https://www.wsj.com/articles/strike-back-against-every-cyberattack-11548624081

OPINION | INSIDE VIEW

Strike Back Against Every Cyberattack

The U.S. can keep foreign hacks at bay by showing its ability and will to retaliate.

By

Andy Kessler

Jan. 27, 2019 4:21 p.m. ET

A press conference on Chinese cyberattacks in Washington, Dec. 20, 2018. **PHOTO:** ERIK S LESSER/SHUTTERSTOCK

Another week, another data breach. The latest is 773 million online accounts for sale, many with passwords included, known as Collection #1. More are likely to come—go ahead and check your status at HaveIBeenPwned.com. All this the same month Marriott admitted that five million unencrypted passport numbers were snatched from its system, probably by the Chinese. Oh, and the Russians might have hacked the Democratic National Committee again after the 2018 midterms. How do we stop this?

The foreign hacks are the most disturbing. Last month members of a Chinese espionage ring known as Advanced Persistent Threat Group 10 (a k a "Godkiller" and "Stone Panda") were charged by the Justice Department with hacking NASA, the Jet Propulsion Laboratory and even IBM . Earlier last year the Chinese were caught stealing submarine data from a U.S. Navy contractor. And horror of horrors, in 2017 an Iranian national hacked HBO and threatened to release unaired episodes and plot summaries from "Game of Thrones."

The U.S. has done close to nothing in response. Sure, special counsel Robert Mueller indicted 12 Russian intelligence officers last summer. I'm sure they're quaking in their boots. Maybe those "Game of Thrones" episodes could have taught our leaders something about retaliation and revenge.

So what is America's policy? That's unclear. But a good start would be to heed the words of Israeli Prime Minister Benjamin Netanyahu, who told the press last week that his state has a permanent policy of hurting "everyone who is trying to hurt us." The U.S. needs a similar stance to halt cyberattacks.

John Yoo, a Berkeley law professor and former Justice Department official, sees a parallel between deterrence in cyber and nuclear warfare. "Offensive nuclear weapons are relatively cheap," he explains to me: "It's defensive systems that are expensive." Think about it. Each mission to drop one nuclear bomb would cost the U.S. about a quarter-billion dollars. But we've spent trillions on our defense and deterrent system. The nuclear triad of intercontinental ballistic missiles, bombers and subs ain't cheap.

Mr. Yoo continues: "Similarly, offensive cyber weapons are cheap. It's defensive cybersecurity tools that are expensive." The cybersecurity market is estimated at $125 billion, and it gets bigger with each successive hack. Government and private firms have ramped up spending on encryption, firewalls, malware and virus protectors, intrusion detectors—it's an arms race. Yet we're still vulnerable.

We need a shift in strategic thinking. So where is our Herman Kahn? Kahn was the author of "On Thermonuclear War" and the father of the massive-retaliation plan for nuclear deterrence. If the Soviets knew the U.S. had a second-strike capability, Kahn argued, there would be no first strike. Mutual assured destruction—peculiarly, a term that was coined by the father of computer architecture, John von Neumann—works as a deterrent. Or it has so far anyway.

Washington should commit to use its weapons against all aggressors. One example of America's potential is Stuxnet, a U.S.- and Israeli-made virus that in 2007 infected Iran's uranium-enrichment centrifuges, causing them to spin out of control. Stuxnet was certainly an offensive cyberweapon, but not a retaliatory one.

The U.S. really needs a second-strike cyberweapons program. In December 2015 the Russians launched cyberattacks on Ukraine, shutting down three power plants (which ran on Windows PCs). The U.S. should have immediately flickered all the lights in Moscow, to show them we can. Meddle in our elections? Fill Russia's VK social network with endless Beto O'Rourke dental videos—it's only fair. When the Chinese stole plans for the F-35 stealth fighter from Lockheed , we should have made every traffic light in Shanghai blink red, announcing "Stop, Don't Hack Us Again." North Korea's Sony hack? Scramble state-run TV signals in Pyongyang. They'll get the message.

Is the U.S. capable of doing all this? It’s been less than a year since Army Gen. Paul Nakasone took over U.S. Cyber Command, or Cybercom in military speak. The group hasn’t announced much about what it’s doing. Is it a giant bureaucracy or an effective team within the military? A friend told me the story of a hacker who took down a Scandinavian country’s internet access for a day because someone annoyed him at a conference. Hire that guy! Let him wear camo and a Metallica T-shirt.

We need to develop an offensive deterrent. An I-hack for an I-hack. Maybe America has all these capabilities already. And of course, secrecy is important lest the other side patch its vulnerabilities. But as Dr. Strangelove lamented, “Of course, the whole point of a Doomsday Machine is lost, if you keep it a secret! Why didn’t you tell the world, eh?” The hack-a-week has got to stop.