COUNCIL on FOREIGN RELATIONS

CFR PRESENTS

Net Politics

CFR experts investigate the impact of information and communication technologies on security, privacy, and international affairs.

Sanctioning Cyber Crime: The New Face of Deterrence

by **Guest Blogger**
May 19, 2015

Merchandise baskets are lined up outside a Target department store in Palm Coast, Florida on December 9, 2013. That year, Target announced it was the victim of a cyber incident that exposed the credit card details of up

*Zachary K. Goldman is the Executive Director of the **Center on Law and Security** at NYU School of Law. He formerly served in the Department of the Treasury's Office of Terrorism and Financial Intelligence and at the Department of Defense.*

With the new cybersecurity sanctions program adopted by the Obama administration last month, the U.S. government is finally beginning to develop the tools to deter financially-motivated cybercrime. With a price tag estimated at **$400 billion** per year, cyber-enabled theft imposes a substantial tax on American businesses. And while the U.S. government has focused on deterring attacks against **critical infrastructure**and on the **military dimensions of cyber deterrence**, financially motivated cyber crime is far more prevalent. In order to stem the kinds of digitally-facilitated crime that saps

to forty million customers. (Larry Downing/Courtesy Reuters).

American competitiveness, the Obama administration should focus on deterring financially-motivated cyber thieves by targeting what they value most: their money. The White House's new cybersecurity sanctions **program** provides the perfect framework to do so—if it's used correctly.

Deterrence is fundamentally about manipulating an adversary's cost/benefit calculations to dissuade him from doing something you want to prevent. Over the last several years, strategists have struggled to adapt venerable Cold War concepts like deterrence to the information age. But deterring financially-motivated cyber criminals—the kinds of people that attacked Target, **Anthem Health**, and many others—requires an approach tailored to hackers that seek to steal sensitive information that can be monetized quickly.

Many companies are also hacked because they hold commercially valuable intellectual property or trade secrets, the theft of which can provide competitive advantages to industry rivals. Indeed, last year the U.S. Department of Justice **indicted** five members of the Chinese military for stealing this type of information from leading American companies, **including** Westinghouse and U.S. Steel—data that would be useful to competitors in China, including state-owned enterprises. **Law firms, too**, have been subject to cyberattack because they hold valuable information about mergers, IPOs, and other corporate activities that can provide an advantage to a competitor (or a company on the other side of the negotiating table).

Companies or groups of hackers steal this information for commercial purposes. They do so for profit, and as such, are sensitive to the costs of their activities. Raise the costs high enough and they will move on to other targets or other activities. Criminals involved in cyber theft therefore have different motivations from state-sponsored actors that target the U.S. military or critical infrastructure. The motivations of cyber thieves also differ from those who engage in cyber espionage to steal government secrets, or "hacktivist" groups that commit acts of cyber vandalism to make a political point.

This is where the new sanctions program, inaugurated by the Obama Administration in April, comes in. The cybersecurity sanctions **program** in some respects resembles traditional sanctions programs. It freezes the assets of people designated for harming computer networks and posing a significant threat to U.S. national security, foreign policy, economic health, or financial stability.

But the sanctions program also contains an innovative provision that allows the government to impose sanctions on companies that are responsible for cyber crime, or who receive or use the proceeds of cybercrime for commercial advantage or private financial gain.

Using this authority, the U.S. government could target, for example, banks in Eastern Europe that function as the back office for cybercrime rings, moving and storing their ill-gotten gains. It could also sanction Chinese companies that receive stolen intellectual property and incorporate it into their products, disadvantaging their American or European competitors. Doing so will freeze targeted companies and individuals out of the international financial system, neutralizing the advantage they thought they procured by using stolen data or intellectual property.

In so doing, the program has the potential to dry up the market for information stolen by cyber means. If companies cannot make money by engaging in cyber theft, they are much less likely to do so. They will, in other words, be deterred.

There will be challenges to using the new sanctions in this way. For starters, the government must feel confident that it can control the potential for escalation, and mitigate the risk that U.S. companies operating abroad will be targeted in retaliation. It also must feel confident in its ability to attribute attacks, and to identify the beneficiaries of commercially-motivated cyber theft. But the first step is to recognize that deterring financially-motivated cyber crime is different from deterring other kinds of cyberattacks. And with the new cybersecurity sanctions program, the United States is beginning to develop and deploy a set of tools designed for the task.