When does a cyberattack mean war?

By Byard Duncan, Reveal

Sen. John McCain, who spent more than five years in Vietnamese captivity, is no stranger to traditional war. But when the Arizona Republican recently brought together officials from three intelligence agencies, his focus was on a more modern frontier: cyberspace.

Given reports of Russian interference in last year's presidential election, McCain wanted to know how the U.S. might appropriately respond. So 20 minutes into the hearing, he posed a blunt question to Director of National Security James Clapper: Would a successful digital campaign to alter the outcome of a U.S. election equal an attack on the U.S.?

Clapper demurred.

"Whether or not that constitutes an act of war I think is a very heavy policy call that I don't believe the intelligence community should make," he said. "But it certainly would carry, in my view, great gravity."

Clapper's response highlighted an alarming point about U.S. cyber policy, one that could prove troublesome as U.S.-Russia tensions mount and an unpredictable new administration gets its bearings: America does not have a clearly defined threshold at which digital offensives escalate into all-out war.

A history of disagreement

In 1996, the U.S. and Russia began meeting in secret to establish a set of common protocols for their respective operations in cyberspace. Since then, they've managed to

agree, via the United Nations, that international law applies in the digital realm — and that countries must take responsibility for the actions of hackers operating within their borders. As recently as 2015, the two parties also agreed that no state should use digital tools to target each other's critical infrastructure during peacetime.

But the common ground essentially ends there. While Russia historically has pushed for treaties that limit the use of digital weapons, the U.S. for years has claimed that cooperation among international police is a better technique for regulating cyberspace.

Throughout this standoff, both sides have taken shots at the other's approach: U.S. critics say any treaty Russia creates would limit free speech by targeting citizens who find a way around the country's censorship infrastructure; Russia maintains that America, in refusing to come to the table, is willfully stoking a digital arms race.

The latter assessment isn't so far off, according to some experts.

"Of all countries, the U.S. has the fewest incentives to reach any binding agreements about the limitations of use of cyber weapons," said Bruce McConnell, a former deputy undersecretary for cybersecurity at the Department of Homeland Security in the Obama administration. "When you have asymmetry in the world, as we still do, there's less incentive in the most powerful superpower to put something on the table that says we won't use this capability."

Yet even as the U.S. has developed and refined its cyber arsenal, its deep reliance on information technology has made it among the world's most alluring targets for hackers, McConnell said. At the same time, its own record of cyber espionage and interference across the globe — even against allies such as Germany and Brazil — repeatedly has damaged its

international credibility.

All the while, Russia has made no secret of its intention to use cyber tools as a means of gaining geopolitical leverage. In 2007, the country allegedly launched a devastating attack on Estonia's government and banks as retaliation for the country's removal of a Soviet-era statue. And in its 2010 military doctrine, Russia acknowledged its interest in waging "information warfare," which can "achieve political objectives without the utilization of military force." That approach aligns with a recent intelligence community assessment that Russian President Vladimir Putin "ordered an influence campaign in 2016 aimed at the US presidential election."

"There is a kind of sparring back and forth that the United States didn't really see but the Russians believed they were engaged in," said Adam Segal, a senior fellow at the Council on Foreign Relations and the author of "The Hacked World Order."

"The U.S. clearly is not an innocent actor in cyberspace," he added. "But I do think Russian behavior crossed a new line."

Cold War II?

During the Cold War, the U.S. and the Soviet Union engaged in a constant dialogue about what might constitute a "red line" and what forms of retaliation might be appropriate. Huge nuclear stockpiles in both countries provided a deterrence structure based on the concept of mutually assured destruction. But as Segal points out in his book, no such dynamic exists in cyberspace, where capabilities can be disguised and attribution is difficult.

"Washington, Moscow, and Beijing have an interest in identifying legitimate targets and thresholds," Segal writes, adding that the three powers likely would agree that a cyberattack with " 'kinetic effects' equivalent to those of a conventional armed attack" could warrant an act of boots-on-

the-ground self-defense.

Indeed, the Obama administration, in a 2011 document titled "International Strategy of Cyberspace," affirmed that "when warranted, the United States will respond to hostile acts in cyberspace as we would to any other threat to our country."

So how severe must an attack be for the U.S. to retaliate? It doesn't always take much, according to Herbert Lin, a senior research scholar for cyber policy and security at Stanford University. Lin points to Operation El Dorado Canyon, a 1986 U.S. airstrike campaign, as an example: After Libyan forces bombed a Berlin discotheque frequented by Americans, killing two and wounding 79 others, the U.S. targeted Libyan airfields and barracks, killing at least 40 people in retaliation.

"In justifying this," Lin said, "we invoked our right to self-defense, saying that this was an action that was intended to discourage future attacks and therefore was legal under the U.N. Charter." The U.N. disagreed.

The event raises questions about the U.S.' willingness to use force following a cyberattack: What happens if a country such as Russia or Iran launches a digital assault against an American factory, accidentally killing 10 workers? Or 20?

"There is no clearly defined threshold, even outside of cyber," Lin said. "If there's no clearly defined threshold outside of cyber, how do you expect there to be one in cyber?"

These boundaries will matter more as countries such as Russia and the U.S. continue to test their tools on adversaries. The U.S.' cyberattacks on Iran's nuclear facilities, for example, were the first (and, so far, the only) to yield physical destruction; they also were criticized as an illegal act of force in a NATO-commissioned report. Meanwhile, Russia's alleged infiltration of U.S. electoral boards might have qualified as an assault on critical infrastructure (therefore violating U.N. protocols), were it not for one fact: The

Department of Homeland Security failed to designate electoral systems as critical infrastructure until Jan. 6 – two months after Donald Trump won the presidency.

Many experts agree that escalating tensions, coupled with ever-developing cyber weapons, call for a new military paradigm. Yet there's not a fully developed picture of how that paradigm should look. This predicament was neatly summed up in a 2015 study in the Texas International Law Journal:

"Traditional kinetic (laws of armed conflict) principles simply do not fit this new wave of warfare. The limitations of applying traditional (laws of armed conflict) to cyber acts have left nation States misguided and confused."

The rules in place

To be clear, there is a solid – albeit imperfect – legal framework that governs how the U.S. and other countries should respond to cyberattacks. The U.N. Charter draws a distinction between actions that constitute a use of force and others that amount only to meddling in another country's sovereign matters. Although it makes no direct mention of "cyber," the charter also dictates what sort of responses might be appropriate in each case.

That doesn't mean it's free of vagaries, though. A 2002 analysis published by the U.S. Naval War College on whether the U.N. Charter's Article 2(4), which bans the use of force, applies in cyberspace offered an equivocal answer.

"It likely will be a long time, if ever, before the practice of States, decisions of the International Court of Justice, or other recognized sources of international law yield a clarification of how Article 2(4) applies to (computer network attacks)," it states.

According to Catherine Lotrionte, Georgetown University's CyberProject director in the School of Foreign Service, most

legal experts would agree on one thing: Russia's alleged efforts to swing the presidential election don't rise to the level of an armed attack – or even a use of force. They were, however, still forbidden under a provision of international law that bans "coercive interference."

So how might the incoming Trump administration – whose affinities for Russia are well documented – respond to similar attacks if they persist?

"There won't be one standard threshold or trigger for all occasions," Lotrionte said. "It will all depend on the nuances of the facts of a specific case."

It's a theme: Few firm boundaries exist in cyberspace – mostly because any nation's military decisions will be flavored by a host of political considerations, such as an adversary's military capabilities. Yet the clearest protocols available might have come from a speech at a legal conference for government agencies in September 2012. There, a legal adviser to the U.S. State Department named Harold Koh explained how the use of cyber weapons factors into the U.S.' larger national defense goals.

He began by posing – and answering – a series of questions: Do international laws apply in cyberspace? (Yes.) Do cyber activities ever constitute a use of force? (Yes.) May a state ever respond to a computer network attack by exercising a right of national self-defense? (Yes.)

But he also acknowledged that many pressing cyberdefense issues, such as how to properly attribute attacks to a nation or group, do not yet have clear legal answers. And they might not come anytime soon.

"Answering … tough questions within the framework of existing law, consistent with our values and accounting for the legitimate needs of national security, will require a constant dialogue between lawyers, operators and policymakers," he

said.

Given Trump’s clashes with the intelligence community, most recently over his associates’ potential ties to Russia, it’s unclear how robust this dialogue will be. Even experts such as Segal, the “Hacked World Order” author, aren’t sure what to expect.

“We don’t really understand necessarily how it’s going to play itself out, what the outcomes are going to be,” he said.