



Cyber Evolution of Terrorist Groups

Mehmet F. Bastug

Assistant Professor, University of Scranton



Orion
Policy
Institute

Orion Op-Eds

September 30, 2021

orionpolicy.org



Mehmet F. Bastug

Assistant Professor,
University of Scranton

Many real-world crimes have long been replicated in cyberspace. Terrorism and extremism are no different. Today's terrorist groups exploit the advantages the Internet has to offer. Just like everything else, crime, terrorism, violence and even war have transformed into cyberspace: online radicalization becomes as significant as face-to-face radicalization, violent groups emerge on the online platforms, and states use hacker groups to attack their enemies. In such a context, cyberterrorism is becoming a national security concern.

ISIS is one of the examples of terrorist groups that utilize the Internet and communication platforms to extend its influence. The group operates websites, online journals, and social media profiles to disseminate terrorist ideology. ISIS also uses the Internet for fundraising and recruitment. Such online appeals support the group's objectives in the physical world, as they simultaneously move forward and engage in digital battles with adversaries. In one such case Ardit Ferizi, a hacker, was arrested for his involvement in a hacking incident related to ISIS in 2015. He was charged with obtaining personally identifiable information of U.S. military members and giving that information to an ISIS recruiter. The so-called United Cyber Caliphate, ISIS's cyber division, launches operations to support the group's objectives. ISIS recruits hackers by making the group appear attractive to interested, adventurous youth. They reach out to young hackers and offer them a role in their digital and "distorted" jihad.

In the world of increased border controls and military and law enforcement capabilities, terrorists may have a better chance penetrating cyber borders instead of physical ones.

Violent extremists are facing continuous international counterterrorism efforts and losing ground in the physical world. Cyber-attacks are enticing to terrorist organizations because they can be perpetrated from anywhere in the world and with relatively fewer resources. DHS's October 2020 national threat assessment report listed cyber threats from nation-states or non-state actors as one of the seven major threats to the Homeland. A large-scale cyber-attack could result in extensive damage to the economy and possible physical harm. The recent Colonial pipeline hack is just one example of the potential harm that can be caused by a cyberattack.

The current cyberthreat landscape suggests that state-backed hacker groups are more of an imminent threat than terrorist organizations. State-sponsored hacker groups are more likely to have resources and capabilities to infiltrate into protected computer systems and inflict considerable harm. However, it should be noted that developing cyber-attack capabilities and initiating destructive attacks take a long time. Discovering vulnerabilities and gaining unauthorized access are time and resource intensive. Terrorist groups are now in the preparation phase and learning how to adapt and evolve to this changing environment. If their activities are not disrupted, they will reach such a capacity sooner or later.

There is an ongoing paradigm shift in national defense. In addition to traditional battlegrounds, land, sea and air, there is now another arena, cyberspace. Governments use hacker groups as proxy armies against their adversaries. They hide behind the anonymity cyberspace provides. The relative success of cybercrime syndicates and state-linked hacker groups has encouraged terrorist groups to invest more in cyberspace.

Cybersecurity is a never-ending battle. We need to always stay one step ahead of malicious actors to protect national security. Be it a nation state, terrorist organization, or a hacktivist group, the attack vectors are similar. Reassessing the risk management strategies, building partnership with the public sector, and implementing a holistic approach in cybersecurity are some good practices to deal with ever-increasing cyberthreats. To deal with cyberterrorism, disrupting cyberterrorist networks and their capacity improvement efforts needs to be on the to-do list of the government.

Web page link:

<https://orionpolicy.org/orionforum/58/cyber-evolution-of-terrorist-groups>

Photo by

1st Page - Timo Wielink via Unsplash

2nd Page - Kevin Ku via Unsplash

© September 2021. All rights reserved by Orion Policy Institute Publications.

Orion Policy Institute is an independent non-profit think tank based in Washington D.C.

1050 Connecticut Ave NW Suite 500,
Washington, DC 20036
orionpolicy.org

