Cyber 9/11: Understanding the Current Reality of Cyberterrorism

Sean M. Sarich

The Pennsylvania State University

Author Note

This paper has been prepared for PLSC 439: The Politics of Terrorism, Sect 001, Fall 2019, instructed by Professor Christopher Cook.

Cyber 9/11: Understanding the Current Reality of Cyberterrorism

Given the rising cyber threat as a whole, there is a very limited amount of research that has been conducted with regard to the use of cyber-attacks by terrorist organizations. However, the terms *cyberterrorism* and *cyber 9/11* have been brandished by many in the national defense circles, most notably among those in the US, UK, and Canada who, largely due to alliances, are currently the most vocal on the topic. Examples cited in these cyberterrorism conversations range from terrorist recruiting efforts to the use of denial of service attacks as preemptive strikes emanating from major Western-state competitors like Russia and China to campaigns launched by hacktivist groups like *Anonymous*. In light of this broad range of sources and the fuzzy attribution appended to them, one might automatically assume that the immediate motion towards obvious Western competitors is simply the leverage of hawkish rhetoric at its finest. Though there could be at least some truth to that assumption given the competitive nature of national budgets, a fair question to ask in order to better appreciate such a clamor over this technical subgenre of terrorism might be: *what is cyberterrorism?*

While this question may seem obvious and easily overcome by a simple search engine query, the reality is that the information on the topic of cyberterrorism requires one to first parse many of the overt uses of the term *terror* and then to read beyond the assumption of false positives given the volume of what at first seems like a misuse of the cyberterrorism appellation. What emerges is the possibility of a paradigm shift, or at least a confluence of attributes, that makes it very difficult to differentiate between technified terrorist operations from state-to-state aggression. Given this fact and the evidence found in the following case study material, the cyber capability required by independent extremist groups to conduct a *cyber 9/11* style attack seems to be overstated. However, further evidence suggests that the resources afforded to state-sponsored

extremist groups blur this capability limitation and make it difficult to distinguish between terrorism by its classical definition from states seeking opportunist alliances with either terrorist groups or nationalist groups under terrorism-for-hire arrangements.

A Survey of the Political Rhetoric Pertaining to Cyber Terror

To curate a sample size of case study material for this cursory study in cyberterror—enough for test the above hypothesis—the doctrinal entries and political discourse of the earlier mentioned countries of the US, UK, and Canada shall be used in light of their somewhat shared information security concerns. The main goal of breaking down these shared yet nuanced goals of the listed countries is to identify the complex nature of cyberterrorism since, as with most things guised under the domain of the internet, attribution tends to be difficult and previous conventions like cybercrime and cyber warfare have emerged to add new meaning to old paradigms. The policy frameworks of each country offer a compelling explanation as to why cyberterrorism might be valid across belligerence genres as well as provides some small validation en masse to the new composite relationship that may exist between competing states and terrorist proxies.

US CYBER STRATEGY

The entirety of the US Cyber Strategy can be found on the Whitehouse.gov website where the technical security objectives of the United States are listed at length. Indeed, the vague acknowledgment of cyberterrorism is listed, most notably in the following block:

> "Non-state actors — including terrorists and criminals — exploited cyberspace to profit, recruit, propagandize, and attack the United States and its allies and partners, with their actions often shielded by hostile states" (2018, p.2).

While there is some hint to the previous assertion that alliances between hostile nations and terrorist organizations exist, the remainder of the document does not provide any sort of concrete example of these liaisons. Instead, it seems to form a shell of policy intentions around the idea that cyberterrorism is somewhat amorphous and that such arrangements are may be used to extend the capabilities of a terrorist organization in order to achieve a broader strategic goal.

UK CYBER STRATEGY

The UK's official stance on cyberterrorism is more clearly listed though much less sure over aspects of greater state liaisons. Mostly, the UK strategy points towards low-capability endeavors that aim to deface official internet sites or leak the information of personal officials to the internet. Likewise, the UK notes that the threat of these low-capability attacks is high and that given the disproportionate effects of cyber capabilities, even a modest uptick in technical means may lead to devastating outcomes. At this point, however, the overall capability of staging a crippling attack is thought to be low and outside of the current objectives of terrorist groups known to be using the internet as an attack vector (HM Government 2016). Though these groups are not listed, an external survey finds that the Islamic State has been linked to the aforementioned defacement and personal information leaks (Alexander and Clifford 2019).

CANADIAN CYBER STRATEGY

Canadian cybersecurity strategy is perhaps the vaguest of all of the official doctrines. The terms *terror, terrorist,* or *terrorism* are only mentioned twice in the entire text with the only substantial statement as follows: "Terrorist organizations are also interested in acquiring advanced cyber tools to conduct attacks" (Public Safety Canada 2019). The Canadian Cyber Security Strategy both completes yet continues the trend of ambiguous statements regarding the cyber capabilities of non-state terrorist groups. Conversely, aspects like cybercrime and state-

sponsored terror are given entire sections of the strategy, yet non-state actors are given two minor mentions in two sentences. This alludes to either the lack of capability by these actors altogether or the fact that this capability is not yet known and is in the process of being quantified.

All told, the expectation in all strategies is that acts of cyberterrorism or events like a cyber 9/11 are possible and may be more imminent than we know. Conversely, the more concretized assessment of the UK and the more minor stance of Canada on the topic of cyberterrorism specifically is that current cyber threat actors from the terror genre are less-than the giants that are vaguely portended or often blocked in with other threats such as in the US cybersecurity strategy. As it will be shown, the common trend in each doctrine in leaving the details of cyberterrorism rather vague is actually beneficial in that the genre itself is evolving due to the aforementioned confluence of belligerence genres.

Assessing the Reality

In an interview with former three-time US Presidential advisor Richard A. Clarke, Clarke (2016) explains that with the proliferation of internet-enabled devices in areas of critical infrastructure, many nations are only increasing their attack surface and opening up their populations to real harm. These critical infrastructural devices range from control systems in power plants to life-support equipment in hospitals that could be game-changers for parties that seek to exact the most control with the minimum amount of operational overhead—the perfect vector for a cyber 9/11 style attack. Indeed, the vulnerabilities built into these critical infrastructure pieces are due in large part to the monumental task of updating and maintaining an expansive network environment with any sort of homogeneity. With such a diverse attack surface strewn across a multitude of different industries, many different belligerence paradigms can leverage flaws in information technology and commit acts of terror that were previously

unavailable or inaccessible. Simply stated, many cyber threats are still developing and emerging as new attacks realize success, causing the lines to blur between the agendas of terrorism, nationalist groups, and state actors.

THE USE OF CYBER CAPABILITIES BY THE ISLAMIC STATE

As mentioned previously, the conventional example in ISIS vs. the UK government yielded little more than low-capability cyber-attacks such as *doxing*—the leak of personal information to the public—and the defacement of government-owned internet properties (Alexander and Clifford 2019). This low-capability approach is less than sophisticated and seems to form the extent of the means often occupied by these lone-terrorist entities. Alexander and Clifford (2019) go on to list the threat of ISIS as "much less capable of full-fledged cyberattacks targeting critical national infrastructure" (p. 88). This is mostly due to issues of funding and the ability of such organization to attract the sort of intellectual talent that often has socioeconomic advantages in the mainstream workforce or in the employ of some of the state-sponsored endeavors that tend to be much more lucrative from the standpoint of advanced equipment and nationalist appeal. This leaves these terrorist groups with little else than the option to conduct the aforementioned low-capability attacks while their remaining efforts are largely spent in using cyberspace and the internet for the mission of both recruiting and spreading propaganda (Charvat 2018).

Given the rudimentary use of information technology to push the goals of traditional terrorism, the rapid expanse of the internet into areas of sparsity and the low barrier of entry to better technology via globalization certainly causes one to consider the future of cyberterrorism operations. With relatively recent ventures, like the founding of the *Cyber Caliphate* and the ability to source free-lance hackers to mitigate the intellectual overhead, there are certainly

means in which groups like IS and Al-Qaeda can overcome their previous limitations and conduct more ambitious operations that would attack areas of critical infrastructure which would equate to the Cyber 9/11 style attack as foretold by the cyber strategies of the US, UK, and Canada. However, the point must be emphasized that current conventional cyberterrorist operations largely revolve around targets of opportunity rather than targets of catastrophic effect.

THE STATE-SPONSORED VARIABLE AND HACKER GROUPS

As the paradigm of cyberterrorism evolves, the utilization of cyber proxies to conduct nefarious operations muddies the conceptual boundaries of cyberterrorism by introducing the confluence of values that might be shared among a competing state and terrorist groups. Essentially, these arrangements feature the terrorist groups or non-state groups as providing the drive and willingness for the operation while the budget and agenda are made available by state actors. In *Cyber Proxies and Their Implications for Liberal Democracies*, Tim Maurer (2018) describes both the dynamic and implication of these proxy arrangements and how they can be used advantageously to avoid attribution in the case of both the non-state intermediary and the state providing the direction. In many ways, this toys with the terror-for-hire concept as states look to limit their profile while terrorist organizations seek to scale up their offenses.

In one of the few case study examples of the cyber proxy concept, the Syrian Electronic Army (SEA) is an interesting illustration of the proximity that can occur between state interests and its fringe supporters. The SEA is a group that emerged in 2011 as a movement to support the al-Assad government in Syria using means similar to the ISIS case study: defacing websites and disrupting targeted web services for notoriety and minor political consequence. However, in 2013 SEA would become most well-known for its attack on the Associated Press Twitter account where it would publish a fake headline stating that the White House had been bombed and that

the President had been injured in the blast. Almost immediately, the tweet made its rounds through the internet and resulted in a plunge in the stock market to the tune of a $136 billion that would eventually correct itself through the remainder of the trading day (Akhgar and Lockley 2014; Cohen 2014; Fisher 2013). While this may not seem like an extreme or devastating action, the event itself exemplifies the asymmetrical nature of cyberterrorism when it meets the power of national alignment.

Despite the SEA being a very small and politically motived group that caused the US stock market to cringe via a single tweet, the group is alleged to have least some funding ties to the Syrian government. In 2013, the *Guardian* had interviewed several anti-Assad hackers the occupied the counter-narrative to the SEA, and the consensus was that the "SEA sometimes works according to orders from Damascus—[s]ometimes they work on their own" (Charles and Harding 2013). The implications of this confluence, though hardly an indicator of some sort of mastermind organization *a al SPECTRE*—the global terror entity famously depicted in the James Bond films—the conceptual basis of the SEA conveys the idea the many belligerence genres are blended under cyberterrorism in light of the scalability of offensive operations using information technology.

Conclusion

In light of the above case studies that highlight the cyber capabilities of various terrorist groups, from the more traditional examples in case of ISIS to the more nuanced ties that SEA occupies with the Syrian government, the threat of a *Cyber 9/11* style event seems rather unlikely as a product of conventional terrorist operations. However, the later example of the SEA does provide some compelling evidence that the cyberterrorism narrative is being advanced by the possibility of terrorist groups liaising with state actors. This was evident in the effects that the

SEA had on the US stock market in 2013 by capitalizing on the effect of the news and social media. This gives rise to new questions that must be answered by future research that will, unfortunately, only be made available once more complex cyber-attacks are either thwarted just in time or proven successful and devastating.

Though the disparity in cyber capabilities that clarifies the lackluster technical prowess of lone non-state terror entities against the lever of cooperative groups with state ties, there are some limits to the above study. This is especially so in the case of assessing the lone terror groups against the effects of defensive operations that are a product of the cybersecurity doctrines mentioned here in the case of the US, UK, and Canada. For example, a recent publication of the NSA and US Cyber Command joint operation against ISIS in 2015 demonstrates the magnitude of the response being wielded against cyberterrorism. Essentially, the joint force had been tracking the growing threat posed by ISIS as it grew from its meager online recruiting efforts into increasingly complex encryption attacks on larger and larger targets. The result was a campaign to cripple the online wing of the terrorist organization with a well-coordinated attack that would envelop the ISIS infrastructure all at once. The resounding success of the operation has all but suppressed the ISIS cyber threat, staving off what could have been the lasting and most obscure tentacles of the terrorist organization if it had been left unmitigated.

The operation against the ISIS cyber capability leads to more questions over what might become of such means if they were left to advance without action. If anything, the joint effort proves that cyberterrorism, when caught early, can be snuffed out before it advances into the type of endeavor capable of serious repercussions on IT segments such as the national or international critical infrastructure—a *Cyber 9/11*. Perhaps the reason for such limited cyberterrorism operations reported in the mainstream media is due to the often clandestine nature of offensive

operations. After all, the joint NSA-DoD mission was conducted in 2015 and only reported to its full extent in 2019 (Temple-Raston 2019).

The other half of the puzzle lay in the muddied waters of terrorism-for-hire. While there is much to be desired from the academic research to provide more depth into the implication of a state in cyberterrorist groups, the idea that ideology can be leveraged by a state to produce mutual goals is not without support. Though the SEA example is somewhat weak, the reason for this could be due in large part to the regional turmoil in Syria where the al-Assad regime has been forced to engage multiple factions on multiple fronts. In the case of terrorist entities seeking willing parties in the vain of "Carlos the Jackal" to carry out cyberattacks on their behalf, however, one need only explore the lever of effect these types of third parties have through a survey of *advanced persistent threats* (APTs) that are more commonly conveyed in the mainstream news as associated with the likes of Russia, China, and Iran. These proxy groups are well known to monetize their expertise regardless of the nature of the work.

In the end, the entirety of the cybersecurity paradigm is one that is only advancing in its complexity. As Richard A. Clarke (2016) warned, the stretch of internet-enabled devices is occurring in confluence with the demands and advance of industry, social progress, and the desire to consolidate services. Such as these various societal demands meet in the form of social media and an *internet of things* culture, so too can we expect that threats will emerge and seek to consolidate their agendas to take advantage of the asymmetries afforded to them through everyday reliance on technology and internet connectivity. As for now, the alarm caused by cyber terrorism is valid in its concern, despite the non-state sponsored variety of terrorists being less apt to use cyber capabilities for much more than recruiting, fundraising, and for minor fear-inducing operations. Given that the skills to conduct harsher cyberattacks are likely to develop in

these non-state groups, there is far more compelling evidence to suggest that current concerns for cyber terrorism are better focused on the current blurred lines between state-sponsored cyber proxies and terrorism-for-hire. Tracking these concerns will largely fall on the shoulders of researchers willing to reach across disciplines to gain a better understanding of the mechanisms that will better predict future cyberterrorism advances and operations.

References:

Akhgar, Babak, and Eleanor Lockley. 2014. "Understanding the Situational Awareness in Cybercrimes: Case Studies." In *Cyber Crime and Cyber Terrorism Investigator's Handbook*, edited by Babak Akhgar, Francesca M. Bosco, and Andrew Staniforth, 101–21. Waltham, MA: Elsevier.

Alexander, Audrey, and Bennet Clifford. 2019. "Doxing and Defacements: Examining the Islamic State's Hacking Capabilities." *CTC Sentinel*. https://ctc.usma.edu/doxing-defacements-examining-islamic-states-hacking-capabilities/.

Arthur, Charles, and Luke Harding. 2013. "Syrian Electronic Army: Assad's Cyber Warriors." *The Guardian*. Guardian News and Media. April 30. https://www.theguardian.com/technology/2013/apr/29/hacking-guardian-syria-background.

Cohen, Daniel. 2014. "Cyber Terrorism: Case Studies." In *Cyber Crime and Cyber Terrorism Investigator's Handbook*, edited by Babak Akhgar, Francesca M. Bosco, and Andrew Staniforth, 165–74. Waltham, MA: Elsevier.

Charvat, Jpiag. 2018. "Cyber Terrorism: A New Dimension in Battlespace ." *Centre of Excellence Defence Against Terrorism* . https://ccdcoe.org/uploads/2018/10/05_CHARVAT_Cyber-Terrorism.pdf.

Fisher, Max. 2013. "Syrian Hackers Claim AP Hack That Tipped Stock Market by $136 Billion. Is It Terrorism?" *The Washington Post*. The Washington Post. Accessed December 15. https://www.washingtonpost.com/news/worldviews/wp/2013/04/23/syrian-hackers-claim-ap-hack-that-tipped-stock-market-by-136-billion-is-it-terrorism/.

Maurer, Tim. 2018. “Cyber Proxies and Their Implications for Liberal Democracies.” *The Washington Quarterly* 41 (2): 171–88. doi:10.1080/0163660x.2018.1485332.

Public Safety Canada. 2019. “National Cyber Security Strategy: Canada's Vision for Security and Prosperity in the Digital Age.” https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/ntnl-cbr-scrt-strtg-en.pdf.

HM Government. 2016. “National Cyber Security Strategy 2016-2021.” https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf.

Temple-Raston, Dina. 2019. “How The U.S. Hacked ISIS.” *NPR*. NPR. September 26. https://www.npr.org/2019/09/26/763545811/how-the-u-s-hacked-isis.

The White House. 2018. “National Cyber Strategy of the United States of America.” https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.