PHYS.ORG

Putting understudied terrorists under a microscope

January 25 2019

Bombs exploding, hostages taken and masked gunmen firing machine guns are all types of terrorist attacks we've seen. According to new Michigan State University research, it's the attacks we don't see—cyberattacks—that happen more often and can cause greater destruction.

"Little work has been done around the use of the internet as an attack space," said Thomas Holt, professor of criminal justice and lead author. "The bottom line is that these attacks are happening and they're overlooked. If we don't get a handle understanding them now, we won't fully understand the scope of the threats today and how to prevent larger mobilization efforts in the future."

Holt's findings, published in *Terrorism and Political Violence*, underscore his concern for awareness and action: ideological cyberterrorist attacks are outpacing physical attacks among far-left groups.

To understand these attacks, Holt analyzed the scope, growth and impact of ideological cyberterrorist incidents from far-left groups, such as the Animal Liberation Front, Earth Liberation Front and the hacker conglomerate group Anonymous. These groups, Holt explained, don't necessarily want to physically harm humans; rather, they're motivated by animal and environmental activism and feel passionate about attacking companies, organizations and government entities that go against their beliefs. Unfortunately, everyday consumers get caught in attack aftershocks from data breaches and information loss.

"These kinds of ideologically motivated attacks are devised to have an emotional and economic impact on groups that go against their beliefs," Holt explained. "If you visit a company's website expecting to see one thing and this group has instead hacked the website and posted customers' personal information, that's a huge issue for both the company and the consumers."

Organizations in Holt's research that have fallen victim to these attacks range from Dow Chemical to the federal government, and in industries ranging from meat production to fashion. He explained that the high-profile nature of the internet—on which these ideological groups can manipulate traffic—is the ideal platform to attack.

"If you're a consumer and you bought a product from one of the victim companies, these attackers would target your data as being associated with something that goes against their ideological beliefs," Holt said. "In another case, the group attacked the federal government by releasing passwords for government agencies."

Holt's research examined physical and cyber terror attacks committed by these far-left groups between 2000 and 2015 in the United States, United Kingdom and Canada.

"The number of physical attacks by these groups was steady for the first few years of our study and then declined over time," Holt said. "At the time, cyberterrorist incidents began increasing and peaked at nine attacks in 2015. While we can't speculate as to why physical attacks have declined, we believe that the cyber component increased because these attacks generate an economic and emotional impact, draw attention to their cause from the public and may be less likely to lead to arrest."

Holt and his team, which included MSU criminal justice colleague Steven Chermak, focused on attacks following four forms of cyber crime: denial of service, or taking a certain resource offline; web defacements, when criminals remove content of a website and replace it with content of their own; data breaches, during which the criminals steal sensitive information about individuals or an organization; and doxing, where the criminals acquire personal information about people and release it online to be used for harassment.

Whether acting as a mobilized organization or an individual, ideological cyberterrorists are as dangerous as the violent extremists seen across the globe. In fact, only one of the incidents Holt observed resulted in an arrest, meaning the actors are still at-large. The mask of the internet makes them harder to catch and easier for them to hide, Holt said.

"These groups might strike domestically, but their damage on the web can be widespread and a concurrent risk for companies and consumers alike. It could be even greater," Holt said.

Next, Holt will examine the radicalization process of online attackers, whether they were cyber-oriented actors first, or whether their ideological beliefs led to cyberattacks. He will also examine attacks attributed to other ideologies, such as jihadist organizations.

More information: Thomas J. Holt et al. Examining Ideologically Motivated Cyberattacks Performed by Far-Left Groups, *Terrorism and Political Violence* (2019). DOI: 10.1080/09546553.2018.1551213

Provided by Michigan State University

Citation: Putting understudied terrorists under a microscope (2019, January 25) retrieved 27 April 2024 from https://phys.org/news/2019-01-understudied-terrorists-microscope.html