ARI 47/2020
17 April 2020

Cyber Terrorism: Why it exists, why it doesn't, and why it will

Stefan Soesanto | Senior Researcher, Cyber Defense Team, ETH Zurich | @iiyonite

Theme

While the discussion on cyber terrorism research and related government policies have hit a wall in recent years, adversarial tactics to create terror in and through cyberspace are only at their beginning.

Summary

For more than two decades, the idea of cyber terrorism has survived in the absence of a concise definition and rigorous case-studies that prove its actual existence. Many researchers have moved the ball forward over the years by investigating –among others topics– whether cyber terrorism is a real or imagined threat, which actors can conduct cyber terrorism, what the motivations behind an act of cyber terrorism might be, and whether terrorism logics in real-space hold true in cyberspace.[1] This article is not going to revise this existing knowledge. Instead, it seeks to explain different government logics on the defensive end for buy-into the cyber terrorism narrative and outline operational thinking on the offensive end to create terror as a desired outcome.

Analysis

The conversation on cyber terrorism began in the late-1990s amidst a wave of high-profile terrorist attacks in the United States, including the bombing of the World Trade Center in 1993 and the Oklahoma bombing in 1995. By 1997, the US Department of Defense conducted its first ever no-notice information warfare exercise to test the cybersecurity of its own systems, and in the same year, the Marsh Commission report on critical infrastructure protection put the growing cyber threat landscape on the policy map in Washington.[2] Following the simultaneous bombings of the US embassies in Kenya and Tanzania in 1998 and the subsequent rise of al-Qaeda, terrorist attacks in and through cyberspace were seen as a potential future threat vector to the homeland. In October 1999, the Naval Post Graduate School prepared the first and to date most comprehensive study on 'cyberterror' for the US Defense Intelligence Agency.

[1] See: Gabriel Weimann, 'Cyberterrorism – How real is the threat', United States Institute of Peace, Special Report 119, December 2004, https://www.usip.org/sites/default/files/sr119.pdf; Zahri Yunos and Sharifuddin Sulaman, 'Understanding Cyber Terrorism from Motivational Perspectives', *Journal of Information Warfare*, Vol. 16, No. 4 (Fall 2017), pp. 1-13; Maura Conway, 'Reality Bytes: Cyberterrorism and Terrorist 'Use' of the Internet', *First Monday*, Vol. 7, No. 11-4, November 2002, https://firstmonday.org/ojs/index.php/fm/article/download/1001/922.

[2] 'Critical Foundations. Protecting America's Infrastructures', October 1997, https://fas.org/sgp/library/pccip.pdf.

The 1999 study included numerous definitions and statements that outlined the contours of cyber terrorism research. The authors for example noted that "*terrorist use of information technology in their support activities does not qualify as cyberterrorism*." Similarly, they also excluded script kiddie techniques, including dictionary attacks, spoofed emails, and the bombardment of e-mail inboxes. Overall, the study narrowly defined cyber terrorism as "*the unlawful destruction or disruption of digital property to intimidate or coerce governments or societies in the pursuit of goals that are political, religious or ideological*."[3] For a study compiled in 1999, this was a well-rounded framework. The only problem was that, in the United States, all cases that could theoretically fit the profile are statutorily considered either acts of cybercrime acts under the Computer Fraud and Abuse Act (18 U.S.C. 1030), or deemed armed attacks/acts of aggression under international law that would trigger the entire toolbox of US national defense mechanisms. For the last 20 years, cyber terrorism researchers have unsuccessfully tried to carve out their own space that could stand apart from cybercrime, hacktivism, and offensive military cyber operations. It should thus not come as a surprise that, writing in 2012, Jonalan Brickey still had to explain that cyberterrorism could be defined as "*the use of cyber to commit terrorism*," or characterized as the "*use of cyber capabilities to conduct, enabling, disruptive, and destructive militant operations in cyberspace to create and exploit fear through violence or the threat of violence in the pursuit of political change*."[4] Similarly in 2014, Daniel Cohen literally wrote a book chapter on 'cyber terrorism: case studies' in which all examples are either cases of hacktivism, cybercrime, or nation state operations.[5]

Different government approaches

With cyber terrorism research hitting a wall very early on, some notions of cyber terrorism were nonetheless picked up by governments and agencies alike. 7000 miles away from Washington D.C., the Japanese government embarked on its mission to combat what it termed 'cyber terror' in the year 2000, when a combination of cyber-linked incidents caused by Japanese left-wing extremists, Chinese nationalistic hacktivist, and the Aum Shinrikyo doomsday sect, shook the public's confidence. In December 2000, Tokyo implemented an Special Action Plan which defined cyber terror as "*any attacks using information and communication networks and information systems that could have a significant impact on people's lives and socio-economic activities*."[6] In practice, this included everything from DDoS attacks, and the defacement of websites, to the deployment of highly advanced tooling like Stuxnet. Curiously, today, Japan's National Police Agency literally uses these three categories to officially define cyber terror.

[3] Defense Intelligence Agency, 'Cyberterror. Prospects and Implications', pp. 10 and 9, respectively https://www.hsdl.org/?view&did=442884.

[4] Jonalan Brickey, 'Defining Cyberterrorism: Capturing a Broad Range of Activities in Cyberspace', *CTC Sentinel*, August 2012, Vol. 5, No. 8, p. 6, https://ctc.usma.edu/wp-content/uploads/2012/08/CTCSentinel-Vol5Iss81.pdf.

[5] Daniel Cohen, 'Cyber terrorism: Case studies', in *Cyber Terrorism Investigator's Handbook*, Chapter 13, https://www.sciencedirect.com/science/article/pii/B978012800743300013X.

[6] Prime Minister's Office, 'Special Action Plan for Cyber Terrorism Countermeasures for Critical Infrastructure', December 15, 2000, https://japan.kantei.go.jp/it/security/2001/cyber_terror.pdf.

For the Japanese government the primary motivation to introduce the term cyber terror was to mobilize government resources and secure the buy-in from critical infrastructure providers to build-out the nation's cybersecurity posture. Cyber terror was thus initially not viewed as a specific form of cybercrime or a distinct area of national defense but was more aching to a natural hazard that could negatively affect society as a whole. Over the years, the cyber terror narrative naturally crumbled as more precise definitions, distinctions, and insights degraded the terrorism aspect. Notwithstanding these developments, the term is still widely used in Japan and has practical implications for public-private cooperation. For example, the National Police Agency's 'Cyber Terrorism Countermeasure Councils' facilitate public-private partnerships and outreach on the prefecture level through discussions, lectures, and demonstrations. Meanwhile the 'Cyber Terrorism Countermeasures Council,' maintained by the Tokyo Metropolitan Police, serves a coordinating hub to secure all big events in Japan –including the 2021 Tokyo Olympics and Paralympics.

In the United States, the attacks on 9/11 introduced a host of legislative measures to tackle the threat of cyber terrorism. Stand out from the crowd are the US Patriot Act of 2001 and the Terrorism Risk Insurance Act of 2002. The Patriot Act provided federal law enforcement new tools to detect and prevent terrorism, including the "*authority to intercept wire, oral, and electronic communications relating to computer fraud and abuse offenses*" (Section 202), "*emergency disclosure of electronic communications to protect life and limb*" (Section 212), and "*interception of computer trespasser communications*" (Section 217).[7] According to the Department of Justice's 2005 Report, Section 202 was used on only two occasions which both "*occurred in a computer fraud investigation that eventually broadened to include drug trafficking*."[8] Meaning, it was never used to tackle a case of cyber terrorism. By contrast, section 212 was used, according to the DoJ's 2004 Report to "*successfully respond to a cyberterrorist threat to the South Pole Research Station.*"[9] While it is indeed true that in May 2003 Romanian hackers intruded into the network of the National Science Foundation's Amundsen-Scott South Pole Station and threatened to "*sell the station's data to another country and tell the world how vulnerable* [the systems] *are*," the DoJ's 2004 Report falsely claims that "*the hacked computer also controlled the life support systems for the South Pole Station*.".[10] In fact, this dramatic detail was not included in any of the FBI's public releases and according to internal memos, the station's network was "*purposely* [less secure] *to allow for our scientists at this remotest of locations to exchange data under difficult circumstances*," and was penetrated two months prior by another hacking group. When it comes to section 217 of the Patriot Act, under which "*victims of hacking and cyber-terrorism* [could] *now obtain law enforcement assistance in catching intruders on their systems*," neither the DoJ's 2004 nor the 2005 report offer any known connection to a cyber terrorism case. Instead, the Sunsets Report merely points out that section 217 was used in "*investigations into hackers' attempts to compromise military computer systems*" and

[7] Public Law 107–56, October 26, 2001, https://www.sec.gov/about/offices/ocie/aml/patriotact2001.pdf.

[8] Department of Justice, 'USA Patriot Act. Sunsets Report', April 2005, p. 6, https://www.justice.gov/archive/olp/pdf/sunsets_report_final.pdf.

[9] Department of Justice, 'Report from the Field: The USA Patriot Act at Work'. July 2004, p. 33, https://www.justice.gov/archive/olp/pdf/patriot_report_from_the_field0704.pdf.

[10] 'Report from the Field', p. 27.

serious criminal cases, such as "*an international conspiracy to use stolen credit cards*."[11] Overall, the DoJ's own reporting shows that even a law that specifically combats terrorism was not utilized to investigate one case of cyber terrorism.

In fact, the closest the DoJ has gotten to successfully prosecute an act of cyber terrorism was back in 2016, when 20-year old Ardit Ferizi –a citizen of Kosovo– was sentenced to 20 years in prison for "*accessing a protected computer without authorization and obtaining information in order to provide material support to ISIL*." and according to Assistant Attorney General for National Security John Carlin, "*this case represents the first time we have seen the very real and dangerous national security cyber threat that results from the combination of terrorism and hacking*." [12] But far from conducting an elaborate cyberattack, Ferizi only gained sys admin level access to a US company server that hosted the personally identifiable information of tens of thousands of US customers –including military personnel and government officials. Ferizi then proceeded to cull the data to approx. 1300 military and government individuals and forwarded it in June 2015 to Junaid Hussain –a former hacktivist and at the time ISIS' most prolific English-language social media propagandist. While Ferizi was subsequently arrested in Malaysia and extradited to the United States in October 2015, a US drone strike took out Junaid at a petrol station in Raqqa, Syria, in August.[13] The incident marked the first publicly known case of an enemy cyber operator being specifically targeted on the kinetic battlefield.

In contrast to the Patriot Act, the Terrorism Risk Insurance Act (TRIA) is a different animal. TRIA became necessary when following the 9/11 attacks, reinsurers began to exclude terrorist attacks from their coverage, with in turn forced insurance companies to excluded them, which I turn stalled development projects in their tracks due to the unavailability of terrorism risk coverage and uncertainty as to who would pay if another terrorist attack occurred. To ease the jitter, TRIA put in place a three-year Terrorism Insurance Program under which the US government would "*share the losses on commercial property and casualty insurance should a foreign terrorist attack occur, with potential recoupment of this loss sharing after the fact*."[14] The program has been reauthorized multiple times and is set to expire at the end of 2027. What makes TRIA important for the contextualization of cyber terrorism is that it does not specifically exclude cyber terrorism nor generally includes it from coverage. Meaning, the way terrorism is defined under TRIA would make it theoretically also applicable for every cyber incident if the Secretary of the Treasury, the Secretary of State, and the Attorney General of the United States, certify the incident to be act of terrorism or a "*violent act or an act that is dangerous to (I) human life; (II) property; or (III) infrastructure*." (Section 102). Complicating the matter further is that in 2016 the US Department of the Treasury issued a notice clarifying that cyber liabilities in cyber insurance policies are considered

[11] 'USA Patriot Act. Sunsets Report', p. 48.

[12] Department of Justice, 'ISIL-Linked Kosovo Hacker Sentenced to 20 Years in Prison', *Justice News*, September 26, 2016.

[13] Frank Gardner, 'UK jihadist Junaid Hussain killed in Syria drone strike says US', *BBC News*, August 27, 2015.

[14] Congressional Research Service, 'Terrorism Risk Insurance. Overview and Issue Analysis', December 27, 2019, p. summary, https://crsreports.congress.gov/product/pdf/R/R45707.

"property and casualty insurance" under TRIA. Meaning, cyber terrorism coverage cannot be excluded from any cyber insurance policy. Now, given that many insurers have chosen to exclude acts of war and other items from their cyber insurance policies, cyber terrorism faces a fundamental theoretical conundrum. Let's assume for a moment we would ask our insurance company to draw up a cyber insurance that does not cover anything. Nothing at all. Let us also assume that a cyber incident occurs, and the US government classifies it as an act of terrorism. Would my cyber insurance –which does not cover anything– still have to cover the incident under TRIA? If true, then is an act of cyber terrorism only cyber terrorism when the US government says it is? Similarly, how would an insurance company correctly price my cyber insurance premium? Would they sell it to me for almost nothing, since it does not cover anything, or would the probability of a cyber incident being identified by the US government as an act of cyber terrorism form the baseline for the premium calculation?

Apart from the US and Japan, numerous other governments have sporadically incorporated the term cyber terrorism into their strategic documents for one reason or another. Austria's 2013 Cyber Security Strategy for example defines cyber terrorism "*as a politically motivated crime of state and/or non-state actors.*"[15] And South Korea's 2012 Defense White paper specifically calls out "*various forms of cyber terrorism: Hacking, DDoS attacks, denials of service, logic bombs, Trojan horses, Worm viruses,* [High-Energy Radio Frequency] *guns etc*." [16] Looking at the variety of cyber terrorism interpretations out there, it ought to be obvious that from a strategic point of view, the conversation on cyber terrorism is all over the place everywhere. But what if we could introduce some sense of sanity into the discussion by operationalizing fragments of cyber terrorism to clarify what threat vectors we ought to be looking for? Let's give it a try.

Operational thinking

From an operational point-of-view, we have to treat an act of cyber terrorism as a black box, similarly to how first responders treat any incident affecting their network. Meaning, for our analysis it does not matter who is behind the attack. It could be a non-radicalized individual with no links to any terrorist organization. It could be a hardcore terrorist group that regularly interfaces with cybercriminals. Or it could be a nation state. Equally, because the attacker's political, religious, and ideological motivations remain largely hidden from us, the "*tie to terrorism may not reveal itself for days, weeks, or months, if ever.*"[17] Therefore our focus has to be on technical attribution e.g. (a) how did the attacker do it, (b) when did he do it, and (c) did he achieve his objective? Analytically, we are thus trying to discern whether the attack was targeted, coordinated, and persistent, rather than diffuse, opportunistic, and random.

[15] Federal Chancellery, 'Austria Cyber Security Strategy', 2013, https://www.bmi.gv.at/504/files/130415_strategie_cybersicherheit_en_web.pdf, p. 21.

[16] Ministry of National Defense, 'Defense White Paper', 2012, https://media.nti.org/pdfs/ROK_2012_White_Paper.pdf, p. 10.

[17] ISE Bloggers, 'Unpacking Cyber Terrorism', May 31, 2016, https://www.dni.gov/index.php/careers/careers-features/129-uncategorised/2497-unpacking-cyber-terrorism.

The second item we have to de-conflict is whether the attack actually terrorized the intended target. The reason for this is simple: Image there is a blackout affecting your entire neighborhood. Then the lights come back on for a moment –everyone is relieved– and then the lights go out again. There are numerous plausible explanations as to why the blackout occurred, and in most cases, those affected might never get to know the underlying reason after the incident is finally fixed. Now, compare that to a blackout that only affects your apartment. You go into the kitchen and your smart-light bulbs do not light up. You look at bulb, tinker around with your network, and search for possible fixes online, but you cannot locate the problem. Then suddenly, the lights go on… and switch off again. Which one of those two blackouts would terrify you more? Analytically, the only two differences that are important to us are: (a) the distance between the attacker and the intended target –e.g. how personal is it? –, and (b) the psychological resonance effect emanating from the attack –e.g. how "terroristic" is it.

Let's briefly showcase this with the help of one real-life case.

In 2007, then 14-year old Polish teenager Adam Dabrowski was struck by a combination of curiosity and evil ingenuity that led him to conduct nightly break-ins into the tram depot of the city of Lodz. His objective: figuring out how the tram network worked and whether he could control the trams remotely. Combined with months of online research and his electronic classes at school, Adam succeeded sometime in early-2008 in converting an old tv remote to exploit a flaw in Lodz' infrared based signaling system. Under the right circumstances –as Adam figured out – it was possible to capture the track switching signal at one junction point and play it back at another junction point to get the same result.[18] According to Miroslaw Micor, spokesman for Lodz police, Adam subsequently treated the Lodz tram network "*like any other schoolboy might a giant train set, but it was lucky nobody was killed. Four trams were derailed, and others had to make emergency stops that left passengers hurt. He clearly did not think about the consequences of his actions*."[19]

Now imagine if Adam would have continued his spree and would have never had been caught. Would this qualify as a case of cyber terrorism? From a strategic point-of-view it ticks several boxes. First, Adam succeeded in collecting actionable intelligence on a critical infrastructure target. Second, Adam was persistent enough to build a targeted exploit over month of dedicated work. And third, Adam did cause bodily harm by disrupting tram operations with his device. But what we are strategically lacking is any information on the attacker's motivation, his objective, and whether he is potentially connected to a terrorist cell. Meaning, Adam's campaign only becomes terrorism in case of self-attribution, e.g. if Adam leaves behind clues that explain his reasoning or a tape that shows him declaring his allegiance to a terrorist group.

[18] John Bull, 'You Hacked: Cyber-Security and the Railways', *London Reconnections*, May 12, 2017, https://www.londonreconnections.com/2017/hacked-cyber-security-railways/.

[19] John Leyden, 'Polish teen derails tram after hacking tram network', *The Register*, January 11, 2008, https://www.theregister.co.uk/2008/01/11/tram_hack/.

Operationally, we do not need any of that information. Technically, Adam's campaign fulfills the notion of targeted, coordinated, and persistent. But on the second pillar it notably falls short. In terms of how personal the attack was, our investigation would have to figure out whether there were any common targets in the trams that were derailed and whether the campaign had any major repercussions for the company that maintains the Lodz tram network. In both instances we will not find much. Similarly, given the low severity and frequency of the incidents, the fallout radius of the attack's psychological effect will be fairly small. To turn Adam –operationally– into a terrorist he would have to do one of two things: Either build more devices and get more people involved to increase the frequency and spread of the derailments. The downside of which is an expansion of trust, information sharing, and a decline in absolute control (e.g. outsourcing). Or, Adam could walk in the opposite direction by targeting specific trams at specific times to terrorizing specific individuals. Which would necessitate an information gathering operation aimed at mapping real-time target locations, habitual movement patterns, and potential insights into a target's social interactions (e.g. espionage).

In essence, by closing the proximity to the desired target and persistently engaging it over time, the modified campaign becomes the vehicle for the subsequent creation of terror –even though the individual attacks stay the same. Thus, rather than looking at the severity of a cyberattack, e.g. physical destruction and disruption –investigating attacker motivations, or question the feasibility of terrorism in cyberspace altogether, analyzing adversarial campaign tactics and maneuvering behavior will provide a much richer framework to explore, replicate, and defend against the terror component. Indeed, valuable lessons have yet to be learned from issues as disparate as cyber stalking and mental recovery after a cyber incident, to hacking back in the civilian realm and converging military cyber operations with information warfare campaigns.[20]

Conclusion

In sum, cyber terrorism is probably best viewed as an operational tactic aimed at a distinct psychological outcome rather than a field of research that connects the cyber domain at the hip to terrorism in real space. Notably, while cyber terrorism research and policy has hit somewhat of a deadlock in recent years, leveraging tactical approaches to create terror in and through cyberspace is only at its beginning.

[20] Ellen Nakashima, 'U.S. Cybercom contemplates information warfare to counter Russian interference in 2020 election', *The Washington Post*, December 25, 2019.