REUTERS

PROVIDENCE Journal | Providence Journal eEdition

Protecting against cyber-attacks

By Senators Lindsey Graham and Sheldon Whitehouse
April 9, 2013

Last year, Congress failed to forge a workable framework for cybersecurity to protect the United States against a fast-growing national security and economic threat. Our cyber-networks remain dangerously vulnerable to outside attack and are the repeated targets of foreign governments intent on stealing the fruits of our intellectual and business efforts. Congress must address this crucial issue.

The threat to our critical infrastructure, national security and economic prosperity was laid out in a February report by Mandiant, a respected U.S. computer security firm. An elite unit of Chinese hackers affiliated with China's People Liberation Army, the report concluded, is likely behind a wave of attacks on U.S. government and business computer systems.

Since 2006, according to the report, the Chinese unit has stolen data – including blueprints, test results, business plans and emails – from at least 115 U.S. companies across a wide spectrum of major industries.

Almost every facet of American life is threatened when intruders exploit our cyber-vulnerabilities. And the risk is not from China alone. Foreign governments like Iran and terrorist organizations such as al Qaeda seek to worm into critical national infrastructure and threaten catastrophe here at home. Foreign agents raid our companies, stealing plans, formulas and designs. Foreign criminal networks take money out of our banks, defraud consumers with scams and sell illicit goods and products, cheating U.S. manufacturers. It may be the greatest illicit transfer of wealth in human history.

If you're a business owner, listen to our top cyber-experts, who say there are only two kinds of businesses: those that have been hacked, and those that don't know they've been hacked. If you're a consumer, know there's a third group: those who know they've been hacked and won't admit it.

Following Congress' failure to act, President Barack Obama has issued an executive order to address some of our nation's vulnerabilities. But an executive order can't accomplish everything that needs to be done.

We both worked hard last year to forge a bipartisan legislative compromise, and still believe it can be reached. To get this right, a bipartisan solution must include the following elements:

First, there must be far more disclosure of cyber-threats. Americans should not be in the dark about the risks we face. The government should do more public reporting, and companies should be candid with shareholders and customers about the problems.

Second, companies that operate critical U.S. infrastructure should meet some basic standard to protect their customers and our way of life. We have discussed ways for government to work with industry to set these standards while allowing private-sector initiative to determine the specific manner of companies' compliance. The model may work for other sectors, as a more nimble, smarter alternative to overly prescriptive administrative regulation.

Third, government agencies and private industries, particularly the communications companies that run the Web's infrastructure, need to share more information about the threats they see on their networks. This will require removing existing legal barriers – while protecting classified information and privacy.

Fourth, prosecutors should have the resources to pursue international cyber-criminals. These cases are technically and legally complex; involve difficult intelligence and diplomatic and foreign law challenges, and require massive forensic capability. Rather than complain about cyber-robbers overseas, we'd like to see them indicted and prosecuted.

Fifth, we need to make sure that training is available to bring Americans into the cybersecurity field, and maintain our technical leadership in this crucial area. Cyber-danger is not going away. More and more of our business and personal lives will take place in cyberspace. Cyber-threats will expand and evolve. America must be prepared.

In all this, we must safeguard the privacy of U.S. citizens. We can keep the United States secure without infringing dearly held liberties. Well-crafted legislation can achieve this.

We must do this, because we never want to see a nightmare scenario become reality.

Imagine waking up one morning to find the power out at home, and no signal on the phone or computer to tell you what's going on. You drive into town and find dozens of people in front of the banks, wondering why the ATMs aren't working. There are lines at gas stations and supermarkets because businesses can't process sales on credit or debit cards.

The failures all around you – no heat or air conditioning, no banking, no Internet or phone, and cash-only sales in the stores that are open – have no end in sight. There may even be smoke on the horizon from a plant on the outskirts of town, aflame because of compromised equipment.

A cyber-attack could cause all this. We need to work together to ensure America never has to face that day.

Senator Lindsey Graham (R-S.C.) is ranking member of the Subcommittee on Crime and Terrorism of the Senate Judiciary Committee and also serves on the Armed Services and Budget Committees. Senator Sheldon Whitehouse (D-R.I.) serves on the Senate Judiciary Committee and is the chairmen of its Subcommittee on Crime and Terrorism. In 2010 he served as co-chairman of the Select Committee on Intelligence's Cyber Task Force.

ANNUAL REPORT TO CONGRESS

Military and Security Developments Involving the People's Republic of China 2013

Office of the Secretary of Defense

Preparation of this report cost the Department of Defense a total of approximately $95,000 in Fiscal Years 2012-2013.

missiles with ranges of 1,000km and speeds of 2,800m/s. China's domestic CSA-9 long-range SAM system is expected to have a limited capability to provide point defense against tactical ballistic missiles with ranges up to 500km. China is proceeding with the research and development of a missile defense umbrella consisting of kinetic energy intercept at exo-atmospheric altitudes (>80km), as well as intercepts of ballistic missiles and other aerospace vehicles within the upper atmosphere. In January 2010, and again in January 2013, China successfully intercepted a ballistic missile at mid-course, using a ground-based missile.

Cyber Activities Directed Against the Department of Defense. In 2012, numerous computer systems around the world, including those owned by the U.S. government, continued to be targeted for intrusions, some of which appear to be attributable directly to the Chinese government and military. These intrusions were focused on exfiltrating information. China is using its computer network exploitation (CNE) capability to support intelligence collection against the U.S. diplomatic, economic, and defense industrial base sectors that support U.S. national defense programs. The information targeted could potentially be used to benefit China's defense industry, high technology industries, policymaker interest in US leadership thinking on key China issues, and military planners building a picture of U.S. network defense networks, logistics, and related military capabilities that could be exploited during a crisis. Although this alone is a serious concern, the accesses and skills required for these intrusions are similar to those necessary to conduct computer network attacks. China's 2010 Defense White Paper notes China's own concern over foreign cyberwarfare efforts and highlighted the importance of cyber-security in China's national defense.

Cyberwarfare in China's Military. Cyberwarfare capabilities could serve Chinese military operations in three key areas. First and foremost, they allow data collection for intelligence and computer network attack purposes. Second, they can be employed to constrain an adversary's actions or slow response time by targeting network-based logistics, communications, and commercial activities. Third, they can serve as a force multiplier when coupled with kinetic attacks during times of crisis or conflict.

Developing cyber capabilities for warfare is consistent with authoritative PLA military writings. Two military doctrinal writings, *Science of Strategy,* and *Science of Campaigns* identify information warfare (IW) as integral to achieving information superiority and an effective means for countering a stronger foe. Although neither document identifies the specific criteria for employing computer network attack against an adversary, both advocate developing capabilities to compete in this medium.

The *Science of Strategy* and *Science of Campaigns* detail the effectiveness of IW and CNO in conflicts and advocate targeting adversary C2 and logistics networks to affect their ability to operate during the early stages of conflict. As *Science of Strategy* explains, "In the information war, the command and control system is the heart of information collection, control, and application on the battlefield. It is also the nerve center of the entire battlefield."

In parallel with its military preparations, China has increased diplomatic engagement and advocacy in multilateral and international forums where cyber issues are discussed and debated. Beijing's agenda is frequently in line with Russia's efforts to promote more international control over cyber activities. China and Russia continue to promote an Information Security Code of Conduct that would have governments exercise sovereign authority over the flow of information and control of content in cyberspace. Both governments also continue to play a disruptive role in multilateral efforts to establish transparency and confidence-building measures in international fora such as the Organization for Security and Cooperation in Europe (OSCE), ASEAN Regional Forum, and the UN Group of Governmental Experts. Although China has not yet agreed with the U.S. position that existing mechanisms, such as international humanitarian law, apply in cyberspace, Beijing's thinking continues to evolve.

Role of Electronic Warfare (EW) in Future Conflict

An integral component of warfare, the PLA identifies EW as a way to reduce or eliminate U.S. technological advantages. Chinese EW doctrine emphasizes using electromagnetic spectrum weapons to suppress or deceive enemy electronic equipment. PLA EW strategy focuses on radio, radar, optical, infrared, and microwave frequencies, in addition to adversarial computer and information systems.

Chinese EW strategy stresses that it is a vital fourth dimension to combat and should be considered equally with traditional ground, sea, and air forces. Effective EW is seen as a decisive aid during military operations and consequently the key to determining the outcome of war. The Chinese see EW as an important force multiplier and would likely employ it in support of all combat arms and services during a conflict.

PLA EW units have conducted jamming and anti-jamming operations testing the military's understanding of EW weapons, equipment, and performance, which helped improve their confidence in conducting force-on-force, real-equipment confrontation operations in simulated electronic warfare environments. The advances in research and deployment of electronic warfare weapons are being tested in these exercises and have proven effective. These EW weapons include jamming equipment against multiple communication and radar systems and GPS satellite systems. EW systems are also being deployed with other sea and air-based platforms intended for both offensive and defensive operations.