3 Cyber gloves off

This year marks a decade since the US and Israel destroyed portions of Iran's covert nuclear weapons program using a computer worm known as Stuxnet, ushering in the modern era of cyber conflict. Ten years on, hackers have grown more sophisticated, societies have become heavily dependent on digital services, and efforts to agree on basic rules of the road for cyber conflict have gone nowhere. It's a mess.

For the first time, the US will attempt to establish deterrence by projecting its cyber power in more assertive ways

Cyber deterrence is hard. The source of an attack and lines between state and non-state actors are blurred in cyberspace. That makes it difficult to be sure whom to retaliate against, and attackers know that. Also, there is still a lack of clear red lines in many areas, meaning attackers can often get away with their misdeeds if they avoid clear 'no-gos' (such as critical infrastructure). Finally, cyber weapons become obsolete fast, and access to targets comes and goes. It's tempting to use a capability when you can, making the idea of Cold War-style peaceful stockpiling of weaponry less likely.

So, if cyber deterrence has never come close to actually working, what's new?

This year is a turning point. For the first time, the US will be undertaking a serious effort to establish real deterrence by projecting its cyber power in much more assertive ways. Not only will this show of strength fail to create an elective system of global deterrence, but it could backfire.

The US is changing its tone—and the doctrine of action and reaction—to become far more aggressive in the cyber world than it's been in the past. After taking a cautious approach while former president Barack Obama was in office, the US is now leaning heavily to-ward greater offensive action in cyberspace, including by freeing the Department of Defense's Cyber Command to unleash preemptive strikes. It's even considering giving private-sector actors leeway to "hack back" when attacked.

In an ideal world, this show of teeth would lead foreign actors to keep their arsenals in check and create a new security equilibrium in which perceptions of US cyber dominance would discourage attacks. That's not going to work—for two reasons.

First, like traditional deterrence, cyber deterrence works best against states. But many of the world's most destructive cyber actors are non-state actors who have less to lose from taking their chances on offense. We're particularly worried that the stolen National Security Agency tools that powered the 2017 'NotPetya' attacks are being updated for current software systems and have been incorporated into sophisticated cyber operations. Non-state actors' temptation to use them against critical infrastructure or corporate networks before systems are upgraded will increase in 2019.

Second, even governments won't back down in reaction to Trump's assertive cyber policy. In the US-Russia rivalry, it's unclear which nation controls escalation dominance—the ability of one side to dominate a conflict as it grows more serious—and whether classic deterrence would work. For weaker states such as Iran or North Korea, there's also an asymmetry of power in the use of cyber weapons that makes them too tempting not to use. Several of the world's most aggressive cyber powers have little to lose in the event of retaliation, given their low level of connectedness (think North Korea). And for China, the stakes are too high to allow the US sole use of a weapon that works. All of this leads to a scary prospect: The Trump administration thinks it's strengthening deterrence (and therefore peace) by deploying its arsenal, but the odds are greater that this show of force leads nations to "see and raise" the US's bet.