The Importance of Defining Cyber Terrorism

By Paul de Souza

The primary purpose of covering this topic is to be able to effectively provide national security professionals with a better understanding of cyber terrorism by compiling and extracting sound knowledge from scholars of the subject in an effort to determine an appropriate, comprehensive definition of cyber terrorism. It is vital to present a clearer view of cyber terrorism as a practical contribution to the national security community.

A study covering current definitions of cyber terrorism by different organizations and how they complement one another can lead the national security professionals to have a better understanding of the reality of cyber terrorism. Finding the cause of such variety of definitions and lack of doctrinal documentation on the subject of cyber terrorism alone can be challenging. This becomes even more challenging when linked to the American national security apparatus and how the various agencies deal with the alleged threat of cyber terrorism.

The United States of America has been challenged with new terror tactics in cyberspace from its adversaries. Many of these new tactics have never been seen before, which means they are not very well understood, particularly when they become increasingly sophisticated. “The modern thief can steal more with a computer than with a gun. Tomorrow’s terrorist may be able to do more damage with a keyboard than with a bomb.”[1] The notion of cyber terrorism goes back to the early nineties, which can be quite surprising. Much progress has been made in cyberspace not only as a way to communicate but also as a way to cause physical damage to systems and people. The National Research Council does not use the term “cyber terrorism” per se, but it gives the reader a look into the future of terrorists using the keyboard to do damage. Cyber terrorism is an unpredictable act. Much like what can be seen in the physical domain when referring to terrorism, the same reality can apply to the cyber domain in terms of unpredictability. However, in the physical domain, a better understanding exists on how to predict and/or counter physical terror attacks, which is often due to the knowledge provided from intelligence sharing. Although strides are being made daily, this type of intelligence collaboration does not really apply yet to the cyber environment as it relates to terrorism, and in order to have better situational awareness, first of all, there needs to be a better, clearer, more concise definition of what cyber terrorism would be, and just as important, there needs to be an understanding of how such definitions can be used in a court of law for prosecution.

Much talk about cyber terrorism exists in the cyber security community as well as in the intelligence community. The use of cyberspace for power projection is already well defined by the Department of Defense, but not much doctrine can be found on the subject of cyber terrorism. The definition of cyber terrorism seems to be very fluid, and determining how much fear or loss of life cyber attacks can create on the American populace is a difficult task. Having a better understanding of cyber terrorism and how it relates to American national security would be beneficial to readers and professionals dealing with terrorism in general.

Cyber Terrorism and the Art of the Possible

Cyber terrorism should basically touch on two main targets in order to be called a cyber terrorism activity: loss of life and destruction of national critical infrastructure with enough disruption and destruction of systems and information to cause a nation to stop functioning in the service of its citizens. One important element of cyber terrorism is fear. Fear should be a core element of cyber terrorism. Much like North Korea threatening movie goers in America through cyber means not to go see the movie "The Interview" with the consequence of people being killed at the movie theaters. In this example, there is a nation, North Korea, making use of cyberspace to compromise systems from Sony (a Japanese company) and making use of cyberspace to disrupt the way of life of Americans. The use of cyberspace as a tool of terror can be identified as a tool of terror. There are many examples of critical infrastructure being attacked by hackers with the intent of disruption and possibility of destruction. The next step up and the threshold that would make these attacks cyber terrorism would be ultimately the loss of life.

Cyber Terrorists would need to follow a similar strategy followed by the US military and US agencies to be able to deploy their cyber attacks with the intent to cause terror. These skills and preparations are in the art of the possible by nation states and even smaller terror groups. Cyber terrorists would need to consider the following:

- Train to acquire the needed skill sets across all levels of organizational responsibility, from applier to manager.
- Training needs to include integrating all cyber terrorist skill sets into a cohesive, mutually reinforcing effort.

Leadership (management) is the glue that holds cyber terrorists together and drives them to reach the desired end state: to deploy cyber attacks in order to destroy and disrupt critical infrastructure, with the intent of killing or injuring people (soft targets), to ultimately cause fear which leads society to change their normal life activities.

The cyber training and capabilities to accomplish such tasks are available to anyone globally with enough technologies to make it all non-attributable. The threat is real but the response to the threat should be equally real and at the current political stage in the United States legislation is behind technology.

Proposed Cyber Terrorism Definition

Based on the author's observations and research a more appropriate recommended definition of cyber terrorism should follow some core components:

- A better explanation of cyberspace as a conduit of terror activities.
- A clear identification of how cyberspace can be used to cause destruction, interception and disruption of national critical infrastructure with the appropriate definition of critical infrastructure by actors with the intent of causing terror and disruption of societal normal activities.
- How indicators of cyber terrorism should be shared with vetted parties and allies.
- How standard US code for domestic and international cyber terrorism applies to cyber.

Military Response

From the Department of Defense's side of the house, cyber terrorism should be seen as any other cyber aggression from a nation state or individual(s) against the DODIN or national critical infrastructure following the normal Title 10 response with all its legal approvals and authorities. A better definition of cyber terrorism can help the DOD augment its responses kinetically or through the wire in the form of cyberspace operations. The DoD in partnership with the IC should be able to leverage Title 50 to take full advantage of a more swift response to cyber terrorism. The FBI and law enforcement agencies should be included as part of the effort thus creating the whole-of-government approach.

[1] National Research Council. Computers at Risk: Safe Computing in the Information Age, 1991, http://www.nap.edu/read/1581/chapter/3(accessed September 10, 2018).

Mr. de Souza is the co-author of the book Strategic Intelligence Management (National Cyber Defense Strategy), he serves as an advisor for the Military Cyber Professionals Association (MCPA), and he is a recipient of the Order of Thor Medal. Paul serves as a Centre of Excellence in Terrorism, Resilience, and Intelligence & Organized Crime Research (CENTRIC) Visiting Researcher at Sheffield Hallam University in the UK, Negev Hi-Tech Faculty Startup Accelerator Advisor, Ben-Gurion University of the Negev, Israel, Guest Lecturer at The Swedish Defence University (SEDU) Försvarshögskolanand, Institute of World Politics (IWP) Board of Advisors for The Cyber Intelligence Initiative (CII) in Washington, DC, and served as a Visiting Research Fellow at the Institute for National Security Studies (IN/SS) at Tel Aviv University in Israel – Cyber Security and Military & Strategic Affairs Programs. Mr. de Souza has over 18 years of cyber security experience and has worked as the Chief Security Engineer for AT&T, where he designed and approved secure networks for MSS (Managed Security Services). Mr. de Souza also worked for Computer Sciences Corporation (CSC) and US Robotics as a security engineer. He was the winner and recipient of the International Cyber Security & Intelligence Conference (ICSIC) 2017 Award from Ontario, Canada. Mr. de Souza has a Masters in National Security Studies (MA) with a concentration in Terrorism from American Military University, West Virginia WV.

The author is also founder of The Cyber Security Forum Initiative (CSFI), a MCPA partner, found at https://csfi.us