Opinion

Why Iran would avoid a major cyberwar

By **Jan Kallberg**

Jan 17, 2020

What's in it for Iran to launch a massive cyber engagement against the free world? What can they win and what would their regime lose? (photoman/Getty Images)

Demonstrations in Iran last year and signs of the regime’s demise raise a question: What would the strategic outcome be of a massive cyber engagement with a foreign country or alliance?

Authoritarian regimes traditionally put survival first. Those who do not prioritize regime survival tend to collapse. Authoritarian regimes are always vulnerable because they are illegitimate. There will always be loyalists that benefit from the system, but for a significant part of people, the regime is not legit. The regime only exists because they suppress popular will and use force against any opposition.

In 2016, I wrote an article in the Cyber Defense Review titled "Strategic Cyberwar Theory - A Foundation for Designing Decisive Strategic Cyber Operations." The utility of strategic cyberwar is linked to the institutional stability of the targeted state. If a nation is destabilized, it can be subdued to foreign will and the ability for the current regime to execute their strategy is evaporated due to loss of internal authority and ability. The theory's predictive power is most potent when applied to target theocracies, authoritarian regimes, and dysfunctional experimental democracies because the common tenet is weak institutions.

Fully functional democracies, on the other hand, have a definite advantage because these advanced democracies have stability and, by their citizenry, accepted institutions. Nations openly adversarial to democracies are in most cases, totalitarian states that are close to entropy. The reason why these totalitarian states are under their current regime is the suppression of the popular will. Any removal of the pillars of repression, by destabilizing the regime design and institutions that make it functional, will release the popular will.

A destabilized — and possibly imploding — Iranian regime is a more tangible threat to the ruling theocratic elite than any military systems being hacked in a cyber interchange. Dictators fear the wrath of the masses. Strategic cyberwar theory seeks to look beyond the actual digital interchange, the cyber tactics, and instead create a predictive power of how a decisive cyber conflict should be conducted in pursuit of national strategic goals.

The Iranian military apparatus is a mix of traditional military defense, crowd control, political suppression, and show of force for generating artificial internal authority in the country. If command and control evaporate in the military apparatus, it also removes the ability to control the population to the degree the Iranian regime have been able until now to do. In that light, what is in it for Iran to launch a massive cyber engagement against the free world? What can they win?

If the free world uses its cyber abilities, it is far more likely that Iran itself gets destabilized and falls into entropy and chaos, which could lead to lead to major domestic bloodshed when the victims of 40 years of violent suppression decide the fate of their oppressors. It would not be the intent of the free world, it is just an outfall of the way the Iranian totalitarian regime has acted toward their own people. The risks for the Iranians are far more significant than the potential upside of being able to inflict damage on the free world.

That doesn't mean Iranians would not try to hack systems in foreign countries they consider adversarial. Because of the Iranian regime's constant need to feed their internal propaganda machinery with "victories," that is more likely to take place on a smaller scale and will likely be uncoordinated low-level attacks seeking to exploit opportunities they come across. In my view, far more dangerous are non-Iranian advanced nation-state cyber actors that impersonate being Iranian hackers trying to make aggressive preplanned attacks under cover of spoofed identity and transferring the blame fueled by recent tensions.

Iran has, in my opinion, no logical strategic incentive to engage in a major strategic cyber conflict with the free world because the Iranians would risk more than they could gain.

Jan Kallberg is a research scientist at the Army Cyber Institute at West Point and an assistant professor at the U.S. Military Academy. The views expressed are those of the author and do not reflect the official policy or position of the Army Cyber Institute at West Point, the U.S. Military Academy, Department of Defense or the U.S. Government.

Share: