Opinion: Why cyber attacks are hard to combat

By Christopher S. Chivvis and Cynthia Dion-Schwarz

Imagine that the United States is hit by a cyberattack that takes down much of the U.S. financial infrastructure for several days. Internet sites of major banks are malfunctioning. ATMs are not working. Banks' internal accounting systems are going haywire. Millions of people are affected.

The first question that policymakers might debate is whether such an attack deserves a military response. But several problems immediately arise. First, would the U.S. government—and specifically the National Security Agency—know for certain who had conducted the attack?

Without being able to attribute the attack, or if there were some uncertainty about who was responsible, it would be very hard to strike back. Unlike conventional attacks, cyberattacks can be difficult to attribute with precision to specific actors. In the event of a major cyberattack, pressure to respond would be immediate—and probably intense. But if a country strikes back and the forensics are erroneous, then the retaliation will have unnecessarily and inadvertently started a war.

Russia's alleged meddling in the 2016 U.S. presidential elections has brought the issue of cyber war again to the top of the news, but the possibilities it raises are only the tip of the iceberg when it comes to the role of cyber operations in modern warfare. Most—although not all—analysts agree that cyber will be a key domain in the conflicts of the future. Exactly how cyber will impact these future conflicts, however, is hard to say with any certainty. Cyber weapons are not like missiles or tanks; because their initial impact is in the information domain, their effects are much harder to judge.

Even in cases where an attack is linked to one specific country—say, Russia—it could be hard to know for sure whether it was directed by the Russian government.

This is because governments like the Russian government appear to rely heavily on third parties to develop their cyber weapons and conduct their attacks. This offers them many benefits—deniability being one of them—but it also offers them less control over what their cyber warriors actually do – creating a so called “principle agent problem.”

In other words, an attack that originates from within the Russian cyber world might be the work of the Kremlin—or it might not. This further complicates the choice of response.

Sometimes, the culprit will be clear, of course. But in these cases, the question is how, specifically, to respond.

Some advisors might push for a cyber counter-attack that inflicts equal damage on the guilty party. But this isn’t always possible. If the perpetrator is a party like North Korea, then there is no equivalent financial system to target. But should the United States instead use conventional military weapons like a cruise missile, perhaps on Pyongyang’s cyber training facilities? A strike like that would clearly risk serious escalation of the conflict. It might be seen as disproportionate if the U.S. financial system had recovered in the interim with relatively minimal real damage.

Imagine, however, that the attack is against the U.S. power grid or oil and gas infrastructure. This kind of attack could easily have military consequences if it were extensive. The U.S. military has backup power generation capability as well as stocks of fuel reserves, but these stores are not infinite. If such an attack on U.S. infrastructure has military consequences, the case for a cyber retaliation—or even a

Tomahawk cruise missile strike—starts looking a lot stronger.

Even if the U.S. power grid were seriously affected by a cyberattack, however, and the United States knew with a high degree of confidence who the guilty party was, there would be reasons for caution—especially if the attack was an isolated incident and there were no other signs of aggression or malign intent.

This is because cyberattacks can have unanticipated consequences. With any military strike, collateral damage is always possible, but with most conventional attacks, methods of assessing and avoiding collateral damage are well developed, and based on well-established physics principles and observational experience.

But cyber weapons don’t operate like missiles or tanks. They attack the underlying network or computer systems. The possibility of unexpected effects in the cyber world is much greater.

For example, a cyberattack on an electrical grid might be intended to knock out the lights in a specific location, but end up affecting a whole region’s energy supply. The world saw this potential with the Stuxnet worm: Apparently intended for a very specific, isolated network (an Iranian control system), the worm was discovered precisely because it spread beyond its intended target into other related networked systems. Stuxnet did not attack other control systems, but only because the designers programmed in a self-destruct date. If the designers had been less cautious, its effects would have been much more widespread.

Therefore, before targeting a cruise missile at that (hypothetical) cyber hub in Pyongyang, the U.S. president would want to have at least some knowledge of both the intentions of the attacker and the consequences (including secondary effects) of the response—otherwise the United States might be starting a war by accident.

But a desperate foreign leader might miscalculate that he can get away with a surreptitious attack on U.S. infrastructure for exactly these reasons—and that in and of itself is cause for concern.

This is why context will make a big difference. It’s relatively easy to assess the damage done by an attack on America’s infrastructure, but less easy to assess the intent of that attack. If the U.S. power grid is seriously disrupted by a cyberattack during an ongoing war with a known aggressor it will be much easier to strike back—with kinetic (i.e. physical) force or with cyber weapons—simply because it will be easy to assume the attack was intentional.

Alternatively, a fearful foreign leader might lash out at the United States if she or he fears the United States is on the verge of conducting a devastating cyberattack. The hostility might come in the form of a massive, pre-emptive cyberattack, a conventional attack, or in the extreme, even a nuclear salvo.

Since the ability to mount cyberattacks depends on keeping targeted vulnerabilities secret, both sides may fear that their adversaries possess capabilities that have far-reaching destructive potential – even when they don’t. This fear in turn could increase the tendency toward pre-emptive action and hence escalation.

Cyber adds new and significant uncertainty to warfare, making it difficult both to deter and respond. It will take time and a great deal more research and analysis before the problem is fully understood.

Christopher S. Chivvis is associate director of the nonprofit, nonpartisan RAND International Security and Defense Policy Center. Cynthia Dion-Schwarz is a senior scientist and the Manager of Cyber and Data Sciences Programs at the nonprofit, *nonpartisan RAND Corporation. This essay is part of an Inquiry, produced by the Berggruen Institute and Zócalo Public Square, on what war looks like in the cyber age.*