The Epoch Times

US-Iran Cyber Conflict Ties to Economic Warfare

Joshua Philipp January 29, 2013

Cyberattacks on U.S. banks have continued since September 2012, and are growing more sophisticated. U.S. Space Command announced it will add an additional 1,000 cybersecurity personnel to its current 6,000 staff. Janet Napolitano, the Secretary of Homeland Security, warned that a cyber 9/11 attack could happen at any time. Iran is the main culprit.

Fundamentally, the conflict with Iran is an economic war. “It clearly aligns with their public documents and announcements,” said Kevin Freeman, CEO of Cross Consulting and Services, and a leading expert on economic warfare and financial terrorism.

Freeman says the attacks go both ways. The Iranians are attacking American banks, while the U.S. is targeting Iranian finances through sanctions.

The conflict is nearly identical to Franklin D. Roosevelt’s use of economic war on Japan in the early stages of World War II, prior to the bombing of Pearl Harbor. It took the form of economic sanctions against Japan, starting with the U.S. ending the 1911 commercial treaty with japan, then with the July 2, 1940, signing of the Export Control Act that could prohibit the export of defense materials. Then, on Oct. 16, 1940, the U.S. put an embargo on all scrap iron and steel to any nation except Britain and those in the Western Hemisphere, and finally, on July 26, 1941, Roosevelt froze Japanese assets in the United States.

“The United States was the main supplier of the oil, steel, iron, and other commodities needed by the Japanese military as it became bogged down by Chinese resistance … it meant that the Roosevelt Administration could now restrict the flow of military supplies into Japan and use this as leverage to force Japan to halt its aggression in China,” states a post by the State Department’s Office of the Historian.

The difference now is that rather than helping guard China from Japan, the U.S. is helping guard Israel from Iran. The sanctions being used by the U.S. against Iran are similar, but rather than respond with a physical attack on the U.S., Iran is launching cyberattacks.

Existing sanctions against Iran mainly target individual firms with ties to Iran’s nuclear industry. The U.S. just rolled out new, much harsher sanctions, however, which directly affect Iran’s foreign trade and its key financial infrastructure by broadly targeting its energy, shipbuilding, and shipping sectors. The new sanctions were included in the U.S. defense bill for 2013.

An analysis from think tank CATO Institute states that while “the sanctions have failed to force Tehran to abandon its nuclear program,” the sanctions have “altered the modus operandi of finance and commerce in Iran and have also contributed to Iran’s inflation woes.”

The Iranian motive for using cyberattacks against U.S. banks can best be summed up by a recent statement from Iraqi diplomat Qais al-Azzawy who urged Arab states to “use the weapon of oil” to put pressure on the United States. He told reporters in Cairo in November 2012 that “The economic weapon is the strongest one to be put into effect now … in light of there being no military power that can stand in the face of Israel at the present time,” Fox News reported.

Cyberwar shares similar traits. It’s a form of warfare that can be used while avoiding a ground conflict, and that allows a nation to fight a war when it couldn’t win a troop-on-troop battle.

The Iranian cyberattacks, meanwhile, have lasted since September and have hit a very long list of banking websites including Bank of America, Wells Fargo, Citigroup Citibank, and PNC. The crackers are using a type of cyberattack known as a distributed denial of service (DDoS), which can overload a website with queries and take it offline.

Freeman said that while a DDoS attack “is a short-term problem,” the real risk is that crackers often use DDoS attacks to create a cover for more advanced attacks, or to monitor the protocol and response time of the target’s security staff.

Homeland Security Chief Janet Napolitano warned on Jan. 24 that a “cyber 9/11” could happen “imminently,” during a speech at the Wilson Center think tank in Washington. Defense Secretary Leon Panetta gave a similar warning in October 2012 of a possible “cyber-Pearl Harbor.”

Just prior to Napolitano’s statement, on Jan. 17, Air Force Space Command announced it would add 1,000 employees to its 6,000 cyber professionals under the 24th Air Force—a 15 percent increase while many other branches are cutting staff amid a tightening budget.

The 24th Air Force plays a broad, important role with cybersecurity and cyberwarfare. “I have the responsibility of major command headquarters but in terms of where the work really gets done to operate and defend Air Force networks, to provide exploitation capabilities and develop attack capabilities, that’s the 24th Air Force,” said Gen. William L. Shelton, according to the Pentagon’s American Forces Press Service.

Ties to Iran

While many news outlets reported that the U.S. government said Iran was behind the attacks, there has not yet been an official statement. Since the attacks began in September 2012, however, there have been several reports of officials speaking on condition of anonymity about Iran’s connection to the attacks.

There was also a document obtained by the FreeBeacon that was allegedly leaked from the Joint Chiefs of Staff’s intelligence directorate, and stated, “Iran’s cyber aggression should be viewed as a component, alongside efforts like support for terrorism, to the larger covert war Tehran is waging against the West.”

The group claiming responsibility (I, II) for the bank attacks is called the Martyr Izz ad-Din al-Qassam Cyber Fighters. They have launched attacks in the past, yet the recent attacks show an unlikely jump in skill. Back in September, the group was asking its followers online to use Low Orbit Ion Cannon, a free tool that launches DDoS attacks, but is only effective when large numbers of participants join in, and that also exposes the user’s private information. Low Orbit Ion Cannon is often used by hactivist groups like Anonymous Operations.

The types of DDoS attacks being used, however, are far beyond the capabilities of any known hactivist group, let alone Low Orbit Ion Cannon. The attacks are encrypted and also use a piece of malware, “Itsoknoproblembro,” to infect computers which are then used to help launch the DDoS attacks.

The Martyr Izz ad-Din al-Qassam Cyber Fighters stated in a Pastebin post that an offensive, low-budget film on YouTube, “Innocence of Muslims,” is the reason for their attacks. They claim they will continue the attacks until all the video links are removed, or until they feel they’ve compensated for the videos through the financial damage their attacks are causing.

The incident goes back prior to the attacks on U.S. banks, and ties to the cyber conflict between Iran and Israel. It started on Jan. 3, 2012, when a hacker going by “0xOmar” posted the credit card data of 400,000 Israelis.

It started a chain of back-and-forth cyberattacks between hackers in Israel, Iran, and Saudi Arabia. Hackers were releasing troves of credit card information belonging to ordinary citizens, at one point hackers shut down the websites of the Israeli and Saudi Arabian stock exchanges, and attacks were also launched on other sectors.

0xOmar claimed he was part of hacker group, “Group-XP,” which claimed to be the largest Wahhabi hacker group of Saudi Arabia, and claimed to be part of Anonymous Operations.

On Jan. 7, 2012, Israeli Deputy Foreign Minister Danny Ayalon announced that the cyberattacks would be treated as terrorism. Israel also announced its formation of the Cyber Warfare Administration on Jan. 13, 2012, which now coordinates cybersecurity efforts between the Israeli defense and security industries.

Noise around the incident caught the attention of terrorist organization Hamas, which proclaimed on Jan. 16, 2012, that hacking was a “new field of resistance.”

Despite individual crackers taking credit for the attacks, however, Iran was suspected to have played a role.

That’s the unfortunate nature of cyberwarfare, but it’s also what makes it such an enticing form of warfare for governments—it is nearly impossible to pin the attacks on a country, especially if the attacks are merely state-sponsored, instead of being state-run, and are launched in collaboration with a hacker group. The Chinese regime, for example, is known to launch state-sponsored attacks in coordination with patriot hacker groups like the Honker Union.

“They look like state sponsored attacks,” said Freeman, regarding the Iranian cyberattacks. “The Iranians certainly have the technical efficiency, and they have the resources. They have the motives, the means, and the opportunity.”