Claiming credit for cyberattacks

May 2 2018, by Kenneth Best

Credit: CC0 Public Domain

The decision to claim credit for a cyberattack on a government or institution depends on both the goals of the attack and the characteristics of the attacker, according to a study co-authored by a UConn political scientist that is one of the first to look into the voluntary claiming of cybersecurity operations.

The type of attacker – whether a state or a non-state actor such as a terrorist group – determines whether credit is claimed for a cyberattack and how it is communicated, according to the study, "Rethinking Secrecy in Cyberspace: The Politics of Voluntary Attribution," forthcoming in the Journal of Global Security Studies. Co-authors of the study are Evan Perkoski, assistant professor of political science at UConn, and Michael Poznansky, assistant professor of political science at the University of Pittsburgh's Graduate School of Public Affairs.

Among the findings of the study:

- Both states and non-state actors face similar decisions in the lifecycle of a cyberattack, yet the characteristics of each can cause their strategies to diverge, "particularly with the optics of credit claiming."
- While most research treats cyber operations as distinct from more traditional elements of state power, states "may be able to leverage their cyber assets to achieve many of the same goals most frequently pursued with conventional forces."
- The decision to privately or publicly acknowledge sponsorship of an attack may provide "crucial information about both their motives and identity."

Perkoski says that in developing the study, a distinction was drawn between cybercrime and cyberblackmail because "they are inherently different forms of cyber operations with different goals in mind."

He notes that typically the goal of cybercrime is personal or financial gain, which does not follow the same logic as states operating against other states in cyberspace. In the case of cyberblackmail, the attacker wants the victim to know something was stolen, such as when North Korea hacked into the servers at Sony following the release of "The Interview," a film about assassinating its leader, Kim Jong-un.

"They hacked into Sony servers, stole certain information, and said we want you to do X or we'll release this information," Perkoski says. "It was a form of pretty basic blackmail. It's not operating on the same kind of pattern of state-on-state or non-state-on-state intervention in cyberspace. In that case, you only want to communicate with the person you've hacked and let them know you have this material. It's a different dynamic than a state trying to coerce an opponent to give up their nuclear arms program."

The researchers began their collaboration studying cybersecurity several years ago while they were both fellows at the Belfer Center for Science and International Affairs at Harvard's Kennedy School of Government. Perkoski is a specialist in political violence and terrorism, while Poznansky studies clandestine and covert interventions.

Perkoski says the alleged Russian meddling in the 2016 U.S. Presidential election fits into the study's findings. Russian operatives reportedly hacked into the Democratic National Committee computers to obtain emails from the Hillary Clinton campaign, and then used social media trolls to sway public opinion toward Donald J. Trump's campaign.

"Russia wouldn't get as many benefits from claiming their operation," he says. "They're not looking to get attention for their message or cause. They're really looking to influence the way events might unfold. Because it's unclear, it makes it hard for the U.S. to take a hard stance against them. You can always play devil's advocate and say maybe it wasn't Russia, as President Trump has said. Maybe it was some guy in his basement hacking on his own. In that case, it makes sense that Russia doesn't want to claim credit, to limit possible escalatory dynamics."

One of the challenges in confirming clandestine state-sponsored activities is that it may only be possible from classified documents. Perkoski says scholars are still learning important details about historic

events with the release of classified documents decades after the events occurred, such as the recent release of documents concerning the controversial 1961 U.S. invasion of Cuba at the Bay of Pigs.

"When we think about what's happening with the U.S. and Russia, Iran, and North Korea and their cyber operations, it may be another 30 or 40 years until we know what's really going on," he says.

Perkoski says the study helps to clarify the fact that not all cyber operations are inherently anonymous, and that actors may claim credit for them, which then opens the door to using cyber tools as almost traditional instruments of state power. At the same time, there is no firm understanding of how non-state actor groups operate in cyberspace.

"We know a lot about how terrorists and insurgent groups come together, and what sustains them, but we don't have a theory of any of this stuff for a hacking organization and whether they follow the same paradigms or not," Perkoski says. "How do you defeat a militant organization or a hacking collective like Anonymous when they're all spread out around the world, they operate in states that don't have extradition treaties with the United States, and they might even operate in some states that give them de facto immunity? We know, for instance, that some Russian hackers don't get support from the government, but they allow them to operate freely because they're operating in Russia's own interest. That raises a lot of questions about understanding these groups."

At the same time, Perkoski says, as advances in cybersecurity improve the ability of government and law enforcement agencies to track hackers, terror groups and militant organizations are moving away from technology.

"There was a period when government agencies were quite effective at using these tools to their advantage and gaining information. Now I think

you're seeing militant groups respond to that and go more low-tech, to avoid some of those weaknesses," he says. "Look at how the U.S. found Osama bin Laden in Pakistan. It wasn't through hacking or satellite imagery. It was by tracking a courier going to his house and meeting with other guys who would go back to Afghanistan. It was very much traditional signals intelligence that the CIA has been using for 50 to 60 years."

Provided by University of Connecticut