Is Cyberterrorism a Real Threat? – Yes

Maura Conway

It was estimated in 2012 that by that time some 31,300 press, magazine, and academic journal articles had already been written on cyberterrorism (Singer, 2012). Albeit the term 'cyberterrorism' was coined in the 1980s (Collin, 1997) and has thus been in existence for more than 30 years now, there is still considerable disagreement about what particular types of activity it describes. In 1991, the US National Academy of Sciences made the now-famous prediction that "tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb" (National Research Council, 1991: 7). So is cyberterrorism now a regular occurrence? Or has it not yet occurred, but nevertheless poses a real threat? It's actually possible to answer 'yes' to both questions; let me explain further.

Cyberterrorism is not a future threat, it's happening now

In her highly-cited testimony before the Special Oversight Panel on Terrorism of the US House of Representatives' Committee on Armed Service in 2000, Dorothy Denning described cyberterrorism as "the convergence of terrorism and cyberspace" and went on to say:

> 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."

This conception of cyberterrorism, which is commonplace amongst academics, is very narrow and renders the target or consequences of an attack a determining feature alongside the required socio-political aim. This is in stark contrast to the conclusions drawn by Sarah Gordon and Richard Ford in a Symantec White Paper discussing Denning's testimony:

> "we believe that the true impact of her opening statement ("the convergence of terrorism and cyberspace") is realized not only when the attack is launched against computers, but when many of the other factors and abilities of the virtual world are leveraged by the terrorist in order to complete his mission, whatever that may be" (2003: 4).

On this analysis, Gordon and Ford are willing to countenance understandings of cyberterrorism that are as wide as to include, for example, the online purchase of airline tickets by the 9/11 attackers (Jarvis et al., 2014: 28). They're not alone, other academics too subscribe to the idea that any use of the Internet by terrorists constitutes cyberterrorism (see e.g. Desouza and Hensgen, 2003: 388). In fact, adopting this approach, probably one of the first cyberterrorist attacks was initiated more than twenty years ago when over a two-week period in August 1997 the Liberation Tigers of Tamil Eelam's (LTTE) swamped Sri Lankan embassies worldwide with email traffic. An LTTE offshoot calling itself the Internet Black Tigers claimed responsibility for the "suicide e-mail bombings" (Tribune News Service 1998).

Others have taken things a step further. George Kostopoulos differentiates in his work between three different types of cyberterrorists: 1.) professionals who "aim at inflicting physical or cyber damage" on their victims, 2.) amateurs who "find pleasure in applying cyber graffiti," and 3.) thieves who "have immediate personal illicit economic benefit from their actions" (2008: 165). Kostopoulos' conception of cyberterrorism thus incorporates everything from virtual nuisance activity to a massive cyber-attack causing 'real world' damage. Essentially, anything 'bad' undertaken via cyber means may be termed cyberterrorism on this analysis. Such an approach has been widely taken-up in media and by some policymakers. In summer 2017, for example, a Qatari newspaper headlined a piece on the alleged hacking of the Qatari government's news agency's website with 'Shameful Act of Cyber Terrorism' (Qatar News Agency, 2017) whilst in India a police complaint was filed under Section 66F of the IT Act (Committing the Offence of Cyber Terrorism) against a butcher for posting a 12-second video clip on his Facebook account depicting the slaughter of a cow on the basis it was offensive to the 'cow-worshiping tradition' of Hindus (Srividya, 2017). To sum-up, on some definitions it is not a question of 'if' or 'when' cyberterrorism will take place, it's already a daily occurrence globally.

An argument based on whose definition of cyberterrorism is the most cogent is unsatisfying to some however, so let's take things a step further: reverting to Denning's "convergence of terrorism and cyberspace" thence 'cyberterrorism' and having due recourse to Denning's own approach to the issue, but also that of Gordon and Ford and others sharing a similar outlook, let's consider the cyber activity of the so-called 'Islamic State' (IS) and whether it can convincingly be described as cyberterrorism. A focus on IS is appropriate for two reasons: i.) it's widely agreed to be a terrorist organisation and ii.) it has made wide use of the Internet. Dispensing then with what many would consider far too expansive definitions, such as that of Kostopoulos, has IS engaged in cyberterrorism on either Denning or Gordon and Ford's definitions?

IS terrorists' cyber activity

IS's online activity has two major components, its social media campaign and its hacking activity.

IS's social media campaign is routinely described in the press as 'slick' and 'professional.' At the peak of their social media activity in 2015, IS were producing upwards of 1,100 items of propaganda monthly (Winter, 2015: 5). At one point, IS-supportive Twitter accounts numbered somewhere between 50,000 to 90,000 (Berger & Morgan, 2015: 7). In terms of formats, IS's official online content has included text (e.g. books, magazines), images (e.g. photo montages, infographics), and videos. In addition to their Twitter presence, which has now been significantly disrupted, IS are also active on a wide range of other social media platforms and content upload sites, including YouTube, Google Drive, JustPaste.It, Google Photos, SendVid, and the Internet Archive (Conway et al, 2017). The purpose of this IS activity is to influence as many Internet users as possible to identify with their violent jihadi ideology and to radicalise sufficient numbers to, in the early part of their online campaign, travel to their self-declared 'caliphate' as so-called 'foreign fighters' or, more recently, to carry out terrorist attacks in their countries of origin in IS's name. IS thus represents a straightforward case of a terrorist group using the Internet to solicit others to

engage in terrorism and thence falls squarely into Gordon and Ford's definition of cyberterrorism on the basis of the above-described activity alone.

In addition to its online propaganda campaign, IS and their supporters have also engaged in hacking activity. This appears much less formal, resourced, and organised than IS's social media campaign, but bears description and analysis in the cyberterrorism context nonetheless, particularly as it's this type of activity that comes closer for many to approximating cyberterrorism than the online influence activity just-described.

IS's hacking capabilities entered the public consciousness in early 2015 when they and/or their supporters hacked the Twitter accounts of the US Department of Defence's Central Command (CENTCOM) and Newsweek. While these and other IS-associated hacks lacked sophistication in both their technological knowhow and targeting, they nevertheless displayed IS's desire to cause virtual damage. IS's hacking activity appears to have been launched and spearheaded by Briton Junaid Hussain (a.k.a. Abu Hussain Al Britani). Hussain, formerly "TriCk" of hacking outfit TeaMp0isoN, quit Britain in 2013 upon completion of a 6-month prison sentence for hacking activity that resulted in former UK Prime Minister Tony Blair's personal contact details being posted online (Murphy, 2015). Killed by a targeted drone strike in Raqqa, Syria in August 2015, Hussain was succeeded in his leadership role by British-educated Siful Haque Sujan until he too was killed, also in a drone strike in Raqqa, in December 2015. The biographies of Hussain and Sujan are illustrative of two important points in the cyberterrorism debate: i.) that it's possible for IS—and therefore probably also other terrorist groups—to get on board relatively skilled hackers and ii.) the targeted killing of both may be an indicator of them and their hacking activity progressing to be viewed as a significant risk by authorities.

Both types of IS online activity described above—social media campaigning and hacking—fit easily into Gordon and Ford's definition of cyberterrorism, given that both are clear-cut examples of the convergence of terrorism and cyberspace. Both types of activity are also routinely referred to in media as being instances of cyberterrorism. Most scholars agree that everyday terrorist use of the Net for influence operations and other purposes doesn't fulfil Denning's criteria however. Nor does the type of hacking activity just described. Argued below, however, is that it can only be a short time before IS or some other terrorist group or their supporters engage in an attack that fulfils even the very narrowest definitions of cyberterrorism.

No major cyberterrorist attack has ever yet occurred, but it's more likely now than ever

As Dunn-Cavelty has pointed out, "careful threat assessments…necessarily demand more than just naval-gazing and vulnerability spotting. Rather than simply assuming the worst, the question that must be asked is: Who has the interest and the capability to attack us and why?" (2011: 2). On Denning's widely accepted definition, no act of cyberterrorism has ever yet occurred. Although a diverse range of terrorist groups, including particularly al Qaeda and IS, have demonstrated an interest in and some capability to develop and deploy rudimentary cyberattack capabilities, there have been no successful terrorist attacks involving them. The reason for this is generally held to be a disconnection between

terrorists' intent and their insufficient technological capabilities. This section challenges the continued veracity of such an approach by underlining terrorists' intent with respect to carrying out an act of cyberterrorism and, more importantly, following up with a discussion of the way in which the workings of the social web, especially crowd sourcing, and developments in the so-called 'Internet of Things' may herald a break with the past as regards technological capabilities.

Who has the interest to attack us and why?

In an oft-quoted 2012 speech in New York, the former Director of the US Central Intelligence Agency (CIA) and then US Defense Secretary, Leon Panetta, laid out the cyberterrorism threat as he saw it:

"A cyber attack perpetrated by nation states [or] violent extremists groups could be as destructive as the terrorist attack on 9/11. Such a destructive cyber-terrorist attack could virtually paralyze the nation… [W]e know that foreign cyber actors are probing America's critical infrastructure networks. They are targeting the computer control systems that operate chemical, electricity and water plants and those that guide transportation throughout this country. We know of specific instances where intruders have successfully gained access to these control systems. We also know that they are seeking to create advanced tools to attack these systems and cause panic and destruction and even the loss of life."

Interesting to note here is that the ex-CIA chief doesn't conceive of cyberterrorism as restricted to cyber destruction carried out by terrorist groups, but that any actor, including states, with the requisite political motive, tools, targeting, and violent impact could be conceived of—indeed, probably would be—as engaging in cyberterrorism.

Panetta went on to paint a word picture of the types of cyberterrorist attack that could unfold:

"They could, for example, derail passenger trains or even more dangerous, derail trains loaded with lethal chemicals. They could contaminate the water supply in major cities or shutdown the power grid across large parts of the country. The most destructive scenarios involve cyber actors launching several attacks on our critical infrastructure at one time, in combination with a physical attack on our country. Attackers could also seek to disable or degrade critical military systems and communication networks. The collective result of these kinds of attacks could be a cyber Pearl Harbor; an attack that would cause physical destruction and the loss of life. In fact, it would paralyze and shock the nation and create a new, profound sense of vulnerability."

This description of cyberterrorism is much closer to Denning's conceptualisation than any other discussed herein thus far. Finally, Panetta warned sceptics that:

"[C]yber attacks are every bit as real as the more well-known threats like terrorism, nuclear weapons proliferation and the turmoil that we see in the Middle East … Before September 11, 2001, the warning signs were there. We weren't organized. We weren't ready and we suffered terribly for that lack of attention. We cannot let that happen again. This is a pre-9/11 moment."

The US Department of Justice's Assistant Attorney General for National Security, John Carlin, said something very similar in a speech delivered at Harvard University in December 2015:

"'Terrorists seek to exploit our reliance on weak or outdated network security to harm our way of life. To date, terrorist groups are largely only experimenting with destructive hacking, but they are developing more advanced capabilities. We've also seen calls to action through Internet jihad by both Al Qaeda and ISIL, and

our international partners have experienced attacks conducted by purported online jihadists. We are concerned that those groups will not hesitate to deploy offensive capabilities if they are able to acquire them."

What the above quotes from a well-informed U.S. government insiders point to is that terrorists definitely have the intention to engage in cyberterrorism, but perhaps not yet the capability to pull off a really major cyberterrorism attack. How might transformations in the online landscape cause this to change?

The Darknet, the IoT, and the transformation of capability

Eugene Kaspersky, a Russian engineer and founder and CEO of anti-virus vendor Kaspersky Lab, is well known for his pronouncements on the threat of cyberterrorism. He had this to say at the 2011 London Cyber Summit:

"I don't want to speak about it. I don't even want to think about it. But we are close, very close, to cyberterrorism. Perhaps already the criminals have sold their skills to the terrorists…There is already cyber espionage, cyber crime, hacktivism, soon we will be facing cyber terrorism."

Kaspersky's prose may be overwrought, but he's not alone in fearing future combinations of cyber with terrorism. In August 2017, the European Union's (EU) Counterterrorism Coordinator Giles De Kerchove remarked to the Spanish newspaper El Mundo regarding IS's cyber capabilities that "on the Darknet you can find system vulnerabilities for sale…Or they can buy the services of Russian hackers, because [IS] have money" (Suanzes, 2017). The EU police agency EUROPOL's *IOCTA 2016: Internet Organised Crime Threat Assessment* contains a section on 'The Convergence of Cyber and Terrorism' (pp.'s 49-51) in which the currently thriving Darknet-based cybercrime-as-a-service industry is depicted as providing easy access to criminal products and services that "can be used by anyone, from technically savvy individuals to non-technically skilled terrorists," explicitly stating that this allows for the launch of cyber attacks "of a scale and scope disproportionate to the technical capability of the actors involved" (p.49). Such suggested outsourcing has been subject to critique however on the basis, amongst other things, that it would not only force the terrorists to operate outside their own trusted circles and thus leave them ripe for infiltration, but even if contact with "real" hackers was successful, the terrorist group would be in no position to gauge their competency accurately; they would simply have to rely on trust, which it has been argued would be very personally and operationally risky (Conway 2003, 10 – 12). What if it were possible to overcome these challenges by relying on online crowdsourcing however?

'Crowdsourcing,' a combination of the words 'crowd' and 'outsourcing,' refers to the practice of outreach to large numbers of people and enlisting some of them, often unpaid, to obtain information or input into or, indeed, completion of a task or project, typically via the Internet. This approach has already been shown to work in terms of instigating low-level 'real world' terrorist attacks. Basically, a raft of recent attacks, including a growing number of vehicle attacks, have been shown to have been inspired rather than directed by IS. The perpetrators were not, in other words, 'members' of IS nor were they told directly by IS to carry out attacks, but were influenced to do so on the basis of consuming IS propaganda instructing their followers to do just that. What these relatively unsophisticated lone actor terrorist attacks have shown is the possibility for small numbers

of people carrying out 'small' attacks to have big impacts, in terms of generating widespread fear. So what type of cyberattacks would likely generate the 'real world' casualties necessary for arriving at the same level of fear as generated by the spate of gun, knife, and vehicle attacks?

In June 2016, Robert Hannigan, then Director of the UK's Government Communications Headquarters, more commonly known as GCHQ, and "the centre for Her Majesty's Government's Signal Intelligence (SIGINT) activities" (gchq.gov.uk), warned that terrorists "are gaining the capability to bring a major city to a standstill with the click of a button." Whilst cautioning that states are currently developing offensive cyber capabilities that could pose a risk to the UK, the GCHQ boss said that terrorist groups are also seeking to weaponise cyber technologies:

"There are certainly states and groups with the intent to do it, terrorist groups, for example, who have no threshold when it comes to the loss of life. We're not quite there yet, but as the world becomes ever more connected that will become a greater risk. At some stage they will get the capability" (Bodkin 2016).

It's generally agreed that critical (cyber) infrastructures globally are insufficiently secured and thus highly vulnerable to attack. The so-called "Internet of Things" (IoT) presents a particularly target-rich environment. According to Intel (2016):

"The 'Internet of Things' is exploding. It is made up of billions of "smart" devices—from miniscule chips to mammoth machines—that use wireless technology to talk to each other (and to us). Our IoT world is growing at a breath-taking pace, from 2 billion objects in 2006 to a projected 200 billion by 2020. That will be around 26 smart objects for every human being on Earth!"

And will include, on a conservative estimation, about one in every five private vehicles (Tucker 2016). GCHQ's Hannigan drew attention to the increasing risks to cities like London as more objects, like cars and household appliances, are connected to the Internet in this manner. The use by IS-inspired attackers of vehicles for terrorism purposes illustrates the attractiveness of these types of attacks. How much more attractive might the possibility of a largescale coordinated automated high-jacking of Internet-connected vehicles be? Even more concerning however should be the possibilities afforded by IoT-enabled healthcare, which may present terrorists with the easiest route to causing physical harm.

Of the 15 billion devices found within the IoT in 2015, 30.3% were in healthcare (Intel 2016). Medical devices such as pacemakers, neuro-stimulators, and drug delivery pumps are increasingly used to manage medical conditions and because they generally communicate via wireless technology have high cyber threat exposure. In 2007, it was revealed that former United States vice president, Dick Cheney, had his heart implant modified for fear of a terrorist attack. The possibility of exploiting the device was confirmed by multiple university-based research groups who suggested a software radio-based attack was possible (BBC News, 2007). As far back as 2011 a security researcher, himself a diabetic, demonstrated how insulin pumps could be remotely turned off and the

device configurations changed without the patient's knowledge (DarkReading, 2011). Balogun *et al* hypothesise in a similar fashion:

"Suppose a smart health system that returns drug prescriptions to a patient were to be threatened by a man-in-the-middle attack. A remote attacker could intercept data and return a health-threatening prescription and thousands of patients' lives could be endangered due to intentional medication errors" (p.52).

The nature of the above-described medical systems, particularly their reliance on wireless technology to operate, means that they could be compromised by highly malicious attackers with relatively low technical skills.

Conclusion

IS's online influence operations cannot, most scholars and many others agree, be legitimately described as cyberterrorism. Terrorist groups are known, on the other hand, to have been actively seeking cyber capabilities for some time and insiders from within government and industry across a range of countries share concerns regarding their developing capabilities in this domain. IS have, to a limited extent, already engaged in cyberattacks, for example, and have successfully retained personnel with technical experience capable of expanding their activity in this domain. Having said this, IS clearly faces many challenges and logistical issues, including the targeted assassination of at least two of their top cyber operatives, that have tempered their cyberterrorism ambitions. This means that they're not yet capable of undertaking a major cyberterrorism attack, though it cannot be ruled out in the longer term. In the meantime, unsophisticated vehicle attacks by IS-inspired lone actors, effectively crowdsourced via the Internet, have proven highly potent. There's no reason that low-level cyberattacks could not be similarly outsourced via the Net, either for payment or by ideological fellow-travellers with the requisite skills. Herman Kahn's observation in his famous Cold War text *On Thermonuclear War* (1960/2007) that "The aggressor has to find only one crucial weakness; the defender has to find all of them, and in advance" appears more apt now than ever. The IoT appears riddled with just such crucial weaknesses and therefore to present an unmatched and mounting array of possibilities for attacks. So, yes, cyberterrorism poses a real and growing threat in our increasingly cyber-dependent world.

References

Balogun, M., Bahşi, H., and Karabacak, B., 2017. 'Preliminary Analysis of Cyberterrorism Threats to Internet of Things (IoT) Applications', in Conway, M., et al., eds, *Terrorists' Use of the Internet: Assessment and Response*, Amsterdam: IOS Press.

BBC News, 2013. 'Dick Cheney: Heart Implant Attack was Credible,' *BBC News*, 21 October 2013, available online at http://www.bbc.com/news/technology-24608435.

Berger, J.M., and Morgan, J., 2015. The ISIS Twitter Census: Defining and Describing the Population of ISIS Supporters on Twitter, Washington D.C.: Brookings, available online at https://www.brookings.edu/wp-content/uploads/2016/06/isis_twitter_census_berger_morgan.pdf.

Bodkin, H., 2016. 'Terrorist Groups Acquiring the Cyber Capability to Bring Major Cities to a Standstill, Warns GCHQ Chief', *The Telegraph*, 9 June 2016, available online at http://www.telegraph.co.uk/news/2016/06/08/terrorist-groups-acquiring-the-cyber-capability-to-bring-major-c/.

Carlin, J.P., 2015. 'Prepared Remarks on the National Security Cyber Threat' delivered at Harvard Law School, Boston, 3 December 2015, available online at http://today.law.harvard.edu/at-hls-dojs-top-national-security-lawyer-discusses-u-s-vulnerability-to-cyberterrorism/?utm_source=twitter&utm_medium=social&utm_campaign=hls-twitter-general.

Collin, B., 1997. 'Future of Cyberterrorism: Physical and Virtual Worlds Converge', *Crime and Justice International*, 13(2): 15-18.

Conway, M., Khawaja, M., Lakhani, S., Reffin, J., Robertson, A., and Weir, D., 2017. *Disrupting Daesh: Measuring Takedown of Online Terrorist Material and Its Impacts*, Dublin: VOX-Pol, available online at http://www.voxpol.eu/download/vox-pol_publication/DCUJ5528-Disrupting-DAESH-1706-WEB-v2.pdf.

DarkReading, 2011. 'Getting Root on the Human Body', *DarkReading.com*, 5 August 2011, available online at https://www.darkreading.com/vulnerabilities---threats/getting-root-on-the-human-body/d/d-id/1136133.

Denning, D., 2001. 'Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy', in Arquilla, J. and Ronfeldt, D., eds, *Networks and Netwars: The Future of Terror, Crime, and Militancy*, Santa Monica, CA: RAND, available online at http://www.rand.org/pubs/monograph_reports/MR1382.html.

Desouza, K.C., and Hensgen, T., 2003. 'Semiotic Emergent Framework to Address the Reality of Cyberterrorism', *Technological Forecasting and Social Change*, 70(4): 385-396.

Dunn-Cavelty, M., 2011. 'Cyberwar: A More Realistic Threat Assessment', International Relations and Security Network (ISN), available online at http://www.css.ethz.ch/en/services/digital-library/articles/article.html/129764/pdf.

EUROPOL, 2016. *IOCTA 2016: Internet Organised Crime Threat Assessment*, The Hague: EUROPOL, available online at https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016.

Gordon, S., and Ford, R., 2003. 'Cyberterrorism?' Symantec White Paper, available online at https://www.symantec.com/avcenter/reference/cyberterrorism.pdf.

Intel Corporation, 2016. *A Guide to The Internet of Things* [Infographic], Santa Clara, CA: Intel, available online at https://www.intel.com/content/www/us/en/internet-of-things/infographics/guide-to-iot.html.

Jarvis, L., Nouri, L., and Whiting, A., 2014. 'Understanding, Locating and Constructing Cyberterrorism', in Chen, T.M., Jarvis, L., and Macdonald, S., eds, *Cyberterrorism: Understanding, Assessment, and Response*, New York: Springer.

Kahn, H., 2007. *On Thermonuclear War*, New York: Taylor and Francis.

Kostopoulos, G.K., 2008. 'Cyberterrorism: The Next Arena of Confrontation', *Communications of the IBIMA*, 6(1): 165-169.

Murphy, L., 2015. 'The Curious Case of the Jihadist Who Started Out as a Hacktivist', *Vanity Fair*, 15 December 2015, available online at https://www.vanityfair.com/news/2015/12/isis-hacker-junaid-hussain.

National Research Council, 1991. *Computers at Risk: Safe Computing in the Information Age*, Washington D.C.: National Academy Press, available online at http://www.nap.edu/books/0309043883/html/index.html.

Panetta, L., 2012. Remarks on Cybersecurity to Business Executives for National Security, New York, 11 October 2012, available online at http://archive.defense.gov/transcripts/transcript.aspx?transcriptid=5136.

Qatar News Agency, 2017. 'Shameful Act of Cyber Terrorism,' *The Peninsula*, 18 July 2017, available online at https://thepeninsulaqatar.com/article/18/07/2017/Shameful-act-of-cyber-terrorism.

Singer, P., 2012. 'The Cyber Terror Bogeyman', Brookings, 1 November 2012, available online at: https://www.brookings.edu/articles/the-cyber-terror-bogeyman/.

Srividya, P.V., 2017. '"Cyber Terrorism" Case Against Man for FB Clip on Cow Slaughter', *The Hindu*, 14 June 2017, available online at http://www.thehindu.com/news/national/tamil-nadu/cyber-terrorism-case-against-man-for-fb-clip-on-cow-slaughter/article19033827.ece.

Suanzes, P.R., 2017. 'El coordinador antiterrorista de la UE: "Lo de Barcelona volverá a pasar, hay 50.000 radicales en Europa"', *El Mundo*, 31 August 2017, http://www.elmundo.es/espana/2017/08/31/59a70a48ca4741f7588b45e4.html.

Tribune News Service, 1998. 'U.S. Tells Of E-mail "Attack" By Rebels', *Chicago Tribune*, 5 May 1998, available online at: http://articles.chicagotribune.com/1998-05-05/news/9805050148_1_sri-lankan-tamil-eelam-liberation-tigers.

Tucker, P., 2016. 'How Will Terrorists Use the Internet of Things? The Justice Department Is Trying to Figure That Out', *Defense One*, 8 September 2016, available online at

http://www.defenseone.com/technology/2016/09/how-will-terrorists-use-internet-things-justice-department-trying-figure-out/131381/.

Winter, C., 2015. *Documenting the Virtual "Caliphate"*, London: Quilliam, available online at http://www.quilliaminternational.com/wp-content/uploads/2015/10/FINAL-documenting-the-virtual-caliphate.pdf.

Further Readings

1. Alkhouri, L., Kassirer, A., and Nixon, A., 2016. *Hacking for ISIS: The Emergent Cyber Threat Landscape*, Flashpoint, available online at https://fortunascorner.com/wp-content/uploads/2016/05/Flashpoint_HackingForISIS_April2016-1.pdf.

2. Balogun, M., Bahşi, H., and Karabacak, B., 2017. 'Preliminary Analysis of Cyberterrorism Threats to Internet of Things (IoT) Applications', in Conway, M., et al., eds, *Terrorists' Use of the Internet: Assessment and Response*, Amsterdam: IOS Press.

3. EUROPOL, 2016. *IOCTA 2016: Internet Organised Crime Threat Assessment*, The Hague: EUROPOL, available online at https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016.

4. Murphy, L., 'The Curious Case of the Jihadist Who Started Out as a Hacktivist', *Vanity Fair*, 15 December 2015, available online at https://www.vanityfair.com/news/2015/12/isis-hacker-junaid-hussain.

Discussion Questions

1. What precisely is cyberterrorism? Is it useful to include in the category 'attacks' that cause no physical harm?

2. Having regard to the increasing prevalence of cybercrime, what's the likelihood of for-profit cybercriminals knowingly assisting terrorists?

3. What are the attractions of engaging in cyberterrorism over more conventional 'real world' attacks?

4. What other IoT-enabled objects, besides medical devices and vehicles, might be vectors for cyberterrorism?

5. Are the fears that terrorists could engage in cyberterrorism resulting in 'real world' harm, including the death of targets, justified?