LAWFARE

CYBERSECURITY: LOAC-MILITARY

Crossing a Cyber Rubicon? Overreactions to the IDF's Strike on the Hamas Cyber Facility

By Robert Chesney Monday, May 6, 2019, 2:27 PM

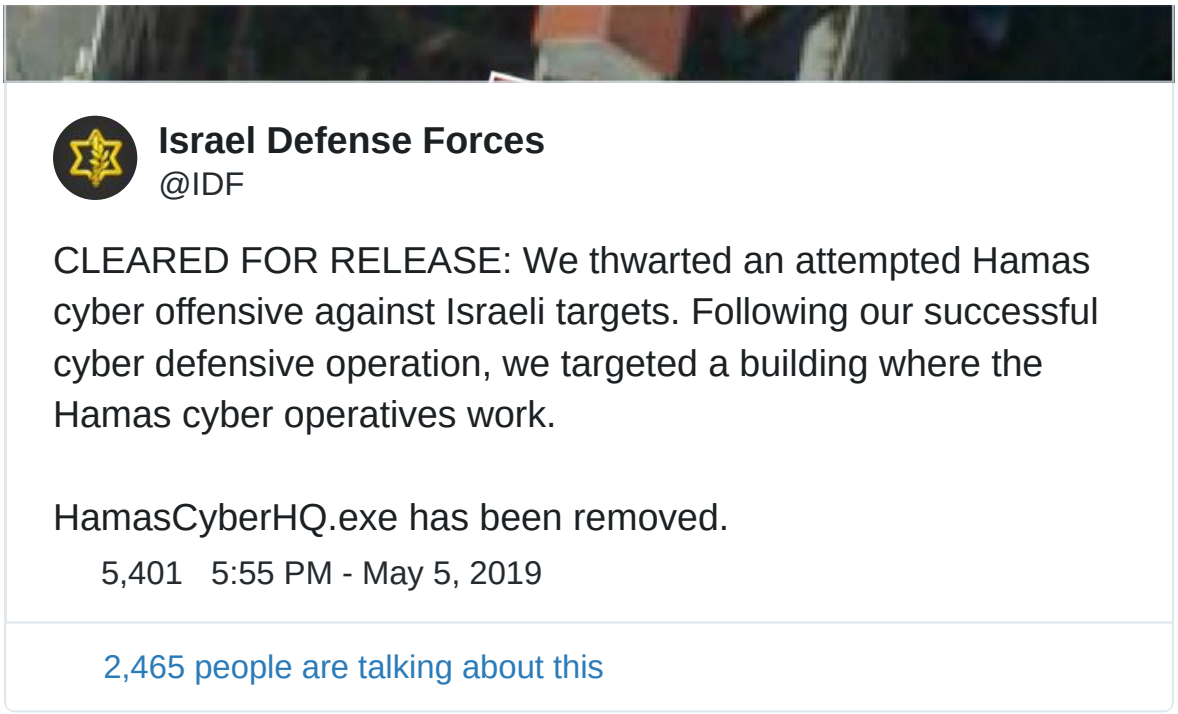
DayZero: Cybersecurity Law and Policy

Amid a massive exchange of rocket fire and airstrikes between Israel and both Hamas and Islamic Jihad this weekend, Hamas attempted a cyber operation against an unspecified civilian target in Israel. The operation failed, and in its aftermath the Israel Defense Forces (IDF) carried out an airstrike that destroyed the building housing Hamas's cyber capability. Some observers are citing the incident as an important—and perhaps dangerous—precedent. Others are questioning the legality of the strike itself. Both these views are misplaced.

Context

Details remain sketchy, but we know this much: Heavy fighting broke out last Friday in Gaza and Israel, with Islamic Jihad and Hamas launching more than 690 rockets and mortars indiscriminately into Israel, and Israel countering with some 320 targeted airstrikes. During these kinetic attacks, according to the commander of IDF cyber division, Hamas attempted to carry out some sort of cyber operation targeting Israeli civilian infrastructure in an unspecified fashion. The operation failed, apparently thwarted by the combined efforts of Unit 8200 and Shin Bet. And then the IDF conducted an airstrike on the building housing the Hamas cyber capability, destroying it and whatever equipment was within (and most likely killing at least some people as well, though I've not yet seen any reporting on that specific point).

Here's an IDF tweet acknowledging the basic elements of the story:



Following the IDF's announcement of the airstrike, some have suggested that Israel has crossed a Rubicon of sorts, creating a precedent for using lethal force in response to hacking. Separately, some are suggesting that the airstrike might have been unlawful given that the initial cyber operation Hamas attempted already had failed before the airstrike commenced.

Is there any merit to either suggestion? I don't think so, for the reasons set forth below.

1. **Did Israel's action really cross a Rubicon—was this an unprecedented kinetic response to a "mere" cyber attack?**

Some commentators have characterized the airstrike on the Hamas facility as an unprecedented kinetic response to a cyber operation. For example, on the Security Affairs blog, Pierluigi Paganini wrote: "The attack could be considered a milestone in modern warfare because it is the first time a cyber attack has been met with an immediate physical air strike."

The implication is that a line has been crossed, with potentially dangerous or at least important implications for future uses of force in response to hacking. I'm not persuaded that is the case, however.

To start, it helps to note that there can be two versions of this claim. The weak version of the claim might be descriptively true, but it is uninteresting. The strong version of the claim is the reverse: It would be very interesting if true, but it is not true.

Consider the *weak* version of the claim first. On this view, Israel's action may be the first example of a state using lethal force in direct response to a cyber operation *in a larger context of ongoing armed conflict*. That version of the claim might be true as a descriptive matter, but it is not particularly interesting or important. Whether novel in practice or not, it is not remotely surprising that a state engaged in armed conflict might treat the cyber capabilities of its adversary as a target. Indeed, so long as the Hamas personnel and equipment at issue constitute a legitimate military objective, it does not matter whether Hamas had just used them. Even if the equipment and personnel were simply sitting there on standby, Israel might have chosen to target that capability just as it might choose to target a military vehicle that was just sitting in a motor pool awaiting later use.

Incidentally, it is not clear that it is true that no state previously has used kinetic force against an opponent's cyber-related equipment or personnel. Something along those lines may well have happened previously in the context of the Russian invasion of Ukraine or in the context of the war in Syria. All we can really say here is that this is the first example that has been publicly described by the state that carried out the operation.

So what about the strong version of the Rubicon-crossing claim, the one that would be interesting and important *if* true? The idea here would be to divorce this airstrike from its larger context of an ongoing armed conflict and treat it as if Israel had simply decided to conduct a kinetic armed attack in response to a failed attempt by Hamas to cause some sort of harm to civilians via a cyber operation.

To see why this artificial decontextualization matters, consider an analogous hypothetical. Imagine that the United States fires missiles to destroy an Iranian Revolutionary Guard Corps (IRGC) building in Tehran after learning that the IRGC had attempted—unsuccessfully—to uses Trisis to cause damage at an industrial facility in the United States. This would raise U.N. Charter questions about whether the initial cyber operation by the IRGC constituted an armed attack triggering America's right of self-defense under Article 51 (and thus overcoming Article 2(4) objections to attacking the building in Tehran), whether the responsive attack was necessary and proportional in the *jus ad bellum* senses of those words (given that the provoking attack already had been repulsed), and so forth. These would be important and interesting questions (see Matt Waxman's article on the topic) and the fact pattern would indeed be novel. But these questions drop out if, instead, the situation is that the United States and Iran are engaged in an armed conflict entailing a massive exchange of fire already. There would still be U.N. Charter and *jus ad bellum* questions about the origins of the conflict, to be sure, but those questions would not turn on the characterization of the attempted cyber operation or the airstrike against the IRGC's kinetic capacity, just as they would not turn on the particulars of any one of the hundreds of other strikes constituting the conflict.

So too, here, with the IDF strike on the Hamas cyber capability. Put simply: Because of the context of armed conflict, the IDF strike does not constitute a precedent of any sort for what types of responses may be proper in the event of a cyber attack *outside* the context of armed conflict.

2. **Was the airstrike legal?**

Some have called this into question, but the arguments are not very compelling. Andrew Liptak writes:

A general principle of warfare and international humanitarian laws hold that attacks must be proportional in response. (For example, a country wouldn't be permitted to launch a nuclear missile against a capitol city if a single soldier is killed in a border skirmish.) Given that the IDF admitted that it had halted the attack prior to the airstrike, the question is now whether or not the response was appropriate. Either way, it opens up a worrying evolution in the state of modern warfare, given the threat that computer hackers can pose to military forces or nations.

As an initial matter, this appears to misstate the IHL/LOAC *jus in bello* proportionality rule. That rule forbids otherwise-proper strikes if the expected incidental harm to civilians or civilian objects would be excessive in relation to the concrete and direct military advantage expected if the strike succeeds. Here, there is not yet any claim (let alone supporting evidence to show) that Israel anticipated any incidental civilian harm, let alone excessive harm relative to the military advantage to be gained from destroying the ability of Hamas to conduct additional cyber operations.

Is the idea instead better framed in terms of the principle of distinction? There are those who argue that most if not all Hamas personnel are civilians rather than combatants (lawful or unlawful), and that they should not be attacked except when in the midst of their own attacks. And by extension, one might then argue that this is true for this building and the critical equipment it contained, too. If that's the spirit of the critique, though, then there is no reason to single out this particular episode as significant; it becomes just one of a great many other occasions to debate ideas like unlawful combatancy and civilian members of organized armed groups who have a continuous combat function.

At any rate, it looks to me like the essence of the critique instead concerns the idea of military necessity (that is, that an attack must be intended to serve a legitimate military purpose), based on the premise that the cyber operation conducted by Hamas had concluded (unsuccessfully) by the time the strike occurred. But, of course, the end of the one operation did not in any way foreclose the start of the next one using those same capabilities, equipment and personnel. The personnel were not *hors d'combat* (unable to engage in military activity), and the

building and equipment presumably were still functioning. So long as one accepts that this was a context of armed conflict, and also that the strike did not violate the principle of *distinction*, there is no basis for questioning the principle of necessity here.

Topics: Cybersecurity and Deterrence, Cyber & Technology, Cybersecurity: LOAC-Military, International Law, International Law: LOAC, Israel-Palestine

---

Bobby Chesney is the **Charles I. Francis Professor in Law** and Associate Dean for Academic Affairs at the University of Texas School of Law. He also serves as the Director of UT-Austin's interdisciplinary research center the Robert S. Strauss Center for International Security and Law. His scholarship encompasses a wide range of issues relating to national security and the law, including detention, targeting, prosecution, covert action, and the state secrets privilege; most of it is posted **here**. Along with Ben Wittes and Jack Goldsmith, he is one of the co-founders of the blog.

@bobbychesney