Cyberterrorism

sʌɪbəˈtɛrərɪz(ə)m/

noun.

What we are (not) speaking about?

Irina Rizmal

Cyberterrorism has come to be understood as one of the leading threats to vital interests of Western states. Even though there is general agreement that a cyberterrorist attack has not yet been experienced, there is consensus on what cyberterrorism might imply. However, contrary to this understanding, when it comes to framing who the potential cyberterrorists are, this consensual definition seems to be marginalised in order to reinforce the narrative of the prevailing discourse of the War on Terror – that Salafist jihadists are preparing an electronic war against the West and the liberal world order; with other actors, potentially more threatening to national security in the cyber sphere, intentionally left out. A specific political discourse is thus created around cyberterrorism, one that is meant to pose as a natural extension of the current discourse on terrorism in general, by artificially attributing cyberterrorist capabilities to already defined, traditional terrorist organisations. If continued, this trend of attributing cyberterrorist capabilities to the wrong actors, portraying cyberterrorism as something that it is not, may ultimately undermine actual counterterrorist efforts in the cyber sphere and damage national security in the long run.

In 2016, 73% of Americans cited cyberterrorism as a leading threat to vital interests of the United States in the next 10 years[1]. It has been described as perfectly combining two of the greatest present-day fears, that of random, violent victimization and the general distrust of computer technology[2]. And given the language commonly used to describe the potential dangers stemming from the cyber sphere, including references to a potential 'Cybergeddon' and an 'electronic Pearl Harbour', complemented with the overuse of the term 'cyberterrorism' by mass media, for incidents ranging from computer viruses, to website defacement, to actual hacking attempts, these results are no surprise. Although there is no precise definition of cyberterrorism, there is general consensus that it involves attacks and threat of attacks on computers, networks and the information stored therein to coerce a government or its people in the furtherance of political or social objectives[3].

However, the label 'cyberterrorist' has in the political discourse mainly been applied to actors and organisations already framed as terrorist, although recognising that these actors have not yet carried out activities that could be labelled as cyberterrorism. Assigning this label of 'the next

[1] Gallup, *Americans Cite Cyberterrorism Among Top Three Threats to U.S.* February 10, 2016. Available at http://www.gallup.com/poll/189161/americans-cite-cyberterrorism-among-top-three-threats.aspx [Accessed March 28, 2017 at 12.47 PM]

[2] Weimann, G. (2005) Cyberterrorism: The sum of all fears? *Studies in Conflict and Terrorism* 28(2) p.131.

[3] Denning, D. (2000) *Cyberterrorism*, Testimony before the Special Oversight Panel on Terrorism of the Committee on Armed Services, US House of Representatives, The Terrorism Research Center.

cyberterrorists' to organisations such as al Qaeda, Hamas and ISIL is justified based on the general use of the Internet by these actors, for purposes such as communication, spreading propaganda, recruitment and fundraising, or, in less words, mainly the spread of extremist content. At the same time, organisations that have and do engage in activities found in the narrower definition of cyberterrorism, such as Anonymous, are labelled merely as 'hacktivists' and their activities as *disruptive*, rather than destructive or threatening to national security, despite attacks on, for example, national critical infrastructure. Therefore, parallel to the process of establishing a narrow(er) consensual definition of cyberterrorism, the framing of cyberterrorist actors follows a seemingly different logic, ignoring the fact that *terrorism*, in general, refers to actions, not actors.

Cyberterrorism, sʌɪbəˈtɛrərɪz(ə)m/, *noun*.

The greatest challenge in reaching consensus on a definition of cyberterrorism has focused around the debate on whether to adopt a narrow, 'target-oriented' definition of the concept, or a broader, 'tool-oriented' one[4]. Proponents of the latter argue that cyberterrorism should be seen as encapsulating general use of the Internet and computers by terrorists[5]. However, widening the definition in this way risks labelling any online activity conducted by terrorist organisations as terrorism, regardless of whether the activity itself is, in fact, terrorist[6]. This precludes any understanding of the concept of cyberterrorism itself, and defines an activity based on the actors engaged, rather than what it actually implies. As a result, the term becomes so misplaced and overused that it no longer bears any clear meaning[7].

For this reason, a number of authors agree that cyberterrorism needs to be clearly defined and separated from other activities terrorist and other organisations and individuals engage in online, including communication, spread of extremist content and propaganda, or cybercrime for terrorist purposes. There is general agreement that cyberterrorism refers to the *means* to carry out an attack, while the motive remains the same as in traditional forms of terrorism[8]. Bearing this in mind, a consensual definition of cyberterrorism, and the one most often referred to, is found in Dorothy Denning's testimony before the US House of Representatives, defining cyberterrorism as "unlawful attacks and threats of attack against computers, networks and the information stored therein" with the intention of intimidating or coercing a government or its people in the furtherance of political or social objectives. For an attack to constitute an act of terrorism, it must also have a serious intended *effect* in terms of human and economic casualties or intense fear and anxiety among citizens – terror[9].

[4] Jarvis, L. and Macdonald, S. (2015) What is cyberterrorism? Findings from a survey of researchers, *Terrorism and Political Violence* 24(7) p.659.

[5] Taliharm, A. M. (2011) Emerging Security Challenges and Cyber Terrorism, *Digital Development Debates* #05. Holt, T. J. (2012) Exploring the Intersections of Technology, Crime and Terror, *Terrorism and Political Violence* 24(2) pp.337-354. Kenney, M. (2015) Cyber-Terrorism in a Post-Stuxnet World, *Foreign Policy Research Institute* (winter) pp.111-128.

[6] Gordon, S. and Ford, R. (2002) Cyberterrorism? *Computers and Security* 21(7) pp.636-647. Ahmad, R. and Yunos, Z. (2012) A Dynamic Cyber Terrorism Framework, *International Journal of Computer Science and Information Security* 10(2) pp.149-158. Jarvis, L. and Macdonald, S. (2015) What is cyberterrorism? Findings from a survey of researchers, *Terrorism and Political Violence* 24(7) pp.657-678.

[7] Weimann, G. (2008) Cyber-Terrorism: Are we barking at the wrong tree? *Harvard Asia Pacific Review* 9(2) pp.41-46. Kenney, M. (2015) Cyber-Terrorism in a Post-Stuxnet World, *Foreign Policy Research Institute* (winter) pp.111-128.

[8] Rogers, M. (2003) The Psychology of Cyber-Terrorism. In Silke, A (ed.) *Terrorists, Victims and Society: Psychological Perspectives on Terrorism and its Consequences*, John Wiley and Sons, Ltd. Lachow, I. (2009) Cyber Terrorism: Menace or Myth? In Kramer et al (eds.) *Cyberpower and National Security*, University of Nebraska Press: Potomac Books. Heickero, R. (2014) Cyber Terrorism: Electronic Jihad, *Strategic Analysis* 38(4) pp.554-565.

[9] Denning, D. (2000) *Cyberterrorism*, Testimony before the Special Oversight Panel on Terrorism of the Committee on Armed Services, US House of Representatives, The Terrorism Research Center.

What about *cyberterrorists*?

When it comes to engaging in debates on who cyberterrorist actors are, in general, a narrative is created in which the potential danger stemming from existing terrorist organisations' use of the cyber sphere should be the primary focus of national security efforts. Despite the general, consensual agreement that cyberterrorism is not to encapsulate the notion of mere online presence of terrorist groups, facts such as a rise in the number of audio or video web messages published online by al Qaeda is highlighted as a cyberterrorist threat[10]. The increase in the number of "Salafist jihadi websites"[11] and websites of terrorist organizations as listed by the State Department[12] is also referred to as an indicator of potential cyberterrorist activity. Thus, although there is agreement that, for the time being, terrorist groups such as al Qaeda mainly limit their online activities to communication, propaganda, data mining, recruitment and fundraising[13], the notion that the opportunities the cyber sphere opens to existing terrorist organisations will not go unnoticed, and that the threat of these actors turning to cyberterrorism is "realistic" (with the infinite number of avenues to explore and exploit), is constantly reinforced[14]. These activities are generally used as evidence of 'cyberterrorist activity' in the political discourse.

The present-day narrative is that the West and the wider, liberal world order, are faced with an "Islamist terrorism", linking the two labels together in one globally threatening concept. Such framing has been used time and time again to justify introduction of certain "emergency measures" and "exceptional" practices, ranging from war to engagement in regime change, state-building and extra-judicial procedures[15], all under the flag of removing threats to the liberal world order and "our way of life", while at the same time, liberating the people suffering under such regimes. Terrorism, in general, has been framed as a concept linked to specific actors, groups and territories, certain religions and ways of life. This allows pursuing prevailing geostrategic interests in specific regions, as linking terrorism to states allows "getting at states, […] and it is easier to find them then it is to find Bin Laden", as Dick Cheney, Vice President of the United States, outlined in 2002[16].

It seems that the same logic is at play when it comes to framing cyberterrorist actors as well. Cyberterrorism is effectively and immensely being securitised and portrayed as a major national security threat, a 'Tier One' security priority and one of the greatest challenges national security agencies will be faced with in the near future. At the same time, the consensual understanding of

[10] Brunst, P. W. (2010) Terrorism and the Internet: New Threats Posed by Cyberterrorism and Terrorist Use of the Internet. In Wade, M. and Maljevic, A. (eds.) *A War on Terror?: The European Stance on a New Threat, Changing Laws and Human Rights Implications*, Springer Science + Business Media, LLC p.71.

[11] Ranstorp, M. (2007) The virtual sanctuary of al-Qaeda and terrorism in an age of globalisation. In Eriksson, J. and Giacomello, G. (eds.) *International Relations and Security in the Digital Age*, Routledge Advances in International Relations and Global Politics p.39.

[12] Minei, E. and Matusitz, J. (2013) Cyberterrorist messages: A semiotic perspective, *Semiotica* 197 p.274. Segal, A. (2016) *The Hacked World Order*, Public Affairs: A Council on Foreign Relations Book p.186.

[13] Lewis, J. A. (2002) *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats*, Center for Strategic and International Studies p.5. Weimann, G. (2005) Cyberterrorism: The sum of all fears? *Studies in Conflict and Terrorism* 28(2) pp.129-149. Nye, J. S. Jr. (2011) *The Future of Power*, Public Affairs p.138. Heickero, R. (2014) Cyber Terrorism: Electronic Jihad, *Strategic Analysis* 38(4) pp.554-565.

[14] Ranstorp, M. (2007) The virtual sanctuary of al-Qaeda and terrorism in an age of globalisation. In Eriksson, J. and Giacomello, G. (eds.) *International Relations and Security in the Digital Age*, Routledge Advances in International Relations and Global Politics p.38. Brunst, P. W. (2010) Terrorism and the Internet: New Threats Posed by Cyberterrorism and Terrorist Use of the Internet. In Wade, M. and Maljevic, A. (eds.) *A War on Terror?: The European Stance on a New Threat, Changing Laws and Human Rights Implications*, Springer Science + Business Media, LLC p.53.

[15] Ditrych, O. (2014) *Tracing the Discourses of Terrorism: Identity, Genealogy and State*, Palgrave Macmillan p.122.

[16] Jackson, R. (2005) Language, Power and Politics: Critical Discourse Analysis and the War on Terrorism, *49th Parallel: An Interdisciplinary Journal of North American Studies* 15.

what constitutes cyberterrorism is clearly and intentionally being marginalised for the sake of framing specific actors as cyberterrorists. Public opinion polls, as the one cited at the beginning of this article, demonstrate that the creation of such a discourse is reaping results – the audience is reacting to such constructed frames and accepting them as a given. The end result is that the threat of cyberterrorism is, just like the threat of terrorism in general, be it chemical, biological or nuclear, having a significant effect on national policies[17], one led by the existing political discourse on terrorism, nicely fitted to the grand narrative of the War on Terror. That is, the narrative that cyberterrorists are, in reality, Salafist jihadi autonomous cells waging an electronic Pearl Harbour against the West. For this reason, specific attributes are used to describe the potential dangers stemming from terrorist use of the cyber sphere, including electronic, digital and cyber *Jihad*[18].

At the same time, actors that have and do engage in activities that can be considered within the narrower definition of what cyberterrorism is, are generally left out of the debate. Organisations such as Anonymous are mainly framed as "hacktivist" groups, using digital means for organisational purposes rather than to commit acts of terror[19]. They are not already labelled as a terrorist organisation and hence neither are their actions in the cyber sphere considered as acts of cyberterrorism. This understanding is maintained despite the fact that, for example, on April 7 each year, Anonymous runs the so-called #OpIsrael, in protest against Israeli policies towards Palestinians, with the aim of "erasing Israel from the Internet", attacking websites of Israel Defence Forces, the prime minister's office, Israeli banks and airlines[20]. Aside from using the cyber sphere to launch and carry out attacks on other computers and networks, groups claiming to be associated with Anonymous and contributing to #OpIsrael have also launched videos, threatening Israel with an "electronic Holocaust"[21]. And this is only one example of Anonymous activity in the cyber sphere. Others include attacks on government and company websites in countries such as Brazil, Spain, Syria, Iran, Italy, the United States and the United Kingdom; attacks on banking systems; and attacks and leaking of information from the Central Intelligence Agency, the Federal Bureau of Investigation, the Federal Trade Commission, and Stratfor[22], to mention a few.

The banking system has been defined as part of national critical infrastructure by a significant number of Western states, and therefore of interest for national security. The information leaked from security services could have contained either personal data of citizens or sensitive information of relevance to national security. And yet, none of these have been framed as cyberterrorist incidents in the general political discourse, as waging a War on Terror against Anonymous would not serve the purpose of a 'grand terrorism narrative'. Anonymous is not a traditional organisation, it is not linked to a specific territory of strategic interest, it does not promote a specific religious, ethnic, or socio-economic group in society, nor does it act on behalf

[17] 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*, RAND Corporation p.288.

[18] Heickero, R. (2014) Cyber Terrorism: Electronic Jihad, *Strategic Analysis* 38(4) p.557. Emphasis added.

[19] Cassim, F. (2012) Addressing the Spectre of Cyber Terrorism: A comparative perspective, *PER* 15(2) p.382.

[20] Segal, A. (2016) *The Hacked World Order*, Public Affairs: A Council on Foreign Relations Book p.36, 180.

[21] Zech, S. T. *Virtual Vigilantes: "Anonymous" Cyber-Attacks Against the Islamic State*, Political Violence @ a Glance, April 7, 2015. Available at https://politicalviolenceataglance.org/2015/04/07/virtual-vigilantes-anonymous-cyber-attacks-against-the-islamic-state/ [Accessed March 28, 2017 at 4.16 PM]

[22] Comninos, A. (2011) Information conflict and New Challenges to Peace Practitioners, *Peace Magazine* (October/November) p.16, 17. Kenney, M. (2015) Cyber-Terrorism in a Post-Stuxnet World, *Foreign Policy Research Institute* (winter) p.119.

of a particular state[23]. Therefore "fighting" Anonymous would not imply a need to topple a foreign regime, or "liberate" a territory, a state or its people. It does not fall into the existing narrative of fighting terrorism, and the group and its activities are therefore neither framed as such. Still, if the "psychological projection of fear" is the final attribute of cyberterrorism[24], does not an unidentifiable actor, attacking government websites and threatening an electronic Holocaust in a video that goes viral online fulfil the wider, if not even the narrower, requirements to be framed as a cyberterrorist actor, given the consensual definition above?

Getting the facts right

It is therefore seemingly obvious that a certain dichotomy is at play when it comes to what the consensual definition of what cyberterrorism is, and the process of framing who cyberterrorist actors are, creating a general political discourse on this issue[25]. This dichotomy requires attention and an attempt to contest the "selective, often wilful, misuse by actors seeking to advance partisan interests" when it comes to framing who is and who is not a terrorist in general[26], a notion that spills-over into the inquiry of cyberterrorism as well.

Cyberterrorist actors seem to be framed for a specific purpose, with specific geostrategic interests in mind. These frames are not questioned. Rather, they are replicated through mass media as well as academic discussions on cyberterrorism. And once they are assigned and accepted as a fact, what *could* happen starts weighing as much as what *is* actually the case[27]. If not even more so. This also removes the challenge of defining what cyberterrorism is, as focus is rather placed on who the actors are. As a result, onlookers are encouraged to identify any act by a group labelled as terrorist as automatically and necessarily a terrorist action, seeing terrorism as inextricably tied to the organisation itself, and not as a means of action[28]. The practice of framing cyberterrorists thus follows the logic of 'the power of a name', whereby once a label is assigned, the logic of why and how this was done disappears, and a series of normative associations is attached to the named subject[29]. Instead of having the analysis of potential threats of cyberterrorism pointing to the existence of new actors – given the consensual definition arrived at and the situation on the ground – already mapped terrorist organisations are artificially assigned a new capacity and a new label, that of cyberterrorists.

Cyberterrorism as a concept thus needs to be disentangled from the existing narrative of the War on Terror, framing cyberterrorist actors to suit specific political and geostrategic interests and wrapped in a political discourse devoid of reality. It is back to the drawing board for national security thinkers and decision makers. If we are to truly erect a national security system capable of developing resources to fend off potential terrorist attacks in the cyber sphere, a reference

[23] Zech, S. T. *Virtual Vigilantes: "Anonymous" Cyber-Attacks Against the Islamic State*, Political Violence @ a Glance, April 7, 2015. Available at https://politicalviolenceataglance.org/2015/04/07/virtual-vigilantes-anonymous-cyber-attacks-against-the-islamic-state/ [Accessed March 28, 2017 at 4.16 PM]

[24] Kenney, M. (2015) Cyber-Terrorism in a Post-Stuxnet World, *Foreign Policy Research Institute* (winter) p.122.

[25] Dunn Cavelty, M. (2008) Cyber-Terror – Looming Threat or Phantom Menace? *Journal of Information Technology and Politics* 4(1) pp.19-36. Jarvis, L. et al (2016) Analogy and Authority in Cyberterrorism Discourse: An analysis of Global News Media Coverage, *Global Society* 30(4) pp.605-623.

[26] Jackson, R. et al (2011) *Terrorism: A critical introduction*, Palgrave Macmillan p.108.

[27] Zulaika, J. (2010) The terror/counterterror edge: When non-terror becomes a terrorism problem and real terror cannot be detected by counterterrorism, *Critical Studies on Terrorism* 3(2) p.259.

[28] Jackson, R. et al (2011) *Terrorism: A critical introduction*, Palgrave Macmillan p.111.

[29] Bhatia, M. (2005) Fighting words: naming terrorists, bandits, rebels and other violent actors, *Third World Quarterly* 26(1) pp.5-22.

needs to be made back to the initial definitions that see *terrorism as action*, cyberterrorism included. In order to really know what we are speaking of when we use the term, the current political narrative on cyberterrorism needs to be deconstructed by exploring the divide between reality and discourse, breaking away from the established frames of cyberterrorist actors and developing security policies in line with actual threats and challenges and not wider political, geostrategic interests stemming from other concepts.

To this end, the terminology used in the announcement on the creation of the Global Internet Forum to Counter Terrorism is to be acknowledged[30]. The platform, created by Facebook, Microsoft, Twitter and YouTube is to enable these giants 'to take a hard line against terrorist or violent extremist content' on their hosted consumer services. Perhaps a small nudge, but one in the right way in terms of branding the content, and not the action of sharing it, as terrorist and/or extremist. The fact that the announcement clearly makes this distinction may show that gradually, the political discourse may be deconstructed in order to conform better to actual reality, and in a way characteristic of the cyber era – pioneered by the tech industry.

[30] Twitter, *Global Internet Forum to Counter Terrorism,* June 26, 2017. Available at https://blog.twitter.com/official/en_us/topics/company/2017/Global-Internet-Forum-to-Counter-Terrorism.html [Accessed June 29, 2017 at 1.58 PM]