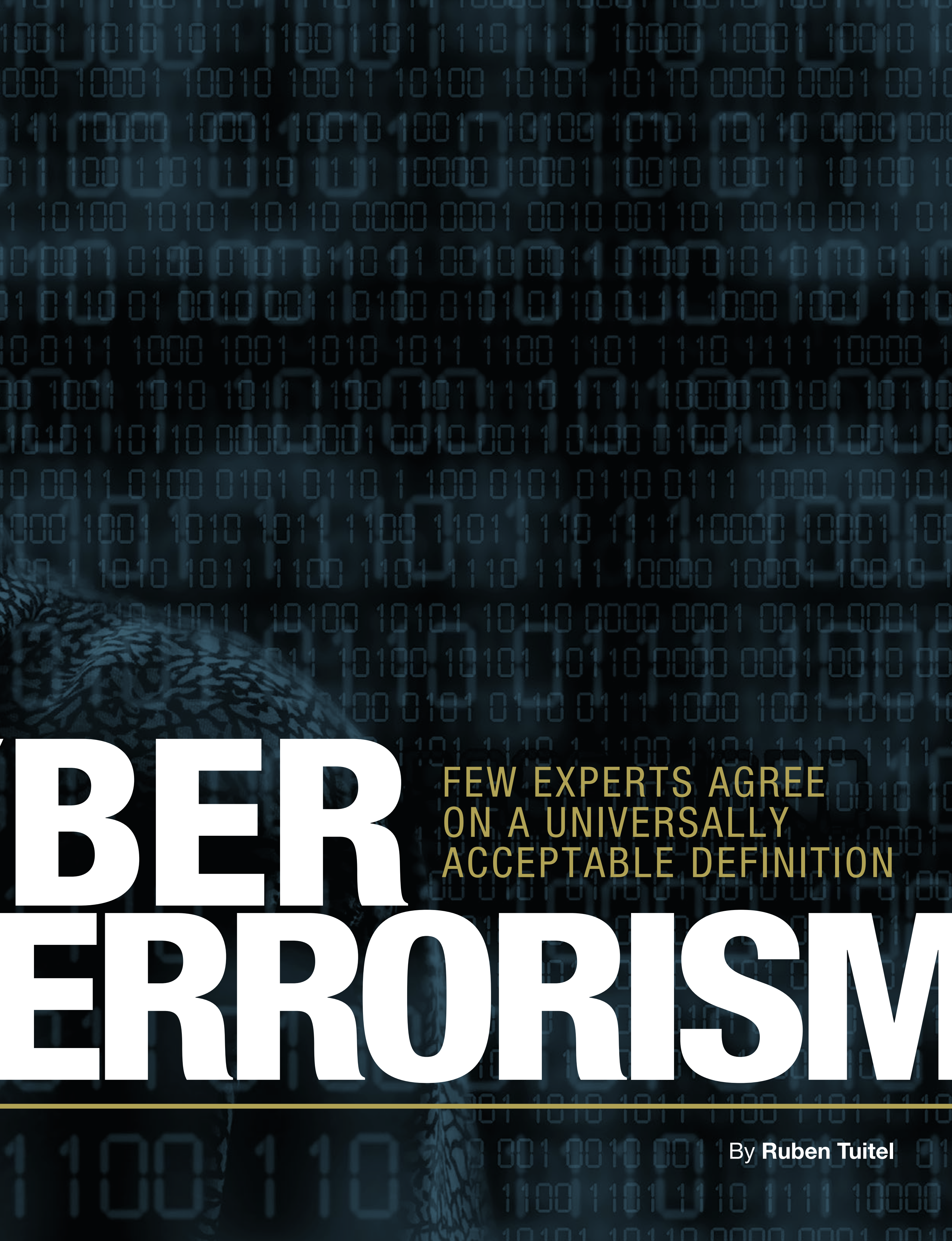
ISTOCK

Defining CY
T



BER ERRORISM

FEW EXPERTS AGREE ON A UNIVERSALLY ACCEPTABLE DEFINITION

By **Ruben Tuitel**

Cyber terrorism is a difficult phenomenon for scholars, legal practitioners and international organizations to define. Additionally, confusion exists over the differences between cyber crime and cyber terrorism. While this article is focused on cyber terrorism, I will briefly discuss cyber crime to highlight the differences. Existing cyber terrorism definitions leave room for debate; therefore, I have proposed my own definition: Cyber terrorism is the use of cyberspace by a nonstate entity to disrupt computer systems, causing widespread fear or physical damage and, indirectly, bodily injury, or causing disruption to such an extent that the credibility of the victim is seriously threatened, in furtherance of political, ideological or religious objectives.

CYBER ATTACK DEFINITIONS

Possible scenarios that resemble a cyber attack include a virus that scrambles financial records or incapacitates the stock market, a false message that causes a nuclear reactor to shut down, or an air traffic control system disruption that results in airplane crashes. Knowing the definition of a cyber attack is essential to differentiate it from cyber terrorism. Although there are many cyber attack definitions, a few are listed below.

The U.N. Office on Drugs and Crime describes a cyber attack as:

> "Cyber terrorism generally refers to the deliberate exploitation of computer networks as a means to launch an attack. Such attacks are typically intended to disrupt the proper functioning of targets, such as computer systems, servers or underlying infrastructure, through the use of hacking, advanced persistent threat techniques, computer viruses, malware, phlooding or other means of unauthorized or malicious access."

In the Joint Doctrine for Information Operations by the U.S. Joint Chiefs of Staff, cyber attacks are:

> "… deliberate actions to alter, disrupt, deceive, degrade, or destroy computer systems or the information they hold."

The Oxford Dictionary defines a cyber attack as:

> "An attempt by hackers to damage or destroy a computer network or system."

Mauno Pihelgas, researcher at the NATO Cooperative Cyber Defence Centre of Excellence in Estonia, defines a cyber attack in the chapter he wrote for the book *Peacetime Regime for State Activities in Cyberspace*, as:

> "… the term attack is considered to be any attempt to destroy, expose, alter, disable, steal, or gain unauthorised access to or make unauthorised use of anything that has value to an organization."

Defining cyber terrorism is more complicated. There are numerous aspects that make it difficult to determine whether a cyber attack can be labeled as cyber terrorism. However, before discussing this, it is important to understand the characteristics of terrorism.

The following characteristics of terrorism, as described in Bruce Hoffman's book, *Inside Terrorism*, are generally accepted. By distinguishing terrorists from other types of criminals and irregular fighters, and terrorism from other forms of crime and irregular warfare, we come to appreciate that terrorism is:

- Ineluctably political in aims and motives.
- Violent — or equally important — threatens violence.
- Designed to have far-reaching psychological repercussions beyond the immediate victim or target.
- Conducted either by an organization with an identifiable chain of command or conspiratorial cell structure (whose members wear no uniform or identifying insignia), or by individuals or a small collection of individuals directly influenced, motivated or inspired by the ideological aims or example of some existent terrorist movement and/or its leaders; and perpetrated by a subnational group or nonstate entity.

DEFINING CYBER TERRORISM

Attribution

For a cyber attack to be regarded as cyber terrorism, it must have been conducted by a terrorist group. This is a matter of attribution, and attributing a cyber attack is difficult. Unlike the real world, cyberspace does not recognize country borders. An Internet user in Country A can buy a product in Country B without realizing he is buying a product in a foreign country. Additionally, it is possible for an Internet user to work through different IP addresses using "proxies" to conceal one's identity online or make use of an anonymous Internet browser such as Tor, and the so-called Deep Web — the "hidden Internet," as detailed in a 2001 white paper published in *The Journal of Electronic Publishing*. Pedophiles have been known to use the latter two to share pornographic pictures and videos, making it difficult for law enforcement agencies to identify and locate them, an article in *The Telegraph* reported in 2012.

UNLIKE THE REAL WORLD, CYBERSPACE DOES NOT RECOGNIZE COUNTRY BORDERS.

Another method of concealing one's identity online is using a virtual private network (VPN). It is often used to connect to company networks from outside the office, enabling employees to work with internal company assets without being exposed directly to the Internet, and thus, possible malicious users, Pihelgas wrote. Setting up a VPN is relatively easy and could be abused by malicious actors since their Internet traffic would be encrypted. "Backtracing," also called backtracking, involves a technical process using "traceroute" tools to acquire the IP address of the attacker. Law enforcement agencies use the process to determine whether the attack was done by a group of hackers or an individual.

However, there is no such thing as complete anonymity on the Internet. Backtracing should, in theory, always lead to the perpetrator. But, law enforcement agencies can misattribute, meaning that someone who isn't involved in the cyber attack is falsely accused. This makes backtracking a difficult task for law enforcement agencies. Pihelgas explains:

> "With the evolution of different anonymity techniques, the difficulty of attribution is one of the primary challenges in reducing the overall insecurity originating from cyberspace and in tracing specific malicious actors. Accurate attribution is required to respond to cyber incidents in both the operational and legal terms. Misattribution is a contrariwise problem, where an attack is made to appear to have originated from another source (incriminating someone else). In addition to slowing down correct attribution, this can result in risky situations where the blame is attributed to an innocent individual, organisation or country. Consequences can vary from conflicts and mistrust between parties to embarrassing incidents becoming public."

Violence in cyberspace

One characteristic of terrorism is violence, or the threat of violence. The World Health Organization defines violence as: "The intentional use of physical force or power, threatened or actual, against oneself, another person, or against a group or community that either results in or has a high likelihood of resulting in injury, death, psychological harm, maldevelopment or deprivation." However, cyberspace is a virtual world — a space of computers, servers, modems and the Internet — so it is questionable whether any violence occurs. While the Stuxnet virus was capable of damaging the centrifuges of the nuclear plant in Iran, no direct physical force damaged the machines. The cyber attack affected a computer system, which led to physical damage. A truck bomb, for instance, results in direct physical damage, while Stuxnet required an extra step to achieve physical destruction. But what

about violence in cyberspace — digital attacks that are initiated from a cyber element aimed at disrupting another cyber, or virtual, element? To bridge the gap between the physical and the virtual world in terms of violence, it is necessary to distinguish between physical violence and cyber violence. Necessary definitions could also include physical cyber attacks and virtual cyber attacks or physical cyber terrorism and virtual cyber terrorism.

Cyber terrorism vs. cyber crime

Distinguishing between criminal and terrorist acts in cyberspace, as well as other malicious activities, is challenging. Creating a clear distinction between different forms of malicious cyber activities is important for the investigation and prosecution of these crimes.

Cyber crimes are seen as the digital versions of traditional crimes, according to a 2013 Congressional Research Service report titled *Cybercrime: Conceptual Issues for Congress and U.S. Law Enforcement*. For instance, identities can be stolen by hacking into customer databases of online shops, while the traditional criminal had to physically steal a wallet. Other cyber crime examples include credit card fraud, hacking company systems, and distributing and/or watching child pornography. Next to that, the activities of cyber criminals are different from those of cyber terrorists because they pursue a different goal and have different motivations. Cyber criminals are motivated by profit and involve crimes such as acquiring money or stealing information that can be sold, according to a 2010 report.

Terrorists, and thus cyber terrorists, are motivated by ideology, according to an International Centre for Political Violence and Terrorism Research article, or a political opinion that involves crimes that are more damaging to society and instill fear and anxiety. Yet, it also seems as if crime and terrorism are converging. The main source behind terrorist operations is money. Without that, it becomes almost impossible to acquire the materials needed to carry out an attack. To finance their actions, terrorists resort to crime such as drug trafficking, but they also make use of digital sources. This convergence however, would also make it increasingly difficult to classify a person as either a criminal or a terrorist.

The difference between cyber crime and cyber terrorism is quite clear; however, it is difficult for law enforcement agencies to expose the perpetrator's identity and the motivation behind an attack in the cyber world, and therefore determine whether the attack was crime or terrorism.

DISTINGUISHING BETWEEN CRIMINAL AND TERRORIST ACTS IN CYBERSPACE, AS WELL AS OTHER MALICIOUS ACTIVITIES, IS CHALLENGING.

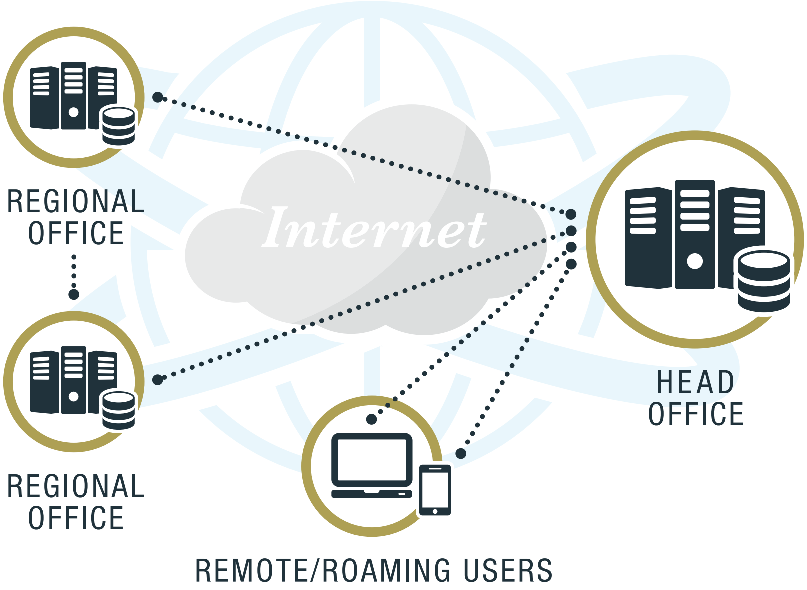
Terrorists seek attention

Less difficult, but still worth mentioning, is that terrorists and other nonstate entities often seek attention from the public. Terrorists want governments to know that the bomb explosion or airplane crash was their responsibility and that they conducted the attack for ideological or political reasons. Terrorists inform the public by posting a YouTube video or sending a "tweet" on their Twitter account, *The Daily Mail* reported. However, so far there is little evidence that a terrorist group such as al-Qaida has committed a cyber attack that caused significant damage. Terrorists may not yet have the knowledge and experience to attack a high-value target, or cyberspace is too covert for them. While cyber attacks are capable of disrupting critical infrastructure such as banks, a truck bomb is probably more destructive and might even be cheaper. Besides, a truck bomb makes a bigger impact on the public and has larger psychological repercussions. Therefore, it is questionable whether cyberspace is attractive enough for terrorists. However, there are several

BANKS *are* POPULAR TARGETS

Banks are popular targets for hackers. Common cyber attacks are distributed denial of service (DDoS) and spear phishing. Both aim to acquire information from clients, which is used to gain more information by calling customer service. Eventually the hackers ask for money transfers. Hackers time this so the DDoS attacks serve as a distraction so they can make use of the overburdened customer service employee. While this does not reach the level of cyber terrorism, banks are a critical aspect in every society. If they fail to operate, many businesses will not be able to continue their daily affairs, which will harm an economy.

VIRTUAL PRIVATE NETWORK (VPN)



The VPN connection is encrypted and protected from the public Internet.

PER CONCORDIAM ILLUSTRATION

Source: http://www.bankinfosecurity.com/banking-cyber-attack-trends-to-watch-a-6482/op-1

scenarios in which a cyber attack could be classified as cyber terrorism, such as an attack on a national electricity system.

POSSIBLE CYBER TERRORISM?

Critical infrastructure and industrial control systems are attractive targets. Failure or disruption could lead to casualties and have a substantial psychological impact. Marc Elsberg describes a worst case scenario in his 2012 book *Black Out*:

> "Cyberterrorist hackers have gained access to TenneT B.V. control systems, the national electricity transmission system operator of the Netherlands, responsible for supplying electricity to the Netherlands and part of Germany. A few hours ago, hackers shut down the electrical grid with a distributed denial-of-service attack which caused a country-wide electrical outage. Hospitals, increasingly dependent on digital systems for patient care are not able to treat patients properly, which leads to a large number of deaths. Emergency services cannot be reached, and communication lines are down. Citizens have no idea what is happening, and while the outage seemed rather innocent in the first few hours, people now are beginning to panic. The authorities are investigating, if possible at all, and only help people needing emergency treatment. Water refinery systems are shut down, which leads to low quality drinking water. The food industry is disrupted, eventually leading to food shortages. It is highly likely that people will soon begin to loot in order to survive."

EXISTING DEFINITIONS OF CYBER TERRORISM

In 2000, information security expert Dorothy E. Denning, when testifying before the U.S. House of Representatives' Special Oversight Panel on Terrorism, defined cyber terrorism as:

> "… the convergence of terrorism and cyberspace. It is generally understood to mean unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyber terrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, plane crashes, water contamination, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyber terrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not."

Denning's definition is quite complete and includes many facets. She states that an attack and "threats of attack" should result "in violence against persons or property," and "attacks that lead to death or bodily injury … would be examples." However, an attack by a nonstate entity is not mentioned. This would mean that the Stuxnet attack by the U.S. and Israel could be regarded as a cyber terrorist attack or even an act of war, based on international law.

Kevin Coleman, an information security expert, defines cyber terrorism as:

> "… the premeditated use of disruptive activities, or the threat thereof, against computers and/or networks, with the intention to cause harm or further social, ideological, religious, political or similar objectives. Or to intimidate any person in furtherance of such objectives."

This definition covers intimidation and the use or threat of "disruptive" activities. Also, this definition does not state that the attack needs to be committed by a nonstate entity.

An article in the *Information Security Journal: A Global Perspective* titled "How can we deter cyber terrorism?" defines cyber terrorism as "an activity implemented by computer, network, Internet, and IT intended to interfere with the political, social, or economic functioning of a group, organization, or country; or to induce physical violence or fear; motivated by traditional terrorism ideologies."

This final example of a cyber terrorism definition comes closest to the original definition of terrorism. It differs in that it describes the use of computers and other IT devices to conduct an attack. Coleman and Denning both define cyber terrorism as being directed against computers, not through the use of them. This is a good example of how definitions on cyber terrorism differ. *Information Security Journal* implies that computers and other IT devices are used as an instrument to commit a terrorist act.

LEAVING THE CONCEPT OF CYBER TERRORISM?

The term "cyber terrorism" may not be appropriate for describing large-scale cyber attacks. The word "terrorism" is used mostly when attacks have killed people or destroyed buildings. Considering that this has not happened thus far, the term "terrorism" should not be used to describe large cyber attacks. There should be a clear distinction about whether cyber terrorism is meant to target computers, uses computers, or both.

Lee Jarvis and Stuart Macdonald also question the use of the term "cyber terrorism" in their 2014 journal article published in *Perspectives in Terrorism*: "Perhaps the best illustration of this boundary problem can be found in debates over whether it is ever appropriate, useful or desirable to describe state violence of any sort as terrorist." The same applies to cyber terrorism. We coin new words and

terminologies for things that might already exist that causes confusion: “This profusion of new terminologies throws up considerable challenges for clarifying terms such as cyber terrorism. Not least amongst these is the inconsistent and interchangeable use of such terms whereby, as [Gabriel] Weimann [of the U.S. Institute of Peace] illustrates: ‘… the mass media frequently fail to distinguish between hacking and cyber terrorism and exaggerate the threat of the latter.’ ” This “profusion of new terminologies” is important to consider when determining a cyberterrorism definition.

SIMILAR STUDY

Research findings from another study by Jarvis and Macdonald, summarized in the article “What is cyber terrorism? Findings from a Survey of Researchers” also address how to describe cyber terrorism. Their study involved a survey of 118 researchers and focused on three definitional issues: (a) the need for a specific definition of cyber terrorism for either policymakers or researchers; (b) the core characteristics or constituent parts of this concept, and (c) the value of applying the term “cyber terrorism” to a range of actual or potential scenarios. Jarvis and Macdonald conclude that while most researchers believe a specific definition of cyber terrorism is necessary for academics and policymakers, disagreement on what this might look like has the potential to stimulate a rethinking of terrorism more widely.

THERE SHOULD BE A CLEAR DISTINCTION ABOUT WHETHER CYBER TERRORISM IS MEANT TO TARGET COMPUTERS, USES COMPUTERS, OR BOTH.

PROPOSING A DEFINITION

Existing definitions of cyber terrorism are quite complete, but leave room for debate. Therefore, I would like to contribute to this discussion by restating my definition: Cyber terrorism is the use of cyberspace by a nonstate entity to disrupt computer systems, causing widespread fear or physical damage and, indirectly, bodily injury, or causing disruption to such an extent that the credibility of the victim is seriously threatened, in furtherance of political, ideological or religious objectives. This definition covers the more essential parts of the term terrorism, such as fear, physical violence and the range of motives, but also the cyber part, by using computers to target computers.

CONCLUSION

While much more can be written on cyber terrorism, this article has shed light on the difficulty of defining it and encourages further discussion. Questions exist on violence in cyberspace and whether it comprises the mere use of the Internet by terrorists. Attributing an attack is probably the most difficult task and can lead to problems for law enforcement agencies. It is important to note that we may never reach a universal definition. Reaching an acceptable definition of cyber terrorism is also dependent on the definition of terrorism, which is still subject to discussion.

But if renowned terrorism experts like Walter Laqueur and Alex Schmid, who both studied hundreds of definitions of terrorism, cannot come to a universally acceptable definition, then who can? Perhaps the term cyber terrorism should not be used to define a disruptive cyber attack. With any luck we can achieve an understanding that improves international cooperation on the difficult subject of terrorism and cyber terrorism. Defining cyber terrorism thus seems to be a real dilemma. □