Why Iran Didn't Admit Stuxnet Was an Attack

By GARY D. BROWN

In July 2010, news broke that a new computer virus had been discovered. To casual observers, it probably elicited little more than a yawn. After all, there seems to be a new "cyber threat" reported every day. The detection of new computer viruses is announced routinely. In most cases, by the time the event is publicized, the major antivirus manufacturers have already developed a patch to address whatever software flaw the malware was designed to exploit.

To more experienced cyber players, however, this July 2010 event was far from routine. "Stuxnet," as the virus came to be known, was far more complex than run-of-the-mill hacker tools. The complicated and powerful code was a self-replicating worm that targeted programmable logic controllers (PLCs), the simple computers used to perform automated tasks in many industrial processes. PLCs are part of industrial control systems, most commonly referred to as Supervisory Control and Data Acquisition (SCADA) systems. SCADA systems are critical to the modern industrial world, controlling such things as water plants, auto manufacturing, and electrical powergrids.

Stuxnet could not spread directly through SCADA systems. It propagated over computers running the Windows operating system. From there, it searched for a certain computer-to-SCADA interface system. If the interface was present, Stuxnet was programmed to determine if it could target a PLC—but not just any PLC. Stuxnet singled out PLCs made by Siemens.[1]

The Stuxnet code showed up on computer systems around the world, where it parked on hard drives, remaining inert if it did not find what it was seeking. The numbers indicate it was aimed at Iran; nearly 60 percent of reported Stuxnet infections occurred on systems in Iran.[2] In fact, at least one system Stuxnet was programmed to target controlled centrifuges critical to the production of nuclear material. It appears that Iran's uranium enrichment facility at Natanz was the specific target.[3] After Stuxnet became public, Iranian officials issued a statement that the delay in the Bushehr nuclear power plant being operational was based on "technical reasons," but did not assert it was because of Stuxnet.[4] At a news conference, President Mahmoud Ahmadinejad stated that malicious software damaged the centrifuge facilities, although he did not specifically mention Stuxnet or Natanz.[5] The passive posture it took on Stuxnet indicates Iran concluded that a public statement that it had been the victim of a cyber attack would not have been in its best interest. This article examines some of the possible reasons why Iran may have drawn this conclusion.

Before Stuxnet, the most notable actions in cyber were probably the events in the

Colonel Gary D. Brown, USAF, is currently serving as the senior legal advisor in U.S. Cyber Command.

Republic of Georgia and in Estonia. Neither rose to the level of a cyber attack. In Georgia, distributed denial-of-service (DDoS) assaults on government Web pages began in about mid-July 2008. Three weeks later, the assaults significantly increased and were accompanied by the Russian military crossing the border into South Ossetia, a Georgian province.[6] Ultimately, the conflict resulted in over 1,000 casualties and tens of thousands of displaced civilians. The cyber portion of the armed conflict in Georgia did not meet the common definition of an attack and, in any event, paled beside the destruction and death resulting from the invasion.

The situation in Estonia in 2007 was different in that it was not accompanied by a kinetic event. After the Estonian government relocated a World War II–era Soviet statue from the center of Tallinn to a military cemetery, Russian "hacktivists" (hackers motivated by patriotism or ideology) began to launch denial-of-service and DDoS actions against Estonian Web sites. Ultimately, the activity resulted in making government, banking, and many other commercial Web sites unavailable to Estonians.[7] Estonia contacted the North Atlantic Treaty Organization (NATO) to ask for support, but was rebuffed. There was agreement that, as serious as the cyber action was, it did not qualify as a cyber attack.

The Estonian experience led to the conclusion that NATO simply does not consider cyber action worthy of being called an attack. For NATO, an attack would trigger a potential self-defense response by the Alliance. "Not a single NATO defence minister would define cyber-attack as a clear military action at present."[8] However, NATO's position on aggressive cyber activities may be changing.[9]

There were initial indications after the discovery of Stuxnet that Iran might state the obvious. In the immediate aftermath of the Stuxnet event, an Iranian official indicated Iran had come under "cyber attack," but he was quickly silenced. Since then, there has been no further indication of how the event would be characterized in Iran.

Although there is no formally agreed-upon definition of cyber attack, most scholars would define it in a manner similar to a more traditional, physical attack. A common definition of cyber attack is "a cyber operation which is reasonably expected to cause death or injury to persons or damage or destruction to objects."

The Stuxnet event was as clearly a cyber attack as any publicly announced event to date. Intentionally designed malware directed against a nation-state resulted in the physical destruction of state-owned equipment.[10] The centrifuges were destroyed as effectively as if someone had taken a hammer to them,[11] and these were not just random bits of equipment. The destroyed centrifuges were a critical component of Iran's nuclear ambitions.[12] Whether the rest of the world likes it or not, Iran is working toward an independent nuclear capability. Another nation interfering with that clearly infringes on Iranian sovereignty. That means that not only was Iran attacked, but also the attack resulted in injury to a significant aspect of government policy.

Iran's "non-position" on the Stuxnet event has been frustrating to practitioners in the field of cyberspace operations. Finally, there was a well-documented, unambiguous cyber attack to dissect! And yet there was little official discussion of the issue because Iran passed up its opportunity to complain of an unjustified attack.

It is unusual that a nation would be attacked and not be willing to state as much. The community of nations (for example, the United Nations, the Arab League, or some other international organization) may be reluctant to tell a nation it has been attacked when it apparently feels otherwise. After all, if a nation does not feel it has been wronged, it is not really within the purview of the international community to try and convince it otherwise. This unusual situation is perhaps unique to cyber. It is difficult to interpret artillery bombardments or invasions by troops as anything other than attacks. However, in the cyber arena, there is a danger to the international community in this benign neglect.

The problem with turning a blind eye to the event is that, not only was Stuxnet an attack, it also was quite possibly an illegal attack under international law. In addition to violating the general prohibition against a use of force against another nation, this event arguably violated the law of war. The law of war requires that attacks be discriminatory, meaning they must be directed against military objectives only. Stuxnet was a self-replicating worm. It contained certain controls, but demonstrably not enough to prevent it from inserting itself into civilian systems around the world.

Iranian Motivations

What would motivate Iran not to just admit it was attacked? As the victim of an attack, it could possibly have gained support from the international community. At a minimum, it might have hoped for statements of condemnation to dissuade future similar attacks against it.

Discussed below are several reasons Iran might have chosen not to declare Stuxnet an attack. Although I have no insight into why Iran chose this course of action, I discuss the possibilities basically in order of probability, starting with the most probable.

Embarrassment. It is possible Tehran is simply ashamed that it lost a significant portion of its hard-obtained ability to create nuclear weapons material to a computer bug, especially when it portrays itself as having a significant cyber capability of its own.[13] Furthermore, to make things worse, the most commonly suggested perpetrator of the event was Iran's archenemy, Israel.

whether the rest of the world likes it or not, Iran is working toward an independent nuclear capability

A video screened at the retirement party for the head of the Israel Defense Forces indicated at least some level of involvement by Israel in the cyber attack on Iran's nuclear program: "The video of Lieutenant General Gabi Ashkenazi's operational successes included references to Stuxnet, a computer virus that disrupted the Natanz nuclear enrichment site [in 2010]."[14]

Irrelevance. Iran may have felt that its complaints would not be taken seriously since it is already on the outs with the international community over its nuclear program: "The United Kingdom and many other countries have serious concerns about the Iranian Government's policies: its failure to address serious international concerns about its nuclear programme; its support for terrorism and promotion of instability in its region;

and its continued denial of the human rights to which its own people aspire and which Iran has made international commitments to protect."[15]

According to an article in the *New York Times*, "The United Nations Security Council leveled its fourth round of sanctions against Iran's nuclear program on Wednesday, but the measures did little to overcome widespread doubts that they—or even the additional steps pledged by American and European officials—would accomplish the Council's longstanding goal: halting Iran's production of nuclear fuel."[16]

this event arguably violated the law of war

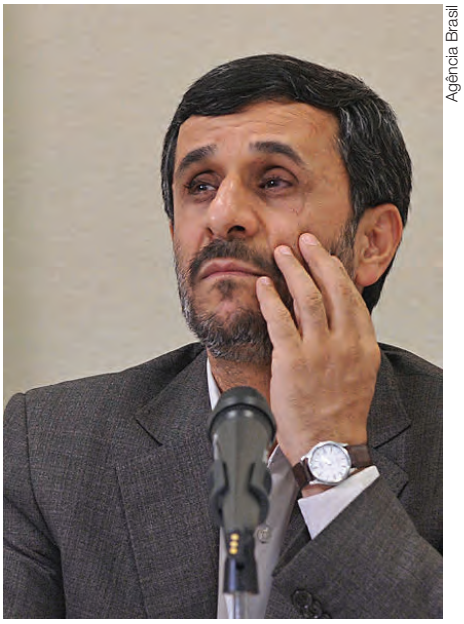
Besides, even if Iran had been able to convince the United Nations it ought to take action, the chances are slim that any action against, or even condemnation of, Israel would survive a journey through the Security Council.

Preserving Future Options. Iran cannot hope to compete in the traditional military sphere with the West, so it is apparently attempting to level the playing field by developing a nuclear capacity. Similarly, it may be hoping to develop an asymmetric cyber attack ability for the same reason. There are reports this is the case.

General Ali Fazli, acting commander of the Basij, was quoted by Iran's state-owned newspaper as saying Iran's cyber army is made up of university teachers, students, and clerics. He said its attacks were retaliation for similar attacks on Iran, according to the semi-official Mehr news agency. There were no further details about the possible targets or the time of the attacks:

Iranian hackers working for the powerful Revolutionary Guard's paramilitary Basij group have launched attacks on websites of the "enemies," a state-owned newspaper reported Monday in a rare acknowledgment from Iran that it's involved in cyber warfare. . . . "As there are cyber attacks on us, so is our cyber army of the Basij, which includes university instructors and students, as well as clerics, attacking websites of the enemy," Fazli said. "Without resorting to the power of the Basij, we would not have been able to monitor and confront our enemies."[17]

A similar consideration might just be called "unclean hands." If a country is up to anything it should not be doing, its government might not feel it prudent to complain when the cookie jar lid pinches its fingers. For example, an alleged Soviet pipeline explosion reported in the early 1980s may have qualified as a cyber attack—but one that was possible only because the Soviets had stolen infected pipeline management software from Canada.[18] As a result, even if the Soviet Union realized it had been "victimized," it may not have been inclined to complain.



Agência Brasil

Iranian President Mahmoud Ahmadinejad claimed Stuxnet virus did not affect nuclear operations

Belief the Action Was Legal. Although most legal experts would conclude that an offensive cyber action resulting in the physical destruction of property is an attack, there is no definitive evidence on the topic. We have little insight into what Iran believes is the state of play on cyber legality. From the inaction of the community of nations, we can infer there are no international restrictions on purely cyber activities. Moreover, other than the legally unchallenged Stuxnet, there is no indication that it is lawful to actually destroy things in another country—even if the destruction is caused by a purely cyber event.

Difficulty of Attribution. It is the nature of cyberspace and the Internet that makes it challenging to find out who is responsible for any given action. Appropriated computers, intermediate hop points, and many other techniques make it tough to know the origin of an activity, much less the originating actor.

In this case, although Iran may feel there are some obvious suspects, they may not be able to prove who was behind Stuxnet. One example of how the Internet has created new challenges in attribution is the rise of independent actors on many levels. Cyber techniques now allow anonymous coordination between actors, so action can be more effective and devastating, but the risk of discovery is smaller.

Of particular note are the hacktivists, who began to garner notice in 2007 with events in Estonia, followed by other significant activity in Lithuania and Georgia the following year. In a wonderful example of blurring the line between state policy and independent criminal actors, a group known as StopGeorgia facilitated the cyber assault on Georgia. This group of nationalistic hackers provided DDoS kits to novice hackers, along with lists of Georgian targets. They also offered more sophisticated malware, complete with instructions on how to employ it. These services were available to anyone who went to the group's Web site.[19]

Not all hacktivists are Russian, however. The Web site WikiLeaks accepts and publishes sensitive information "leaked" to it by members of the public. After the site published classified documents that had been stolen from the U.S. Government, many private companies in the United States took steps in an attempt to make WikiLeaks less effective. Most of the actions were taken by financial companies that refused to process payments for WikiLeaks.[20] As a result of the financial companies' actions, the loosely affiliated hacker group Anonymous responded by freely distributing downloadable malware with instructions on how to use it to harm the targeted companies.

The activity reported to have been taken by Anonymous hacktivists did not result in physical damage to computers. Even if it had, however, it may not have made sense to treat the action as a cyber "attack" because the perpetrators were individual civilians, acting only under suggestion from a higher organization. Because it is often impossible to know the individuals behind a nefarious cyber action, at least in real time, some countries are more comfortable treating all cyber events as criminal cases rather than potential acts of war. This may be how Estonia viewed the action against it in 2007: "It was clear to the Estonian

authorities that the cyber attacks could—and should—be treated as cyber crime."[21] On the other hand, even Estonia might see things differently if the "cyber attack" were destructive—like Stuxnet—rather than a denial-of-service attack or something similar.

As a subset of this rationale, in the bizarre world of international intrigue, it is possible (although it has not been widely suggested) that Iran itself concocted the Stuxnet scheme to make it appear a victim of Western powers, while at the same time providing an excuse for delays in its nuclear program. This theory is purely speculative, and no evidence is offered to support it.

In addition to the rationales discussed above, there are several that do not seem to apply to Iran's motivation in this case. Even if they are not relevant in the case of Stuxnet, however, they are interesting in the larger sense of cyber operations.

Fear. In theory, a country could be afraid of the reaction of the adversary to being called out. A cyber adversary might suddenly decide more aggressive options were in order if they were caught in the act. However, the circumstances here make it unlikely that fear played a role in Iran's decision.

Deception. It is possible the victim of a cyber attack may want to keep its detection of the attack a secret. The offended nation may want to gather intelligence on adversary tactics, for example. This constraint would probably disappear once the attack becomes public, however.

Overcome by Events. If a cyber attack occurs in the context of kinetic activities, it may not merit mention. This is similar to the situation that occurred in Georgia. With bombs falling and tanks rolling, cyber disruption did not merit much attention—although that case did not rise to the level of cyber attack. This is also what happened when Israel reportedly used cyber techniques to take down air defenses in Syria before an air raid that destroyed a military construction site in 2007.[22] The cyber event may have been an "attack," but when it is done in conjunction with falling bombs, it gets lost in the cognitive debris.

In the end, it probably does not matter in this specific case that Iran did not officially declare it had been attacked. Although there are reasons as detailed above to conclude that Israel was behind Stuxnet, it is doubtful the international community would have found enough evidence to establish conclusively that Israel was responsible. Even if it had, no effective action was likely to survive contact with the United Nations Security Council.

It is unfortunate that the clearest example of cyber attack appears to have passed by without a conclusive determination, which could have been driven by a statement from the victim country. Stuxnet may now fade into the sunset like so many other offensive actions that were famous in their day—Titan Rain, Moonlight Maze, Operation Aurora.[23] It looks to become just another uncategorized cyber action, and we may have missed our best opportunity to begin setting out boundaries for illegal behavior in cyberspace.

So far, the customary practice of nations in cyberspace seems to be, "Do unto others whatever you can get away with." Sadly, until a major player like the United States suffers a catastrophic cyber event, it appears likely to stay that way. **JFQ**

NOTES

[1] Seán P. McGurk, Department of Homeland Security, statement before the U.S. Homeland Security and Governmental Affairs Committee, Washington, DC, November 17, 2010.

[2] Michael Joseph Gross, "Stuxnet Worm: A Declaration of Cyber-War," *Vanity Fair* (April 2011); Symantec, "W32.Stuxnet," September 17, 2010, available at <www.symantec.com/security_response/writeup.jsp?docid=2010-071400-3123-99>.

[3] Yossi Melman, "Computer virus in Iran actually targeted larger nuclear facility," *Haaretz.com*, September 28, 2010, available at <www.haaretz.com/print-edition/news/computer-virus-in-iran-actually-targeted-larger-nuclear-facility-1.316052>.

[4] See Ministry of Foreign Affairs, Islamic Republic of Iran, weekly briefing, October 5, 2010, available at <www.mfa.gov.ir/cms/cms/Tehran/en/NEW/137891.html>.

[5] Mark Clayton, "Stuxnet: Ahmadinejad Admits Cyberweapon Hit Iran Nuclear Program," *Christian Science Monitor*, November 30, 2010, available at <www.csmonitor.com/USA/2010/130/Stuxnet-Ahmadinejad-admits-cyberweapon-hit-Iran-nuclear-program>.

[6] Stephen W. Korns and Joshua E. Kastenberg, "Georgia's Cyber Left Hook," *Parameters* (Winter 2008), 60.

[7] Eneken Tikk, Kadri Kaska, and Liis Vihul, *International Cyber Incidents* (Tallinn, Estonia: Cooperative Cyber Defence Centre of Excellence, 2010), 33.

[8] Ibid., 26n106.

[9] "Defence Ministers Approve Cyber Defence Concept and Take Next Step in Defence Reform," March 10, 2011, available at <www.nato.int/cps/en/natolive/news_71432.htm?selectedLocale=en>.

[10] Sharon Weinberger, "Is This the Start of Cyberwar?" *Nature*, June 9, 2011, 142.

[11] Ibid., 143. Also see Jeffrey Carr, "What Is Cyberwar?" August 12, 2011, available at <www.slate.com/id/2301253/>.

[12] Gross.

[13] "Commander Stresses Iran's Capability to Repel Cyber Attacks," July 8, 2011, available at <www.azadnegar.com/article/commander-stresses-irans-capability-repel-cyber-attacks>.

[14] Christopher Williams, "Israeli Security Chief Celebrates Stuxnet Cyber Attack," *The Telegraph*, February 16, 2011, available at <www.telegraph.co.uk/technology/news/8326274/Israeli-security-chief-celebrates-Stuxnet-cyber-attack.html>.

[15] UK Foreign and Commonwealth Office, "Britain's Relations with Iran," available at <www.fco.gov.uk/en/global-issues/mena/017-iran/>.

[16] Neil MacFarquhar, "U.N. Approves New Sanctions to Deter Iran," *The New York Times*, June 9, 2010.

[17] Nasser Karimi, "Iran's Paramilitary Launches Cyber Attack," Associated Press, March 14, 2011.

[18] Richard A. Clarke, *Cyber War: The Next Threat to National Security and What to Do About It* (New York: Ecco/HarperCollins, 2010), 93.

[19] The group's Web site was available at <www.stopgeorgia.ru>. Jeffrey Carr, "The Rise of the Non-State Hacker," *Inside Cyber Warfare* (2010), 15.

[20] Fahmida Y. Rashid, "PayPal, PostFinance Hit by DoS Attacks, Counter-Attack in Progress," December 6, 2010, available at <www.eweek.com/c/a/Security/PayPal-PostFinance-Hit-by-DoS-Attacks-CounterAttack-in-Progress-860335/>.

[21] Tikk, Kaska, and Vihul, 25.

[22] David Eshel, "Cyber-Attack Deploys in Israeli Forces," September 15, 2010, available at <www.aviationweek.com/aw/generic/story_channel.jsp?channel=defense&id=news/dti/2010/09/01/DT_09_01_2010_p42-248207.xml>.

[23] Kevin Hall, "The 7 worst cyberattacks in history (that we know about)," September 22, 2010, available at <http://dvice.com/archives/2010/09/7-of-the-most-d.php>; "A New Approach to China," January 12, 2010, available at <http://googleblog.blogspot.com/2010/01/new-approach-to-china.html>.