of agents and contacts using a variety of methods. In recent years, multiple cases of economic espionage and theft of dual-use and military technology have uncovered pervasive Chinese collection efforts."

It is noteworthy that while the taciturn national security community is now loudly ringing the alarm about the threat from Chinese cyber espionage, the business community remains relatively quiet about the losses from these persistent attacks. It is time for both the government and the private sector to speak out against the actors perpetrating this theft and agree on appropriate penalties for states that engage in these tactics. But we must act now, before it is too late.

The parallels between the warnings about the terrorist threat prior to 9/11 and the Chinese cyber threat today, while not exact, are disturbingly similar.

The computers were targeted and stripped of information about dissidents in China that I had been working to assist.

We are beginning to witness the consequences of this inadequately addressed cyber threat. According to a March 13, 2012, *New York Times* article, "During the five-month period between October and February, there were eighty-six reported attacks on computer systems in the United States that control critical infrastructure, factories and databases, according to the Department of Homeland Security, compared with eleven over the same period a year ago."

In an interview with the *New York Times,* Homeland Security Secretary Janet Napolitano said, "I think General Dempsey said it best when he said that prior to 9/11, there were all kinds of information out there that a catastrophic attack was looming. The information on a cyberattack is at the same frequency and intensity and is bubbling at the same level, and we should not wait for an attack in order to do something."

The parallels between the warnings about the terrorist threat prior to 9/11 and the Chinese cyber threat today, while not exact, are disturbingly similar. However, we know the consequences of inaction for terrorism: The failure to address the al Qaeda threat before 9/11 cost more than three thousand lives, cost tens of billions in economic damage, and led to two wars costing upwards of $1 trillion.

The economic and security costs of failing to prevent a "cyber Pearl Harbor" are too great to anticipate, but if the government and business community takes proactive steps now, we could prevent untold damage to the global economy. ◆