DECEMBER
2014

George C. Marshall Institute Policy Outlook

Sony Attack Signifies New Twist in Cyber Conflict

Eric R. Sterner
Fellow, George C. Marshall Institute

Attacking another country's sources of economic power and its political and cultural cohesion is an old practice in warfare. The former was most clearly explored in the theories of strategic bombing that sprung up after the invention of the airplane in the first part of the twentieth century. The latter is considerably older; history is rife with stories of invading armies pulling down temples to local deities. Invariably, both kinds of attacks involved political actors at war. They were already killing one another on a large scale.

Cyberspace is rapidly changing that calculation. It has made these non-military sources of power vulnerable while giving adversaries new tools to use when attacking them. In doing so, they are bypassing a nation-state's defenses entirely to attack private actors. The United States government may well be helpless to prevent such attacks, failing in its first task of providing for the common defense.

Two recent cyber campaigns illustrate this new age of conflict's arrival and signal a new twist. First, the hacking campaign against Sony Pictures by the so-called Guardians of Peace has escalated from corporate espionage and public humiliation that undermined the company's value to threats of violence against third parties who either show or view its movie, "The Interview." Because the parody, which has not been publicly released, involves two celebrities nominally hired by the CIA in an attempt to assassinate North Korean leader Kim Jong Un, investigators suspect that The Guardians of Peace is really a front group for the North Korean government. The Guardians of Peace removed and deleted data, breaking servers in the process. Sony responded by cancelling the movie's premier and promotional tours, while quietly telling theater owners that it would not contest decisions not to show the movie. Enough of them pulled out so that Sony withdrew the movie from its scheduled Christmas release.

Second, Bloomberg news reports that hackers from Iran launched a campaign against the Las Vegas Sands Corporation in retaliation for an off-hand comment by the company's CEO and majority shareholder, Sheldon Adelson, about using nuclear weapons to sway Iran's negotiating position about its nuclear programs. The Iranian hackers destroyed servers, laptops, and desk computers throughout the company and left personally threatening messages for Adelson.

These attacks have several things in common. Shadowy groups carried them out and they nominally served the interests of two pariah states known to employ legions of hackers as a kind of unacknowledged militia. Both sought to do damage, not just steal information, and included personal information about company employees in their attacks. Unlike most corporate cyber attacks, which

1601 North Kent Street, Suite 802 • Arlington, VA 22209
Phone (571) 970-3180 • Email: info@marshall.org • Website: www.marshall.org

involve theft or espionage, these attacks also meant to hurt their targets' business prospects. More importantly, perhaps, they seem designed to punish their targets for expressing certain ideas, sending the message that certain public speech will result in punishment. After all, North Korea and Iran both engage in such practices at home.

Attacking the exercise of first amendment rights is not the only potential consequence of the attacks. In the Adelson case, they may reflect an attempt to influence domestic political processes in the United States for the purpose of strengthening Iran's hand in international negotiations about its nuclear program. Adelson, a strong supporter of Israel, is active in Republican politics and often supports those who take a hard line against Iran. It would be logical for an attacker to think it possible to neutralize his political involvement by attacking his business interests. At a minimum, it might dissuade others from adopting similar positions vis-à-vis Israel or Iran, lest they too become targets of overseas cyber attackers. (While Sony is not similarly engaged politically, the attackers may seek to dissuade others from similarly disparaging North Korea or its leader.)

These kinds of cyber campaigns differ from the usual fare. Criminal theft, as well as private- and state-sponsored espionage, are among the most frequent cyber attacks on private actors and draw considerable public attention. A recently released cyber threat report from the Internet security firm Sophos, for example, focuses on the evolution of criminal tactics and society's vulnerabilities. The security firm McAfee follows similar lines, with greater attention to espionage. Additionally, the threat of attacks on critical infrastructure has been a concern since analysts first started writing about cyber warfare in the early 1990s.

The cyber attacks on Sony and the Las Vegas Sands Corp., however, suggest a new twist in cyber conflict. They signify a shift to more politically motivated attacks from states directed at private actors. Their purpose is not just to steal money or secrets, but to suppress the expression of ideas and opinions, if not thinking them. (China has employed this kind of tactic against several countries, including South Korea, Japan, and the United States.) In the past, grass-roots hacktivists have pursued such attacks against corporations and states, but it has been more rare to see states employ them.

Washington is entirely unprepared to deal with this kind of threat to the fundamental liberties it is charged with protecting. Indeed, the Defense Department does not even envision itself in this role. It is primarily concerned with protecting its own networks, which has been the case under several presidents. Similarly, domestic law enforcement agencies cannot realistically reach states or their overseas agents when they launch such attacks. The Department of Homeland Security has the lead for protecting critical infrastructure, not protecting free speech. In short, the departments and agencies principally charged with protecting the country do not envision resisting this kind of attack as part of their key function. Private actors in the West may find themselves largely on their own when it comes to facing politically-motivated cyber attacks from foreign governments. Sony's decision to withdraw "The Interview" from its planned release signifies a victory for North Korea and these kinds of tactics.