THE SACRAMENTO BEE sacbee.com

The Conversation: Time to mobilize for cyberwar

Special to The Bee

Published Sunday, Apr. 08, 2012

Join the conversation: How worried are you about cyberattacks and cyberthefts? And what should Congress do about cybersecurity? Leave a comment at the end of this story, or go to our Facebook page.

Iran's drive to become a nuclear power hinges partly on a facility outside the small mountain town of Natanz. According to intelligence analysts, the facility houses thousands of centrifuges used to enrich uranium to levels that could support nuclear weapons development, which has raised worldwide fears of a nuclear Iran. Amid faltering negotiations with the West to curb Iran's drive for nuclear power and with enrichment activities well under way, the Natanz facility mysteriously began to suffer technical difficulties in late 2009 and early 2010.

Without warning and for no apparent reason, nearly a thousand centrifuges began speeding up and slowing down, in ways that seemed calculated specifically to destroy them. At the same time, the systems monitoring those centrifuges did not register a single problem. Those centrifuges were destroyed, according to reports, and Iran's nuclear program was set back months – maybe years.

The computer programs running those centrifuges had been infected with a highly sophisticated computer worm, known as Stuxnet. This worm was 20 times more sophisticated than any worm or computer virus previously discovered, and news reports suggested that Israeli and American militaries had worked together to create it. Thus, if true, the United States and Israel launched a cyberattack on Iran's nuclear facilities no less effective than a nighttime air raid with missiles and smart bombs – but one that was far more secretive and deniable.

The Stuxnet attack on Natanz is one of many cyberattacks or cyber-intrusions in recent years, some of which have targeted U.S. government agencies and American corporations. These attacks and intrusions have stimulated a debate in Congress on how best to address national security in the digital age – without compromising our privacy, our civil liberties and our democracy.

Beyond Stuxnet, other cyberattacks have been in the news but are not as well known. In 2007, Estonia's government websites were taken offline by computer attacks originating from within Russia, although the Russian government denied involvement. In 2008, the Russian government was more clearly involved in a concerted cyberattack on the neighboring country of Georgia. Weeks before Russia sent ground troops into Georgia, Georgian government websites were taken offline with massive computer attacks, possibly the first time a cyberattack had been launched in conjunction with a shooting war.

Hackers and hacktivists strike

Other cyberattacks have been unleashed by organized crime, which can take down sites of large companies and charge them "protection money" to stop the attacks. Recent reports even suggest that a company's competitors are likely to engage in attacks to gain a business advantage. Loosely organized hackers or hacktivist groups also have unleashed their anger and made political statements by taking down the sites of Sony Corp., the Department of Justice and the FBI.

These examples overlook the most common attacks: those undertaken not to harm computer systems but to steal information. According to U.S. government reports, many of the nation's largest, most advanced companies have been subject to intrusions and theft of their intellectual property. U.S. officials have pointed the finger at the Chinese government, acting on behalf of its own companies seeking to steal and copy innovations by American companies.

The most talked about example took place in January 2010, when Google announced that cyberattacks from China were designed not to take Google offline but to steal valuable information and software. Other companies have been subject to attacks, including Citigroup, among the nation's largest banks, and Lockheed Martin, the nation's largest defense contractor. Major U.S. energy companies have been compromised and subject to theft in an attack originating from China, now known as Operation Night Dragon. Wildly varying estimates suggest that such cybertheft costs the U.S. economy anywhere from $2 billion to $400 billion per year.

Beyond corporate secrets, political secrets are also targeted. Congressmen have been subject to infiltration and theft of information. So has the Pentagon, whose war strategies and technology plans were stolen.

Critical networks run U.S.

These incidents and the potential for more grievous attacks are why Congress has spent the past few months vigorously debating how to deal with cybersecurity – the set of issues centered on high-tech networks and national security. Indeed, many in Congress believe that the United States, of all nations, has the most to lose in a world of cyberconflicts.

As the world's most connected nation, the United States relies on electricity networks and those networks rely on computers. We rely on electronic networks for our financial transactions. Our air traffic control systems rely on computer networks. Our adversaries could kick the legs out from under our society by taking out these key, critical networks. In early March, the Obama administration presented senators with a simulated cyberattack crippling New York City's electric grid to demonstrate the possible economic and civilian damage.

The United States has the most to lose for another reason: Our conventional military enjoys superiority over enemy forces on land, sea and air. Far less expensive than investing in planes, aircraft carriers and intercontinental missiles, our enemies can invest in digital weapons that have the potential to change the game entirely and render moot our advantages.

Experts have debated whether the risk of cyberwar is real or merely an exaggerated threat. Some argue an exaggerated threat would serve to enrich defense contractors, to increase appropriations to particular agencies and military branches, and to sneak through rules limiting our freedoms online. But we must provide some common sense in thinking about a Pearl Harbor-like cyberattack – shutting down the nation's largest electricity grids would probably require the resources of a foreign government and would provoke a war with that government.

Real political considerations limit the likelihood of major cyberattacks, but even if the likelihood is low, the harm could be large. Failing to prepare for such a possibility would be like failing to prepare for an unlikely but devastating natural disaster. We have already experienced consistent network intrusions compromising intellectual property and national security plans. So arguments over whether the threat is exaggerated have somewhat receded, and we have moved on to more specific arguments.

Congress works on what to do

There is fairly widespread agreement in Congress that "something" should be done about cybersecurity. There is far less agreement, however, over what exactly should be done.

The White House has supported legislation proposed by Sen. Joe Lieberman, which empowers the Department of Homeland Security to adopt security standards for critical infrastructure networks, such as our power systems, transportation systems and communications networks. Republicans argue that the bill is "too regulatory" in imposing standards on industry. Led by Sen. John McCain, eight Republican senators have proposed competing legislation that would encourage sharing information about cyberthreats among private entities, including Internet service providers such as Comcast and AT&T, online providers such as Google and Amazon, and companies ranging from PG&E to Exxon. The bill would also encourage these private entities to share cyberthreat information with government agencies through incentives such as protection against lawsuits.

• The first disagreement concerns the role of private industry and ensuring innovation. Privately held communications networks happen to be our public's critical infrastructure. For example, private networks such as those controlled by Internet service providers – AT&T, Comcast and Verizon – carry 80 percent to 90 percent of all Internet traffic: government, military and private. Some believe the private companies do not have sufficient market incentives to protect that infrastructure and may skimp on investing in security. As a result, the Homeland Security should establish security standards.

Opponents argue that a company's networks and reputation are its most valuable assets, so companies have sufficient commercial incentive to invest in security. More importantly, they say, Homeland Security standards would make us less safe. Threats change daily and standards might be written for yesterday's threats. Standards may also result in a mentality of "checking the box" to meet a standard and avoid liability, rather than of actually meeting tomorrow's threats. At the same time, the White House argues that standards could be flexible and that any bill without some standard will have too limited an effect.

• The second disagreement concerns the role of intelligence agencies, military authorities and domestic law enforcement. Intelligence agencies, such as the National Security Agency, are supposed to gather intelligence on agents of foreign powers – spy vs. spy, not spy vs. American citizen. Military authorities also target foreign powers and have historically been subject to limitations in enforcing domestic law. Law enforcement, however, does investigate domestic crimes by American citizens – but under legal limitations meant to impede unrestricted fishing expeditions. These divisions turn generally on the location of a culprit and incident (here or abroad), the target (a military or industrial) and the person acting (foreign citizen, government or an American citizen).

For cybertheft and cyberattacks, these distinctions are less helpful. Someone sitting at a desk in China could cause damage in California. The culprit may be in China or Chicago, a hacker or foreign spy or foreign uniformed soldier; determining the culprit requires gathering specific information. Intelligence agencies and military authorities have particular expertise in this area, and many relevant intrusions originate abroad. But concerns abound that these outward-facing entities could be turned against American citizens – and used to gather information and build extensive dossiers on our digital lives.

• The third major disagreement focuses on civil liberties and privacy. Here, the disagreement is less between Republicans and Democrats. Rather, specific members of Congress have raised privacy concerns, and privacy and civil liberties organizations have been particularly vocal. As noted, Republicans emphasize encouraging information-sharing among private companies and with government agencies, and Democrats do not disagree on that point. But some private companies may share threat information with the government that law enforcement usually cannot access without a search warrant or some other legal order.

According to some readings of both the McCain and the Lieberman bills, this may include sensitive personal information or generally protected free speech in emails. Further, many civil liberties advocates argue that intelligence agencies and military branches should have a limited role in securing domestic networks, such as providing information and expertise to civilian authorities and the private sector, and not be able to extensively monitor private communications or gather information from private companies that the intelligence agencies ordinarily would need court orders to receive.

Sharing data is test of privacy

We would not, in theory, want government agencies such as the NSA, still distrusted by many for its warrantless wiretapping scandal, or FBI to monitor all our online activity that we engage in through personal or business computers. But, under the proposed legislation, they could potentially get such information through private parties.

ACLU legislative counsel Michelle Richardson, reacting to the introduction of McCain's bill, stated that parts of the bill permitting extensive sharing were "a privacy nightmare that will eventually result in the military substantially monitoring the domestic, civilian Internet." The Center for Democracy & Technology has raised the same concerns about the Lieberman bill, as that bill would permit the Homeland Security to designate a military agency to take the lead on cybersecurity.

At the same time, it may be better to adopt cybersecurity legislation now, rather than doing so in the wake of an attack where temporary hysteria results in legislation far less sensitive to our privacy.

Finally, concerning freedom of speech, the bills appear to provide entities legal immunity for engaging in "counter-measures" against cybersecurity threats. But policy advocates fear that this immunity may open a backdoor threat against network neutrality: companies like AT&T or Comcast could take counter-measures to block unpredicted traffic from popular peer-to-peer technologies, online video and sites that the record labels and studios consider "rogue" copyright-enablers.

Our goal is not to judge which side is right in these disagreements. Rather, we believe that these disagreements should be put before the American people. Critical networks such as the Internet, financial networks and electricity grids touch every part of our lives. Rules for strengthening our security will affect not only our security but also our ability to innovate and to enjoy the privacy and freedom of anonymous speech necessary in a democracy.

One way to increase our security is to raise the level of discourse, understanding and involvement of more Americans in this important debate. This can be accomplished in part by understanding different cyberthreats and understanding the potential threats to civil liberties. This would place policymakers and the public on a similar footing for discussing the issues. Doing so will also help to ensure that decisions about our economy and security are made as democratically as possible, in the open and not taken without adequate public discussion about the role of industry, the leadership of civilian authorities and the protection of civil liberties.

Marvin Ammori is an affiliate scholar at Stanford Law School's Center for Internet & Society. Ammori and Luke Pelican also represent technology companies on legal and public policy matters.