Electronics Gadgets and Terrorism

By

Dr.Vinod Kumar Singh

Associate Professor Physics K .S. Saket P G College Ayodhya

Email: vks423272@gmail.com

The technology proficiency of terrorist organizations is on a swift rise.

As governments continue to unravel the planning behind the Paris attacks, groups such as the Islamic State and Boko Haram are using consumer technology products and social media to communicate and propagandize.

"The Islamic State uses a wide variety of communication technologies, just as we do, the public," said Joe Hall, chief technologist at the Center for Democracy & Technology, a Washington, D.C.-based nonprofit organization dedicated to ensuring the Internet remains open, innovative and free.

The Islamic State devotes a division of its commanders to educating both sympathizers and members alike on how to use new, encrypted communications.

"The efficacy of their operation is largely derived from the emphasis on easy-to-use, popular technologies — by creating a dual use for Twitter and others as not only social media platforms but also as both broadcast channels and tools," said Michael S. Smith II, a Congressional counter-terrorism consultant at Kronos Advisory.

Smith serves as a liaison for hacking collective Ghost Security Group — a counterterrorism organization that uses data mining to combat extremist groups. Ghost Security Group found the following applications receive the most attention among

members and supporters of the Islamic State: Twitter, Facebook, Telegram, Threema, Kik, Wickr, SureSpot and WhatsApp, which is owned by Facebook. Ghost Security Group sent the information to Smith, who is not a member of Ghost, to share with governments.

'Encrypt almost everything'

The expansion of encryption is not going to slow down.

"Very soon regular commercial laypersons' communications devices — such as your phone or [Apple's] iMessage — are going to have to be very, very secure by default," Hall said. "We're going to encrypt almost everything in the near future."

Encryption's increasing ubiquity comes from the benefits of securing oneself against everyone from common criminals to government-level hackers. And the answer is not by trying to staunch the flow of products or access to applications to certain groups.

Eliminate Barriers to Aggressive Collection of Information on Terrorists

Complex bureaucratic procedures now in place send an unmistakable message to Central Intelligence Agency (CIA) officers in the field that recruiting clandestine sources of terrorist information is encouraged in theory but discouraged in practice.

Inside information is the key to preventing attacks by terrorists. The CIA must aggressively recruit informants with unique access to terrorists' plans. That sometimes requires recruiting those who have committed terrorist acts or related crimes, just as domestic law enforcement agencies routinely recruit criminal informants in order to pursue major criminal figures.

CIA has always had a process for assessing a potential informant's reliability, access, and value. However, the CIA issued new guidelines in1995 in response to concern about alleged serious acts of violence by Agency sources. The guidelines set up complex

procedures for seeking approval to recruit informants who may have been involved in human rights violations. In practice, these procedures have deterred and delayed vigorous efforts to recruit potentially useful informants. The CIA has created a climate that is overly risk averse. This has inhibited the recruitment of essential, if sometimes unsavory, terrorist informants and forced the United States to rely too heavily on foreign intelligence services. The adoption of the guidelines contributed to a marked decline in Agency morale unparalleled since the 1970s, and a significant number of case officers retired early or resigned.

Recruiting informants is not tantamount to condoning their prior crimes, nor does it imply support for crimes they may yet commit. The long-standing process in place before 1995 provided managers with adequate guidance to judge the risks of going forward with any particular recruitment.

Recommendations:

- The Director of Central Intelligence should make it clear to the Central Intelligence Agency that the aggressive recruitment of human intelligence sources on terrorism is one of the intelligence community's highest priorities.

- The Director of Central Intelligence should issue a directive that the 1995 guidelines will no longer apply to recruiting terrorist informants. That directive should notify officers in the field that the pre-existing process of assessing such informants will apply.

The Federal Bureau of Investigation (FBI), which is responsible for investigating terrorism in the United States, also suffers from bureaucratic and cultural obstacles to obtaining terrorism information.

The World Trade Center bombers and the foreign nationals arrested before the millennium sought to inflict mass casualties on the American people. These incidents

highlight the importance of ensuring that the FBI's investigations of international terrorism are as vigorous as the Constitutionallows.

The FBI's terrorism investigations are governed by two sets of Attorney General guidelines. The guidelines for Foreign Intelligence Collection and Foreign Counterintelligence Investigations (FI guidelines), which are classified, cover the FBI's investigations of international terrorism, defined as terrorism occurring outside the United States or transcending national boundaries. Domestic terrorism is governed by the Attorney General guidelines on General Crimes, Racketeering Enterprise and Domestic Security/Terrorism Investigations (domestic guidelines). The domestic guidelines would apply, for example, to an investigation of a foreign terrorist group's activities in the United States if the FBI does not yet have information to make the international connection required for the Fl guidelines.

Both guidelines set forth the standards that must be met before the FBI can open a preliminary inquiry or full investigation. The domestic guidelines authorize a preliminary inquiry where there is information or an allegation indicating possible criminal activity. A full investigation may be opened where there is a reasonable indication of a criminal violation, which is described as a standard "substantially lower than probable cause."

The domestic and Fl guidelines provide the FBI with sufficient legal authority to conduct its investigations. In many situations, however, agents are unsure as to whether the circumstances of a particular case allow the authority to be invoked. This lack of clarity contributes to a risk-averse culture that causes some agents to refrain from taking prompt action against suspected terrorists.

THREATS ASSOCIATED WITH IT INFRASTRUCTURE

When the IT infrastructure is attacked, the target can be the IT itself. Alternatively, the true target of the terrorist may be another of our society’s infrastructures, and the

terrorist can either launch or exacerbate the attack by exploiting the IT infrastructure, or use it to interfere with attempts to achieve a timely and effective response. Thus, IT is both a target and a weapon that can be deployed against other targets.

A terrorist attack that involves the IT infrastructure can operate in one of three different modes. First, the attack can come in "through the wires" alone. Second, it can include the physical destruction of some IT element, such as a critical data center or communications link. Third, the attack can rely on the compromising of a trusted insider who, for instance, provides passwords that permit outsiders to gain entry. All of these modes are possible and, because of the highly public nature of our IT infrastructure and of our society in general, impossible to fully secure. Nor are they mutually exclusive—and in practice they can be combined to produce even more destructive effects.

Most of the nation's civil communications and data network infrastructure offer soft IT targets, but they tend to be localized either geographically or in mode of communication, and if no physical damage is done tend to be recoverable in a relatively short time. One can imagine the use of IT as the weapon in a series of relatively local attacks that are repeated against different targets—banks, hospitals, or local government services—so often that public confidence is shaken and significant economic disruption results. This report is focused on catastrophic terrorism, and the committee's analysis is aimed at identifying those threats in particular and proposing S&T strategies for combating them. Of course, serious efforts are needed to employ security technologies that research might generate to harden all elements of the IT infrastructure to reduce the damage potential for such repeated attacks.