THE WALL STREET JOURNAL.
WSJ.com

OPINION | Updated May 21, 2013, 7:19 p.m. ET

Steven Stalinsky: China Isn't the Only Source of Cyberattacks

The Syrian Electronic Army and other Middle Eastern hackers are targeting the U.S.—and succeeding.

By STEVEN STALINSKY

On Friday, the Financial Times became the latest victim of the Syrian Electronic Army when the pro-Assad group hijacked the newspaper's technology blog and its Twitter account. Since the hacker group emerged in 2011, it has attacked the Associated Press, the BBC, Al Jazeera, Harvard University and even Oprah Winfrey's Facebook page and the satirists at the Onion.

The next victim is anyone's guess. Unfortunately, it doesn't look like the U.S. government or cybersecurity agencies are equipped to root out this particular threat.

To be sure, Washington is well aware of the major threat that cyberwarfare generally poses to the country's security. At a March 12 Senate hearing, Director of National Intelligence James Clapper reviewed the Worldwide Threat Assessment of the U.S. intelligence community and put the cyberwarfare threat at the top of the agenda. "When it comes to the distinct threat areas, our statement this year leads with cyber . . . state and nonstate actors are gaining and using cyber expertise," he said.

Mr. Clapper went on to acknowledge that "some terrorist organizations have heightened interest in developing offensive cyber capabilities," but qualified that by saying: "They will probably be constrained by inherent resource and organizational limitations and competing priorities."

The truth is grimmer. Since Sept. 11, 2001, terrorist groups have shown much more than a "heightened interest in developing offensive cyber capabilities." They are actively engaged in attacks.

Speculation about and preventive measures against cyberattacks have focused almost entirely on China and Iran. So far, virtually no one has looked at the Arab and Islamic world in this context—despite the fact that for the past decade a considerable number of cyberattacks and threats against the U.S. and other Western countries have emanated from there.

Just days before 9/11, the Saudi newspaper Al-Riyadh published an interview with the Saudi hacker "Robin Hood," otherwise known as Abu Walid, who spoke of his "hobby" of targeting U.S. and Israeli websites. Walid claimed to have attacked the FBI and the Environmental Protection Agency, as well as a Defense Department network center from which he claims he obtained military data.

David Klein

Sometimes these hacks have clear real-world consequences. On April 23, when the Syrian Electronic Army tweeted from the AP's account that the White House had been attacked and President Obama wounded, the Dow plummeted 143 points. Over $136 billion was lost within three minutes of the false tweet. The market rebounded once the hoax was exposed.

Hamza Bendelladj, an Algerian, allegedly stole millions of dollars by hacking bank websites between 2009 and 2011. U.S. authorities believe that he hacked private accounts in more than 217 banks and financial companies world-wide, causing over $2 billion in damage. On May 7, he was extradited to the U.S. and is currently awaiting trial in Georgia.

If these hackers can't hurt the market or U.S. companies, at the very least they want to terrify people. Last month the shadowy underground groups Tunisian Cyber Army and al Qaeda Electronic Army announced via Twitter that they had hacked Pentagon, State Department and Department of Homeland Security websites as part of their #opBlackSummer campaign. The campaign, they promise, will include continuing attacks against U.S. government websites as well as websites connected to infrastructure, finance and the computer systems of U.S.-based airlines.

A large number of cyberattacks from the Middle East have directly followed fatwas issued by influential sheiks specifically supporting them. Many of these religious leaders are considered mainstream in their home countries and have sizable followings on Twitter, Facebook and YouTube. They sell their products including apps, books and DVDs on iTunes and Amazon. Ironically, their websites are hosted on U.S. servers.

For example, a major Salafist website is hosted in New Jersey. The site is owned by Sheik Abu Muhammad al-Maqdisi, once mentor to the late leader of al Qaeda in Iraq, Abu Musab al-Zarqawi, and now imprisoned in Jordan.

On Feb. 6, 2013, the site published a fatwa by the influential Mauritanian Sheik Abu Mundhir al-Shinqiti, which came in response to a user's question about the permissibility of hacking and using fraudulent credit card information on U.S. retail websites. The fatwa stated that since the citizens of "infidel" countries are legitimate targets, taking their property "is permissible."

The first known fatwa providing religious backing for such attacks and other forms of cyber-jihad was issued by Saudi Grand Mufti Sheik Abd al-Aziz Al-Sheikh and reported by a Saudi government magazine, Al-Dawa, in May 2000. The fatwa approved the use of viruses and other methods of online attacks.

Since then, according to my research, there have been over 50 significant fatwas addressing cyberwarfare. Among the most important: In August 2008, the Fatwa Committee of Al-Azhar University in Egypt—Sunni Islam's most influential body—issued a fatwa supporting the hacking and damaging of American and Israeli websites. Widely lauded by other sheiks, the fatwa is still being used to provide religious justification for cyberjihad.

In 2008, the popular Saudi preacher Salman al-Odah—he has 2.2 million Twitter followers and supervises Islamtoday.net—said in a fatwa posted on the Saudi Web forum brydah.com that "some professionals" could "provide support in hacking offensive [i.e., infidel] sites, which would be a positive act."

In June 2011, the leader of the Kuwaiti branch of the Muslim Brotherhood, Dr. Tareq al-Suwaidan, called for electronic jihad against Israel in a television interview. "I hope that a group of hackers will get together, and will wage resistance over the Internet, targeting Israeli and Zionist sites and destroying them electronically," he said. "I view this as better than 20 jihad operations."

These sheiks are just a few of the dozens of influential leaders who support cyberwarfare against the U.S. and its allies. But chances are that most security experts in the West have never heard any of these names—let alone know that there are regularly fatwas calling for cyberattacks.

In addition to the growing army of Islamist cyberwarriors, there is an even larger number of secular anti-West Arab and Muslim hacker groups that are associated with anarchists and hacker collectives, such as Anonymous, about which the West knows very little. If further damage to national security is to be prevented, the activities of these groups must be researched, monitored, translated and tracked so that they become a central part of today's cybersecurity debate.

Mr. Stalinsky is the executive director of the Middle East Media Research Institute.

A version of this article appeared May 22, 2013, on page A17 in the U.S. edition of The Wall Street Journal, with the headline: China Isn't the Only Source of Cyberattacks.