INSS Insight No. 1191, July 10, 2019

The US Cyberattack on Iran: The Campaign-Level and Strategic Dimensions

Ron Tira

The international media reported that the United States conducted a cyberattack on command and control computers belonging to Iran's air defense and surface-to-surface missile apparatuses. The working premise of this essay is that these reports are factually correct. The United States decision not to retaliate against Iran for the downing of the UAV with a kinetic attack, and its choice instead of a standalone cyberattack, i.e., absent synergy with complementary kinetic steps, further entrenches the US posturing as an actor deterred by risks and costs. In this sense, it may well be that the downside of the cyberattack outweighs it benefits. While it does illustrate capabilities, it also helps cement the United States positioning – in Iran's eyes and its own – as a risk-averse actor.

The international media reported that the United States conducted a cyberattack on command and control computers belonging to Iran's air defense and surface-to-surface missile apparatuses. The working premise of this essay is that these reports are factually correct.

The Particular Context

Since withdrawing from the nuclear deal (JCPOA), the United States has tightened the pressure on Iran – mostly in the form of the gradual reinstitution of economic sanctions – designed to lead to negotiations over a new, improved agreement, without reaching military confrontation. For its part, Iran is trying to skirt the United States pressure, or at least gain enough cards to allow it reach a consensual outcome from the current dynamics rather than an externally coerced outcome. Iran seeks – or at least sought – to defer the moment of truth until the United States reaches the election year (it may be that President Trump's scope for maneuvering and appetite for risk will ebb then, and it may be that by the end of the election year a new president will enter the White House) or to create a situation in which Iran's interests are taken into account and not overridden by the US economic pressure.

To do so, Iran has tried to create deterrence by demonstrating its capabilities to harm the interests of the United States and its allies, as well as its willingness to make use of those capabilities while inching toward the brink of a violent crisis. Therefore, Iran put on a

display of its capabilities and willingness to disrupt maritime traffic in the Strait of Hormuz. Moreover, because the Saudis have in recent years built an overland oil-pipe network connecting the Gulf with the Red Sea, bypassing the Strait of Hormuz, it was important for Iran to demonstrate its capabilities to attack the said land-based infrastructure, possibly from both Iraqi and Yemenite soil. Iran's willingness to push the envelope and take risks that might cross a line reached a new height with the downing of the US UAV on June 19, 2019.

The United States was ready to "retaliate" for the downed drone by means of a kinetic attack, though the word "retaliation" in this context is inaccurate, as it is difficult to define a strategic rationale of "retaliation." The strategic rationale seems to have been both to set limits for Iran, thereby shaping rules of the game in the Gulf that the United States can tolerate, and to demonstrate to Iran that the United States too is willing to cross the line separating force application from force projection. However, the United States changed its mind about using kinetic force, reportedly opting instead to demonstrate its ability to conduct a cyberattack against Iran's air defense and surface-to-surface apparatuses.

A Standalone Cyberattack: The Campaign-Level Dimension

The effectiveness of cyberattacks against the computer systems of Iran's air defense and surface-to-surface missiles apparatuses, without resorting concurrently to additional lines of operation, might be limited, because within a relatively short time (days or weeks) the Iranians may be able to identify and root out the malware, and have the targeted systems up and running again.

A cyberattack against such systems is effective primarily if it is a preparatory action to an ensuing kinetic attack against the same systems, or if it is designed to provide freedom for some other conventional line of operation. For example, a cyberattack against air defense systems can facilitate a kinetic attack against them or gain the freedom to enter the airspace usually protected by these systems for a limited amount of time. It is effective to attack with cyber command and control networks when one intends to carry out an immediate kinetic offensive against the apparatuses these networks command and control. In other words, it is more effective to use cyberattacks in synergy with conventional military lines of operation.

With the exception of instances in which cyberattacks can lead to physical destruction of equipment (and there have been no reports that this was the case here), standalone cyberattacks that are not part of a larger campaign might not achieve lasting results, and might prematurely expose capabilities – both in terms of the cyber access to the targeted systems (the attack vector) and in terms of the cyber weapon (APT). To date, the

exposure of cyberattack capabilities against weapon systems was marginal. Potential opponents are not necessarily familiar with the possible attack vectors and existing malwares, and therefore their exposure might be disadvantageous. The Iranian learning curve could thus become steeper, and Iran might gain a certain advantage in the learning competition.

Cyberattacks: The Strategic Dimension

The cyberattack allowed the United States to demonstrate its capabilities to Iran, thus contributing to US deterrence, as well as expand the range of pressure applied on the Islamic Republic. In addition, Iran's trust in its weapon systems and its belief it will have them at its disposal at the moment of truth might erode, which could affect Iran's confidence and therefore also its conduct. Moreover, because the US strategy is to apply economic pressure on Iran while avoiding an armed conflict, the decision to replace the kinetic attack with a cyberattack allowed the United States to retain its strategy. A kinetic attack might have led to an unpredictable path whose future development would have been difficult to forecast, and might have inadvertently and undesirably diverted the United States from its chosen strategy.

However, the American decision also has negative ramifications. First and foremost, the fact that Iran has carried out a series of attacks on ships, overland pipelines, and now an American UAV without being immediately and contextually punished with sufficient magnitude to deter it from attempting similar attacks in the future, turns the Iranian uses of force into "permissible" according to the emerging rules of the game.

The US decision is problematic in a deeper sense as well. The arm twisting between the United States and Iran on the path to negotiations can develop into at least three different scenarios: one, with only economic pressure; two, with economic pressure plus bilateral demonstrations of force; or three, with a limited military conflict. In the first scenario, if the United States applies a steamroller of economic pressure to Iran, the US advantage is obvious. The leverage is unilateral, and Iran has few cards to play. In the third scenario too, that of a limited military conflict, the US advantage is unequivocal. Iran has no ability to resist the intensity, effectiveness, and tempo of the US war machine. The United States thus benefits from a competitive advantage in the first and third scenarios, but its relative advantage in the second scenario is lesser. However, the US decision to change the kinetic attack to a cyberattack actually makes it more likely the conflict will develop according to that second scenario.

In the second scenario, the two sides are prone to demonstrate their capabilities to operate against one another in very measured ways, and here the US advantage is reduced. This becomes more acute at a time when Iran does not recoil from using kinetic force, but the

United States does. Iran will likely continue to gradually violate its nuclear agreement commitments and, from time to time, stage attacks against maritime traffic, pipelines, and US military assets, and for its part, the United States will provide examples of capabilities such as cyberattacks. Thus, a reciprocal equation with certain mutual aspects emerges. Each illustrates its capabilities to the other; both sides gain and lose cards on the road to the US presidential election.

Likewise, Iran will steer the conflict to where it can maximize its capabilities. Iran cannot establish naval or air supremacy or even denial over time in the Strait of Hormuz, and it is incapable of disrupting the overland flow of oil for any significant period. It has relatively limited capabilities in a direct conflict of mid to high intensity. But Iran is quite adept at maximizing its capabilities when all it is called on to do is illustrate them from time to time in a low friction, clandestine manner, such as attacking a single vessel or causing localized damage to pipelines.

In an even deeper sense, one can say that in any strategic clash, one must multiply the sides' capabilities by their willingness to use them, i.e., the sides' appetite to take risks and pay the price. Notwithstanding the power of the United States, both sides are deterred by the costs and risks of a military conflict. But Iran manages to posture as if it is willing to bear the risks and costs of the use of force (and of a gradual retreat from its nuclear agreement commitments), while the United States is seen as lacking the will to take risks and incur the cost of using force.

The choice of a standalone cyberattack, i.e., absent synergy with complementary kinetic steps, further entrenches the US posturing as an actor deterred by risks and costs. In this sense, it may well be that the downside of the cyberattack outweighs it benefits. While it does illustrate capabilities, it also helps cement the United States positioning – in Iran's eyes and its own – as a risk-averse actor.