The Washington Post

How cyber operations can help manage crisis escalation with Iran

Brandon Valeriano and Benjamin Jensen

June 25, 2019

Signaling restraint, President Trump opted not to escalate the ongoing crisis with Iran by ordering precision airstrikes that would have resulted in civilian casualties. The discussion of potential responses to Iran's aggression, however, presents a false choice between conflict that results in death and backing down completely.

Instead, the United States chose to disrupt Iranian military targets with two distinct covert cyber operations. The United States appears to have sought to disable Iranian missile sites and eliminate the Iranian military's command and control capabilities.

The case illustrates the new character of strategy in a connected era. In times of crisis, countries increasingly opt for non-military coercive instruments of power, including cyberattacks and economic sanctions, to control escalation risk. As we note in a recent Cato Institute foreign policy analysis article, "rather than escalate with conventional military options, cyber operations offer rivals a way to respond to provocations without significantly increasing tension in a crisis."

Cyber operations are more political warfare than decisive battle instruments. They provide decision-makers valuable intelligence and potentially coercive options that help avoid direct military confrontation and can reduce the severity of the response.

The current crisis began with Iran seeking covert responses to the challenge of economic sanctions. U.S.-based cyber security firms noted an increase in Iranian hacking and spear-phishing attempts — when emails seek access to computer systems by pretending to originate from a trusted source. And there were also several conventional attacks attributed to Iran on shipping in the region.

In response, the United States deployed additional military assets to the Persian Gulf. After accusing Iran of shooting down the Global Hawk surveillance drone on Thursday, the United States faced the choice of limited military strikes to signal resolve — or choosing options representing less of an escalation.

Cyber strategy: What the data reveals

Events in the gulf reflect a larger pattern of cyber exchanges between rival nations, and echo the results of a series of survey experiments by our team and others. Data on cyber conflict between rival states between 2000 and 2016 suggests that Iran and the United States have engaged in 20 cyber conflicts during this time period. Iran has launched 13 operations, while the

United States launched seven operations. A decade ago, the Stuxnetoperation successfully penetrated Iran's nuclear production facilities and digitally destroyed some equipment used in the enrichment of uranium.

Since then, the United States tends to use cyber options to respond to Iranian aggression. And Iran often relies on cyber espionage directed against nongovernmental targets — or hits American allies in the region, in attacks such as the computer virus attributed to Iranian hackers that targeted Saudi Arabia's oil production facilities.

Trump's decision to respond to Iranian aggression with cyber operations aligns with recent findings from our ongoing war games and survey experiments. Based on 277 war game experiments involving a mix of national security practitioners, the business sector and college students at international relations-related programs, we find that parties are reluctant to escalate with cyber options in a crisis, preferring to use them — as we saw happen with Iran — in a more proportionate or equivalent response. Teams use cyber operations in a way that signals risk and preserves future options to manage a crisis.

The general public also tends to favor proportional responses involving cyber retaliation. Cyber responses offer great powers response options that stop short of military force, preserve flexibility and limit risk. In our ongoing research, we see a similar logic at play in survey experiments funded by the Carnegie Corporation of New York. We surveyed a representative sample of Americans, Russians and Israelis to run an experiment on the use of cyber operations in a scenario similar to the current standoff between Washington and Tehran. We randomly assigned 1,500 of the respondents the option of responding to an unfolding crisis with cyber options and offered the other 1,500 more traditional diplomatic, economic and military response options.

The findings were clear: Cyber options can help de-escalate deadly militarized disputes. The majority of the survey responses (764 total) in the cyber options group favored a de-escalatory approach, compared to proportional (620) and escalatory (156) alternatives. These levels were similar to the non-cyber treatment.

What's interesting in relation to the Iranian crisis is that when participants chose to escalate, 69 percent preferred cyber options, while 26 percent opted for a proportional cyber response. Survey respondents across these three countries used cyber options in a manner that preserved their flexibility and set conditions for follow-on operations.

Is this a digital off-ramp to war?

For leaders, managing an escalating international crisis with a rival nation is one of the most challenging situations. Contrary to conventional wisdom, cyber options preserve flexibility and give leaders an off-ramp to war. National security decision-makers are increasingly turning to cyber responses to manage great power competition.

When there is a crisis, some analysts argue that cyber options function best not as deterrence, but to manage an out-of-control situation — and avoid outright war. The question remains how the opposition is likely to perceive these moves. Will they recognize them as methods to tamp down the drums of war or see them as aggressive moves that require escalatory responses?

Social science research suggests the public and military operators view these cyber moves as ways of avoiding war. The hope is that those directing the management of a crisis believe the same thing.