Preventive drone attacks based on digital traces are a gray area under international law

March 28 2024

Credit: Unsplash/CC0 Public Domain

Identifying terrorists by analyzing their online activities is an approach that is sometimes at odds with international law, especially if the outcome is death. A study has documented this problematic legal and

ethical issue.

These days, virtually everyone leaves footprints in the digital world. Terrorists are no exception. Intelligence agencies realized this a long time ago in the wake of the 9/11 attacks—before Facebook and even before Myspace, when forums reigned supreme on the Internet and mobile phones were just in their infancy. The United States made extensive use of this digital windfall to track members of Al-Qaeda, and other countries soon followed suit.

Since then, social network analysis (SNA) has become an indispensable tool in digital tracking. It is used as much to catch local criminal groups as to track down terrorists in countries at war. SNA is also used in military operations designed specifically to kill suspected members of terrorist organizations, for example by means of drone raids.

A team of lawyers and sociologists from the University of Geneva has shown that such preventive use raises serious questions in international law and probably leads to a significant number of errors.

Their study, which was recently published in the *Journal of Conflict and Security Law*, is the first to combine sociological methodology with legal analysis. By analyzing a body of reports and academic articles by historians, lawyers and journalists, the team assessed how often SNA is used in anti-terrorist operations, how it is used and for what ends.

These are questions that are often frustrated by the armed forces' lack of transparency, particularly as regards war situations, such as in Syria or Afghanistan.

Contact with terrorists doesn't make you a terrorist

too

Since 11 September 2001, anti-terrorist operations have often been assimilated—from a legal perspective—into international conflicts. But as Michael Moncrieff, lead author of the study, points out, the fight against Al-Qaeda in Afghanistan or Daesh in Syria is different in nature from a traditional conflict. "In the Russia-Ukraine war, there is a clear distinction between the combatants—you know who's who. That's much less clear in the war against terrorism."

In conflict situations, however, there is a requirement under international humanitarian law that you must know who you're dealing with. Especially if you are intending to eliminate them. The law draws a fundamental distinction between fighting forces—who, from a legal perspective, are the sole legitimate targets of action—and everyone else.

De facto, "some groups that are considered terrorists fulfill the criteria for 'organized armed groups,'" explains study co-author Pavle Kilibarda. "They can therefore be deemed to be engaged in armed conflict and considered legitimate targets under international humanitarian law."

But if an individual is affiliated with a terrorist group, does that make them a combatant by default—even if, for example, they are not directly engaged in hostilities? Moreover, how do you determine what constitutes affiliation?

These are thorny questions, especially as information from the ground frequently contains little about anti-terrorist campaigns. The role of SNA is often to compensate for precisely this lack of information. In broad terms, an individual's affiliation with a given group is determined by the type of relationship (family, friend, acquaintance) or how often they have contact with a particular known or presumed terrorist.

The authors believe that from a legal perspective, such proximity criteria are not sufficient to incriminate an individual. "Even if someone has repeated online contact with a terrorist, that does not necessarily make them a member of the group," Moncrieff believes.

Drone attacks solely based on digital traces

SNA use is particularly problematic if it is the sole criterion on which operations to kill terrorists are based. "It's a very different situation from criminal enquiries, where SNA can be used to identify suspects as a prelude to questioning them and establishing their guilt," Moncrieff explains. "A drone raid is by nature final and irreversible."

According to the researcher, witness reports tend to indicate that such errors have occurred relatively often, particularly in Afghanistan. Although the armed forces are rarely transparent about their operations, numerous indicators converge to suggest that SNA is widely used in anti-terrorist operations.

According to certain experts on the ground, 90% of drone attacks are at least partially the result of social network analyses. Similarly, witness statements obtained from several independent studies suggest that it often requires very little for an individual to be designated a terrorist and eliminated. For example, American veterans of the Afghanistan conflict report that people were targeted for the sole reason that they had been in the company of a terrorist.

However, Moncrieff does not believe that this means SNA should be banned as a weapon in the fight against terrorism. "It can be very helpful in understanding the organizational features of terrorist groups, anticipating what they are going to do and determining who is collaborating with whom."

But on-the-ground use indicates that it is often employed to determine individuals' affiliation with groups on the basis of proximity. Sometimes, a simple online exchange is sufficient. "For this reason, SNA should never be the primary or even the only tool used in decisions as irreversible as physical elimination."

More information: Michael Moncrieff et al, Social network analysis and counterterrorism: a double-edged sword for international humanitarian law, *Journal of Conflict and Security Law* (2024). DOI: 10.1093/jcsl/krae002

Provided by Swiss National Science Foundation