Defense One

Cyberwar on Iran Won't Work. Here's Why.

A renewed campaign of covert network attacks is more likely to spur Tehran's nuclear efforts than hinder them.

John Glaser

August 21, 2017

The Iran nuclear deal is increasingly at risk, with President Trump threatening to overrule his top national security advisers and defy the assessment of international monitors to declare Iran non-compliant with the agreement's stipulations. The problem for the administration, however, is that no viable alternative is better than the Joint Comprehensive Plan of Action. If Trump rips up the JCPOA, the U.S. would forfeit the stringent limitations placed on Iran's enrichment activities and the international community would lose the unprecedented transparency it now has on Iran's nuclear program. Even more daunting, the United States would become isolated in its approach to Iran, opposed by Europe, Russia, China, and much of the rest of the world.

Perhaps a more realistic concern is the prospect that the administration will nominally uphold the deal, while engaging in aggressive covert action against Iran. Increasingly, when traditional military and diplomatic options appear too costly, states turn to cyber warfare. But a stepped-up cyber offensive against Iran is very unlikely to yield desirable results. Not only is it unlikely to be effective in its immediate objectives, but it risks antagonizing Iran into precisely the kinds of behavior the hawks want to forestall.

Cyber-attacks fall into two basic categories: Computer Network Exploitation and Computer Network Attack. CNE essentially equates to espionage. It is simply the newest method of engaging in one of the oldest activities of states: snooping on enemies. CNA, on the other hand, is the practice of attacking foreign systems or infrastructure in order to destroy or incapacitate enemy networks.

When cyber weapons complement the use of conventional power, as when Israel employed a CNA to incapacitate Syrian air defense systems before it bombed a suspected nuclear enrichment facility in 2007, their tactical utility can be quite high.

However, cyber power is not very effective as an independent tool of coercion. Successful coercion requires the targeted state to know both the identity of the attacker and the attacker's intended message. This is often difficult in cyberspace because the identity of the attacker is frequently obscured and because isolated cyber-attacks don't clearly communicate intended messages, making the target's compliance unlikely.

Other factors also undermine the utility of CNA operations. Collateral damage and spillover effects are frequently unavoidable, for example. Cyber weapons are also effectively single-use tools of foreign policy because a targeted adversary can generally diagnose and patch whatever vulnerability allowed the attack. As well, CNA weapons carry a high probability of blowback. Targeted states can reverse-engineer the malicious code, replicate it, and then use it themselves. This only increases the likelihood that adversaries will respond to a cyber-attack, not with capitulation, but with defiance or counter-attack.

The Stuxnet virus is often held up as a fantastic success. As part of a larger U.S.-Israeli effort to sabotage Iran's nuclear facilities, Stuxnet is probably the most sophisticated, complex, and powerful cyber weapon ever used. According to *Wired* magazine, Stuxnet "was unlike any other virus or worm that came before. Rather than simply hijacking targeted computers or stealing information from them, it escaped the digital realm to wreak physical destruction on equipment the computers controlled."

Initial estimates exaggerated the damage caused by Stuxnet, claiming it set back the Iranian nuclear program by three to five years. Later assessments said the computer worm damaged only about 980 centrifuges (at the time, one-fifth of the total at the Natanz plant), and delayed Iran's overall nuclear program by a matter of months. The International Atomic Energy Agency (IAEA) reported that, during Stuxnet's attack window in 2009 to 2010, Iran actually increased the number of operating centrifuges, and increased production of low-enriched uranium from 80 kilograms per month to 120 kilograms per month. This suggests that Iran was spurred to boost production in the face of cyber-attacks.

In the aftermath of Stuxnet, and indeed right up until the November 2013 Joint Plan of Action interim agreement in which Iran agreed to temporarily freeze portions of the nuclear program as negotiations with the P5+1 continued, Iran's number of operating centrifuges and stockpile of enriched uranium continued to grow. From 2008 to 2013, Iran's stockpile of low-enriched uranium grew from 839 kilograms to 8,271 kilograms, almost a ten-fold increase.

"At best," according to the University of Toronto's Jon Lindsay, "Stuxnet thus produced only a temporary slow-down in the enrichment rate itself." Other experts are even more skeptical. Ivanka Barzashka, Research Associate at King's College London and a Fellow at Stanford, argues that "evidence of the worm's impact is circumstantial and inconclusive." Brandon Valeriano and Ryan Maness, in their book *Cyber War Versus Cyber Realities* contend, "It is wholly unclear if the Stuxnet worm actually had a significant impact on Iran."

The broader diplomatic picture adds weight to these skeptical analyses. To the extent that Stuxnet's objective was to delay enrichment production and coerce Iran to make more dramatic concessions in diplomatic negotiations than it otherwise would have, it seems to have failed. Indeed, Iran had demonstrated a willingness to engage in pragmatic diplomacy with the United States and make concessions on its nuclear program long before Stuxnet.

In a secret diplomatic overture sent to the Bush administration through the Swiss embassy in 2003, Iran offered to open up the their nuclear program to intrusive international inspections and to sign the Additional Protocol of the Non-Proliferation Treaty in exchange for an end to America's hostile policy toward Iran. At the time, they had only 164 operating centrifuges, compared to the 5,060 they got under the JCPOA.

And again in 2010, after lower-level negotiations with the United States on an interim agreement stalled, Iran, with help from Turkish and Brazilian negotiators, agreed to the benchmarks of an Obama administration proposal to ship out Iran's low-enriched uranium to a third-party country to satiate concerns about weaponization. Though this coincided with the period of the Stuxnet attack, the virus was not revealed as such until months later and there is no indication the damaged centrifuges actually motivated Iran to agree to the fuel swap.

Iran's willingness to make concessions in return for American accommodation makes the utility of Stuxnet seem dubious. According to Trita Parsi, the president of the National Iranian American Council who has interviewed Iranian officials on the issue at length, Iran was deliberately doubling down on its nuclear program in order to show the West that the coercive approach would not work in the absence of diplomatic concessions.

In addition to the meager, even counterproductive, impact of Stuxnet on Iran's nuclear program, the unprecedented cyber-attack wrought other negative consequences. First, it had notable spillover effects. Though the Stuxnet worm was designed not to "propagate beyond Iranian nuclear centrifuges…it infected over 100,000 computers worldwide before it could be stopped," according to West Point scholars Erica D. Borghard and Shawn W. Lonergan.

Second, Stuxnet drew blowback: it motivated Iran to launch multiple waves of cyber-attacks against American banks and Saudi Arabia's Aramco oil company. Then-Defense Secretary Leon Panetta, in a hyperbole typical of official statements on cyber security, said Iran's retaliatory cyber-attacks were "probably the most destructive attack the private sector has seen to date."

The Trump administration has limited options on its Iran policy outside of the JCPOA. Whether or not the president makes good on his threats to effectively abrogate the deal, one thing is for sure: a renewed covert cyber war is unlikely to produce any benefits worth the trouble. Such an approach will only antagonize Iran and boost the regime's motivation to once again pursue a nuclear weapons capability in earnest.

John Glaser is Associate Director of Foreign Policy Studies at the Cato Institute.