Political Violence and Terrorism in Cyberspace

https://www.e-ir.info/2024/12/18/political-violence-and-terrorism-in-cyberspace/

MARIANO VARESANO, DEC 18 2024

The digital revolution and the introduction of the World Wide Web are some of the most significant and impactful global phenomena of the past three decades. The consequences of increasing global networked connectivity branch out into every aspect of daily life and international politics at such a speed that they are often elusive, both for the policy analyst and the policymaker. One of the (relatively) less explored areas of the digital revolution concerns the relationship between cyberspace[1] and political violence, with particular reference to instances in which digital tools are not facilitators of violent action but are its very ends, as well as the means through which it is perpetrated. Understanding the theoretical and practical possibility of cyberterrorism is precisely the purpose of this paper. Is it possible to conceive of a properly terrorist action taking place entirely in a digital environment? Has an attack that could be called cyberterrorism ever occurred? What are the methodological and operational differences between such an attack and a physical one, and what are the interpretive and theoretical differences for the terrorism scholar? These are the main questions guiding the present paper.

In the first part, I will introduce the concept of cyberterrorism by presenting the main definitional issues and some useful categorizations. The goal is not to find an unambiguous definition of the term but rather to clear the field of some of the terminological confusion by highlighting what *cannot* be called cyberterrorism. The second part will analyze five case studies of actions potentially labeled as terrorism conducted in cyberspace. I anticipate that none of the cases under consideration will be properly termed a cyberterrorist attack: The central assumption of this paper, which will be taken up extensively later, is that such an attack has not yet occurred. In the third part, I will set out some considerations of the consequences that the introduction of cyberspace might have on the concepts and practices of asymmetric warfare and terrorism. This part will be the most conceptual and speculative: Beyond the concrete risk of terrorist threats from cyberspace, we will use the latter to understand (and expand on) some of the characteristics peculiar to asymmetric conflicts. I will conclude with some thoughts on the future of political violence in cyberspace.

Definitional issues

The definition of cyberterrorism, like that of terrorism, is slippery and politically contested ground. The addition of the prefix “cyber” adds further confusion not only because of the vagueness and generality of an environment as intangible as cyberspace, but also because of the absence of any phenomenological reference of (unanimously recognized) cyberterrorist action. The attempt is, therefore, that of defining a phenomenon that has probably never occurred.[2] Despite this difficulty, the literature that attempts to define the concept is extensive.[3] Since the purpose of this paper is not to provide a precise definition of the phenomenon, I will proceed to draw its contours by exclusion, highlighting its essential features but especially its distinctions from other concepts pertaining to the cyber sphere.

In this respect, the work of Micheal Kenney[4] might be helpful. He distinguishes a cyberterrorist attack from a generic cyberattack, from an act of cyber warfare, and, even more relevantly, from an act of “hacktivism”.[5] In the first case, we define a cyberattack as an action carried out through digital tools aimed at disrupting, destroying, spying on, or stealing data and communications in a computer or network. Thus, the two main elements are the use of digital tools as a means of conducting the attack and the rendering of digital tools as also the target, while the motivations driving the attacker are indifferent (in most cases it is financial gain, in which case we speak of cybercrime or cyberfraud). If the motivation is politico-strategic and the actor behind the attack is a state (or a group

that can be traced back to a state), we are likely dealing with an act of cyberwarfare: Defined as a politically motivated cyberattack aimed at destroying networks and infrastructure of the targeted actor and ensuring that it cannot retaliate.[6]

The distinction between cyberterrorism and hacktivism is perhaps the most delicate. At first sight, the line seems very blurred: A "hacktivist" is a non-state actor who carries out offensive actions in cyberspace to advance a political claim. One would almost be tempted to translate into the cyber domain the famous maxim "someone's terrorist is someone else's freedom fighter", turning it into "someone's cyberterrorist is someone else's hacktivist". However, such relativism risks undermining some basic democratic freedoms related to the use of the Internet, such as the free expression of political ideas online. At present, in fact, in the absence of egregious acts of violence conducted through the network, there is a risk of extending the label "cyberterrorism" to include nonviolent acts such as defacing[7] a site or temporarily suspending a service, implicitly also broadening the label "terrorist" to individuals or groups who merely bring out a political instance through the web.

For similar reasons, it is important to distinguish cyberterrorism from the use of the Internet by terrorist groups. This is one of the most classic dichotomies about the definition of this term: A "narrow" definition that includes only those attacks that depend on cyberspace to be carried out (*cyber-dependent*) is contrasted with a "broader" one that includes all cases in which digital means merely facilitate the operations of terrorist groups (*cyber-enabled*).[8] Net of rare (albeit relevant) exceptions,[9] scholars of the phenomenon generally converge on a narrow definition.[10] This approach is also adopted in the present text, for two reasons. The first is to avoid bringing under the label "terrorism" actions that would not be included if they took place in the physical world (propaganda, training, financing through illegal activities, etc.). The second and more relevant reason takes up the point regarding freedoms mentioned above: Over-extending the category of (cyber)terrorism would produce the practical effect of making anti-terrorism legislation applicable to a very large number of actions conducted online. The many risks of such an extension of the concept include the possibility of repression of activists and dissidents[11] and the application of excessively severe penalties in the case of nonviolent actions such as simply consulting material produced by terrorist organizations and disseminated online.[12]

Not surprisingly, extended (and often hyper-dramatized) definitions of cyberterrorism have been adopted instrumentally over time by political figures (especially in the United States) to legitimize greater control over the digital sphere. Continued references to alleged "Digital Pearl Harbour", "Cyber 9/11", or "Cyber-Katrinas" serve, according to Pablo Mazurier, to "emphasize how important the preventive role of state power is in controlling the activities of users on the Internet while reinforcing in the collective unconscious the idea that, if these tragic occurrences have not yet materialized, it is only due to the work of law enforcement".[13] Examples of building a political discourse around the alleged terrorist threat from cyberspace are not lacking in Europe, either: In 2016, then French Interior Minister Cazeneuve proposed a European initiative against strong encryption of communications (the same used by messaging apps such as WhatsApp, and considered by many experts to be a useful tool for ensuring user privacy), because "many messages exchanged by terrorists would now be encrypted and intelligence would struggle to intercept them".[14] Beyond the practical utility of blanket opposition to encryption of communications ("there is no way to take strong encryption out of the hands of those who are determined to use it", as noted by digital rights attorney Nate Cardozo),[15] these examples clarify that the classic trade-off between individual liberty and collective security, already present in the physical world and central to issues of political violence and terrorism, translates perfectly into cyberspace and also results in the adoption of narrower or wider definitions of cyberterrorism.

Case studies

In this section, I will try to apply the categories presented above to some possible case studies. First, however, a premise is in order. The amount of small- to medium-scale cyberattacks occurring daily around the world is unprecedented, and increasing. Faced with such a quantity of possible case studies, it is necessary to give oneself selection criteria. I have adopted two: one temporal and one logical. The first criterion is to consider only attacks that have occurred at least five years ago, so as to ensure that the consequences can be estimated and that there has been sufficient investigation (although, as we shall see, even this time frame is often insufficient to get a clear picture). The second criterion is related to the need to put into practice the theoretical categories outlined in the

previous section: I will try to select a case that exemplifies each concept discussed so far.

The first case is purely speculative: It concerns an attack that allegedly took place as part of the Nagorno-Karabakh war in 1999, when hackers allegedly altered a hospital's databases by swapping patients' blood types, risking their deaths as a result of wrong transfusions. I found only one source[16] mentioning the case, citing "unconfirmed reports": The attack, therefore, might fortunately have never occurred. However, I chose to present it as illustrative of a case of "pure" cyberterrorism: It is an attack conducted through the network targeting a computer system (a hospital's database), with a political-strategic purpose (as a probable action carried out in the context of war, or at any rate without pursuing any individual gain), with a strong psychological effect of spreading terror among the population and the potential consequence of reaching a huge number of victims. Other possible examples, typically cited among the main risks of "pure" cyberterrorism, involve tampering with the control systems of critical infrastructure with high destructive potential such as dams or nuclear power plants. Up to this date, there has never been such an attack.

The second case under consideration is among the most famous and successful cyberattacks in history. In June 2010, a malware[17] named Stuxnet was introduced through a USB stick into the control system of the uranium enrichment plant in Natanz, Iran. Stuxnet took control of the facility's computer system and changed the speed of rotation of the turbines, which went out of control until they caught fire and exploded.[18] Stuxnet is remembered as "the first digital weapon"[19]: It is the first (and so far only) cyber tool capable of causing extensive physical damage to an infrastructure. Can this attack fall under the definition of cyberterrorism?

Stuxnet was designed in cooperation by the United States and Israel as part of the "Olympic Games" plan, created with the goal of sabotaging Iran's nuclear program. While from the point of view of means and targets the attack took place entirely in cyberspace and with cyber weapons, from the point of view of motivation and objectives this looks more like a classic cyberattack or act of cyber warfare than a cyberterrorist attack. First, the infrastructure hit coincides precisely with the strategic objective the attackers wanted to pursue: A nuclear infrastructure is hit to undermine nuclear developments. Thus, the "abstractness" and disconnect between material target and strategic objective typical of the "grammar" of terrorism[20] is absent. Second, there is a lack of evidence that inciting terror was among the attackers' goals. The infrastructure hit was far from population centers and the attack did not result in any deaths: Likely, the material target of the attack (slowing down or preventing Iran's enrichment of uranium) was far more important than any symbolic and psychological goals.

The third case concerns a hacker group linked to the Islamic State. Two months after the Caliphate was proclaimed in 2014, the @KhalifaHackers account emerged on Twitter, run by a hacker group claiming many attacks against "anti-Islamic" targets.[21] Among the operations conducted are the hacking of the app of the local newspaper "Albuquerque Journal" and, most importantly, the hacking of the Twitter profile of Centcom, the U.S. Central Military Command, in 2015. Similar operations are also conducted by a plethora of other various politically connected organizations. It is worth mentioning, for example, the "Syrian Electronic Army", a group of eight Syrian hackers that has carried out cyber operations on behalf of the Assad regime since 2011. The main targets hit (all during 2014) are variously accused of spreading fake news about the ongoing war (such as CNN, whose Facebook and Twitter profiles are hacked), spying on citizens (such as the company Microsoft and the phone app Angry Birds), or being direct political enemies (such as some Saudi government sites, defaced or seized).[22]

The problem with categorizing these kinds of operations as "cyberterrorist" is that although the motivations are political and the objectives include spreading panic and terror among the population, their intensity is far too low and their consequences meager. The point is effectively made by Peter Singer who, in describing similar operations conducted by al-Qaeda against Israeli websites or by the "Izz ad-Din al-Qassam Cyber Fighters" group against some U.S. banks, writes that "these attacks the equivalent of a crowd standing in your lobby blocking access or a gang of neighborhood kids constantly doing "ring and runs" at your front doorbell. It's annoying, to be sure, but nothing that would make the terrorism threat matrix if you removed the word 'cyber'".[23] To cite another effective physical metaphor, Alessandro Curioni describes DDoS attacks[24] (among the most widely used for this type of unsophisticated operation) as a "very intense and concentrated bombardment [after which] the system returns to normal operation. […] As if flights at an airport resumed normally after thousands of bombs have been poured over

it".[25] As much as the goals of the attackers include spreading terror among the population, the results are still far from that goal.

A relevant exception, taking up the case of "Cyber Caliphate", is the use of cyberattacks to expose the location of targets and thus make it easier to hit them physically. This is what happened in 2014 to activists from the site "Raqqa is Being Slaughtered Silently", which was dedicated to exposing atrocities committed by ISIS in the Syrian city of Raqqa. Through an email containing malware, the "Caliphate hackers" exposed their position, making them extremely vulnerable to violent reprisals.[26] In this case, the components of violence and terror are present, but they take shape outside of cyberspace, in the physical world. This is therefore an example of terrorist use of the Internet, rather than actual cyberterrorism.

We conclude our analysis of case studies with arguably the most famous hacktivist group in the world. Anonymous is not an organization, but rather a "fluid, loosely connected network of hackers, activists and pranksters who coordinate their activities on an ad hoc basis".[27] In some cases, it could be called a "brand" to be affixed to hacker operations of various kinds. The fluidity of the group makes the number of small attacks attributable to it endless: We will limit ourselves here to citing a single representative example case. In 2012 Anonymous gave operational support to a hacker group named OpIsrael in conducting a series of attacks against Israeli government sites, with the main purpose of defacing them by displaying messages in favor of the Palestinian cause.[28] These and other subsequent operations were framed by the attackers as "a new electronic war against the Israeli occupation", but in fact, they had the same effect as graffiti on government buildings would have in the physical world. Once again, alongside a political motivation and the purpose of instilling fear, there are technical capabilities that are still too limited to cause damage comparable to that of a physical terrorist attack.

Cyberspace, terrorism, and asymmetric warfare

The aforementioned Alessandro Curioni calls warfare conducted in cyberspace "the mother of all asymmetric warfare".[29] Indeed, the immateriality of this environment, its pervasiveness, and the possibility of operating in it while easily concealing one's identity make it an ideal place for this kind of struggle. In this section I will consider cyberspace purely as a concept: Apart from its concrete uses—which, as we have seen, have so far been very limited, at least as far as terrorism is concerned—I will attempt to identify its potential and conceptual role in the theory and practice of terrorism and asymmetric warfare. To do so I will make use of Alessandro Colombo's analysis[30] of the elements of terrorism and asymmetric warfare, and try to transpose its main concepts into cyberspace.

Colombo first identifies three elements of the "grammar" of terrorism: (1) abstractness (mentioned earlier: it consists of the disconnect between the material target of the attack and the political/strategic objective), (2) a peculiar spatiality (hitting targets indiscriminately, even randomly) and (3) a convoluted temporality (the major effect of terrorism is not the harm caused by an attack in the present but the threat of even greater suffering to be inflicted in the future).[31] The analysis goes on to describe two other characteristics peculiar to terrorism: its justification in the name of exceptionalism, of a supreme good that requires the use of violence outside the norm, and its theatricality, a spectacularization of violence that amplifies its spread and psychological effect.[32] The other concepts I will borrow from Colombo's work concern asymmetric warfare, described as a clash in which asymmetry is manifested on the planes of power (in terms of military capabilities: the stronger will want to raise the level of confrontation while the weaker will want to keep it low intensity), space (the stronger will want to confine the use of violence to the battlefield and sanction its territory, the weaker will want to extend violence by encroaching on the opponent's territory) and information (the stronger will want a perfectly transparent battlefield, the weaker will want to hide as much as possible).[33]

How are these characteristics transformed when entering cyberspace? Let us answer this question by starting with the "grammar" of terrorism. The first difference between attacks against physical structures and operations against digital targets lies in the line of defense: While in physical space states equip themselves with armies and counter-terrorism agencies capable of defending the civilian population from attacks, in cyberspace the first line of defense is the civilian population.[34] Indeed, behind the computer screens of companies and critical infrastructures are

employees and ordinary citizens who could allow malware to break into the computer system even by simply opening the wrong email. In cybersecurity jargon, such instances are known as “human vulnerabilities” and are by far the most common cause of successful cyber attacks.[35] Because of such vulnerabilities, the preferred targets of any cyberterrorists will always be civilian infrastructure even if the long-term political target is a country’s state or military: The nature of cyberspace thus incentivizes the abstractness typical of the terrorist act.

Secondly, the spatiality and temporality of cyberterrorism are then equally undefined. Once placed on the network, a piece of malware has the potential to spread even beyond the control of the attackers themselves: The risk of “friendly fire”, that is, of infecting one’s own systems with the malware one is using as a weapon, is a real danger that every malicious cyber actor seriously considers. If the weapon being used is so elusive as to be beyond the control of the attackers themselves, cyberterrorism represents an extreme amplification of the peculiarities of terrorism in terms of spatiality and temporality: The threat is extended indefinitely in both time and space.

Thirdly, the geographic element, which has always been very important in the considerations of terrorists and revolutionaries (think of the debate on the effectiveness of “urban guerrilla warfare” or “foquismo” from the forests, or the role of mountains in the formation of “sanctuaries” for many fighters) evidently loses meaning: The new obstacles for the cyberterrorist are the protection systems from time to time employed by the target, and the new opportunities for attack are the vulnerabilities and flaws in the systems that are discovered.

What about the theatricality of the act? Can an action conducted exclusively in cyberspace provoke the same emotional reaction of terror caused by a bomb or mass shooting? The absence of the psychological and emotional element is often cited among the reasons for the lack of actual recorded cyberterrorist attacks.[36] However, a study conducted in 2016 on the psychological effects of cyberterrorism would seem to show that a cyberterrorist attack is capable of generating the same states of anxiety and demands for greater security and control from authority as a physical attack.[37] Indeed, given the pervasiveness of the Internet and digital tools in the daily lives of much of the world’s population, it is understandable their impairment has the potential to generate panic in a similar way that a physical threat would. Developments in the fields of the Internet of Things and Artificial Intelligence are digitizing more and more activities of daily life, generating new potential targets, ever closer to the population. A computer screen, home appliances, or a company’s computer system can thus be the “stage” for terrorist theatrical action in no different way than a crowded square can be.

Given the elements of temporal permanence of the threat and pervasiveness of the targets just highlighted, the justification for the cyberterrorist act may not be that of exceptionalism, as is often the case with traditional terrorism (because the malware will remain in circulation indefinitely, potentially even after the supposed “emergency” is over), rather it will probably be closer to the Maoist concept of permanent warfare, or, to quote two influential contemporary authors of Chinese military strategy, “limitless warfare”.[38]

How does asymmetric warfare change in light of the characteristics of cyberspace highlighted? On the plane of *power*, it seems that cyber weapons provide a strong advantage to the weaker party, given their relative ease of access and potential to target the weak points (systems’ vulnerabilities) of an (especially Western) computerized and digitized society. On the plane of *space*, the attempt of the stronger actor to “sanitize” its territory to preserve it from violence is futile in cyberspace: Connectivity is the fundamental and defining characteristic of this environment, and the protection of a portion of it for securitarian purposes can only come at the expense of democratic freedoms (as is the case, for example, in China with the “Great Firewall”). Even on the *information* level, the strongest actor sees its attempt to have a perfectly transparent battlefield thwarted because of the encryption and anonymity offered by the network. These are the reasons why the struggle waged in cyberspace may indeed become “the mother of all asymmetrical wars”.

Conclusions: the future of political violence in cyberspace

If cyberspace offers such substantial advantages to weaker actors willing to engage in a form of violent political struggle against a stronger enemy, why have we never witnessed an actual cyberterrorist attack? One frequent explanation (that of the absence of theatricality and a strong psychological effect) has already been addressed in the

previous section, along with reasons why it may not be convincing.

A second reason paradoxically stems from one of the advantages of cyber weapons: anonymity. Those who conduct violent action for political purposes often have an interest in claiming it unequivocally. Perpetrators must make themselves visible to gain concessions[39] and influence the target's behavior. Cyberspace, however, surrounds each action with a blanket of uncertainty that makes it extremely difficult to attribute it with certainty to one perpetrator, instead making multiple conflicting claims virtually impossible to confirm or disprove.

The third (and probably the main) reason why we may never have witnessed a cyberterrorist attack is, trivially, that of technical capabilities. While it is true that many of the simpler attacks examined above (defacement of sites, intrusion into social pages) "show[ed] the absence of capabilities of the attacked […] rather than reflecting the capabilities of the attackers",[40] it is also true that more complex attacks capable of generating significant damage require extraordinary technical capabilities in many fields of knowledge. To use Peter Singer's words again:

Taking down a hydroelectric generator […] doesn't just require the skills and means to get into a computer system. It's also knowing what to do once you are in. To cause true damage requires an understanding of the devices themselves and how they run, the engineering and physics behind the target. […] To be blunt, neither the 14-year-old hacker in your next-door neighbor's upstairs bedroom, nor the two- or three-person al-Qaida cell holed up in some apartment in Hamburg are going to bring down the Glen Canyon and Hoover dams.[41]

These words date back to 2012. Time will tell whether the technical difficulties in causing significant damage through cyberspace will continue to ensure its security from terrorist attacks. Regardless of its practical use for terrorist purposes, in any case, the introduction of cyberspace is already an extremely significant innovation in the complex framework of international security and the practice of asymmetric warfare.

Notes

[1] In this text I will use the word "cyberspace" in the generic sense of a digital environment in which data and information are exchanged.

[2] Michael Kenney, *Cyber-Terrorism in a Post-Stuxnet World*, *Orbis* 59, no. 1 (2015): 111–28, https://doi.org/10.1016/j.orbis.2014.11.009.

[3] For some examples, see Laura Mayer Lux, "Una Definición de Ciberterrorismo,"*Revista Chilena de Derecho y Tecnología* 7, no. 2 (2018): 5–25, https://doi.org/10.5354/0719-2584.2018.51028; Lee Jarvis and Stuart Macdonald, "What Is Cyberterrorism? Findings from a Survey of Researchers," *Terrorism and Political Violence* 27, no. 4 (2014): 657–78, https://doi.org/10.1080/09546553.2013.847827; and the wide (although not very recent) gathering of definitions in Rabiah Ahmad and Zahri Yunos, "A Dynamic Cyber Terrorism Framework,"*International Journal of Computer Science and Information Security (IJCSIS)* 10, no. 2 (2012): 149–5.

[4] Micheal Kenney, *op. cit.*

[5] Union of the words "*hacker"* and "*activism*," it is intuitively definable as activism carried out through actions in cyberspace.

[6] Micheal Kenney, *op. cit.,* p.114.

[7] *Defacing* is the act of illicitly changing or replacing the home page of a website.

[8] United Nations Office on Drugs and Crime (UNODC), *Counter-Terrorism in the International Law Context* (Publishing and Library Section, United Nations Office at Vienna, 2021), p.177; "Cybercrime Module 14 Key Issues: Cyberterrorism", UNODC, accessed June 10, 2023, https://www.unodc.org/e4j/zh/cybercrime/module-14/key-issues/cyberterrorism.html; Lee Jarvis and Stuart Macdonald, *op. cit.,* p.659; Babak Akhgar and Eric Luiijf,

"Definitions of Cyber Terrorism," essay, in *Cyber Crime and Cyber Terrorism Investigator's Handbook* (Amsterdam: Elsevier, 2014).

[9] Eben Kaplan, "Q&A: Terrorists and the Internet," *The New York Times*, March 6, 2006, https://archive.nytimes.com/www.nytimes.com/cfr/international/slot2_030606.html, cited in Micheal Kenney, *op. cit.*

[10] However, it is important to note, as UNODC does at the site cited in footnote 8, that this approach is not prevalent among policymakers.

[11] UNODC, "Cybercrime Module 14 Key Issues: Cyberterrorism", *op. cit.*

[12] Fabio Vigneri, "Cyberterrorismo: Realtà O Finzione? Profili Problematici Di Definizione e Contrasto," *Opinio Juris*, July 26, 2021, p.22, accessible at https://www.opiniojuris.it/cyberterrorismo-realta-o-finzioneprofili-problematici-di-definizione-e-contrasto/.

[13] Pablo Mazurier, "Sul Concetto Di Cyber-Terrorismo e Cyber(in)Sicurezza", *Centro Interdipartimentale Di Studi Strategici, Internazionali e Imprenditoriali (CCSSII)*, Università Degli Studi Di Firenze, 2017, p.5.

[14] Carola Frediani, *Guerre Di Rete*, (Roma: Laterza, 2017), cap. "Reti di terrore".

[15] Carola Frediani, *Op. Cit.*

[16] Babak Akhgar and Eric Luiijf, *op. cit.*, p.16.

[17] An umbrella term that generically indicates "malicious software". It is often confused with the term "virus", which indicates a specific type of malware. In this case, the malware in question was technically a "worm".

[18] Information security expert Giorgio Sbaraglia gave a detailed and technical description of the Stuxnet case (in italian) at https://www.giorgiosbaraglia.it/la-guerra-cibernetica-caso-piu-famoso/.

[19] Carola Frediani, *op. cit.,* cap. "Stuxnet, la prima arma digitale".

[20] Alessandro Colombo, "Terrorismo, Radicalismo Politico e Guerra Asimmetrica," essay, in *Violenza e Politica: Dopo Il Novecento* (Bologna: Società editrice il Mulino, 2020), p. 180.

[21] Carola Frediani, *op. cit.,* cap. "Reti di terrore".

[22] Babak Akhgar and Eleanor Lockley, "Understanding the Situational Awareness in Cybercrimes: Case Studies," essay, in *Cyber Crime and Cyber Terrorism Investigator's Handbook* (Amsterdam: Elsevier, 2014).

[23] Peter W. Singer, "The Cyber Terror Bogeyman," Brookings, July 28, 2012, https://www.brookings.edu/articles/the-cyber-terror-bogeyman/.

[24] Distributed Denial of Service: This is one of the technically simplest forms of cyberattack, in which a large amount of data traffic is directed at a target to make it temporarily unavailable to other users.

[25] Aldo Giannuli and Alessandro Curioni, *Cyber War: La Guerra Prossima Ventura* (Milano: Mimesis, 2019), p.54.

[26] Carola Frediani, *op. cit.,* cap. "Reti di terrore".

[27] Micheal Kenney, *op. cit.*

[28] Cohen, Daniel. "Cyber terrorism: Case studies." In *Cyber Crime and Cyber Terrorism Investigator's Handbook*.

Elsevier, 2014 p.167.

[29] Aldo Giannuli and Alessandro Curioni, *op. cit.,* p.49.

[30] Alessandro Colombo, *op. cit.*

[31] Alessandro Colombo, *op. cit.,* pp.180-183.

[32] Alessandro Colombo, *op. cit.,* pp.183-188.

[33] Alessandro Colombo, *op. cit.,* pp.191-196.

[34] Aldo Giannuli and Alessandro Curioni, *op. cit.,* p.49.

[35] Aldo Giannuli and Alessandro Curioni, *op. cit.,* p.60.

[36] Robert Jackson, Jørgen Møller, and Georg Sørensen. Relazioni internazionali. 5th ed. Milano: Egea editore, 2020, p. 411.

[37] Michael L. Gross, Daphna Canetti, and Dana R. Vashdi, "The psychological effects of cyber terrorism,"*Bulletin of the Atomic Scientists* 72, no. 5 (August 4, 2016), https://doi.org/10.1080/00963402.2016.1216502.

[38] Quiao Liang, Wang Xiangsui, *Guerra senza limiti,* Libreria editrice goriziana, Gorizia, 2001.

[39] Robert Jackson, Jørgen Møller, and Georg Sørensen, *op. cit.,* p. 412.

[40] Carola Frediani, *op. cit.,* cap. "Reti di terrore".

[41] Peter Singer, *op. cit.*

References

All translations were made by this author. All websites were last visited on 5th September 2024, at 16:00 ECT.

Ahmad, Rabiah, and Zahri Yunos. "A Dynamic Cyber Terrorism Framework." *International Journal of Computer Science and Information Security (IJCSIS)* 10, no. 2 (2012): 149–58.

Akhgar, Babak, and Eleanor Lockley. "Understanding the Situational Awareness in Cybercrimes: Case Studies." Essay. In *Cyber Crime and Cyber Terrorism Investigator's Handbook*. Amsterdam: Elsevier, 2014.

Akhgar, Babak, and Eric Luiijf. "Definitions of Cyber Terrorism." Essay. In *Cyber Crime and Cyber Terrorism Investigator's Handbook*. Amsterdam: Elsevier, 2014.

Cohen, Daniel. "Cyber terrorism: Case studies." In *Cyber Crime and Cyber Terrorism Investigator's Handbook*. Elsevier, 2014. https://doi.org/10.1016/c2013-0-15338-x.

Colombo, Alessandro. "Terrorismo, Radicalismo Politico e Guerra Asimmetrica." Essay. In *Violenza e Politica: Dopo Il Novecento*. Bologna: Società editrice il Mulino, 2020.

Frediani, Carola. *Guerre di Rete*. Roma: Laterza, 2017.

Giannuli, Aldo, and Alessandro Curioni. *Cyber War: La guerra prossima Ventura*. Milano: Mimesis, 2019.

Gross, Michael L., Daphna Canetti, and Dana R. Vashdi. “The psychological effects of cyber terrorism.” Bulletin of the Atomic Scientists 72, no. 5 (August 4, 2016): 284–91. https://doi.org/10.1080/00963402.2016.1216502.

Jackson, Robert, Jorgen Moller, and Georg Sorensen. *Relazioni internazionali*. 5th ed. Milano: Egea editore, 2020.

Jarvis, Lee, and Stuart Macdonald. “What Is Cyberterrorism? Findings from a Survey of Researchers.” *Terrorism and Political Violence* 27, no. 4 (2014): 657–78. https://doi.org/10.1080/09546553.2013.847827.

Kaplan, Eben. “Q&A: Terrorists and the Internet.” The New York Times, March 6, 2006. https://archive.nytimes.com/www.nytimes.com/cfr/international/slot2_030606.html.

Kenney, Michael. “Cyber-Terrorism in a Post-Stuxnet World.” *Orbis* 59, no. 1 (2015): 111–28. https://doi.org/10.1016/j.orbis.2014.11.009.

Mayer Lux, Laura. “Una Definición de Ciberterrorismo.” *Revista Chilena de Derecho y Tecnología* 7, no. 2 (2018): 5–25. https://doi.org/10.5354/0719-2584.2018.51028.

Mazurier, Pablo. “Sul Concetto Di Cyber-Terrorismo e Cyber(in)Sicurezza.” *Centro Interdipartimentale di Studi Strategici, Internazionali e Imprenditoriali (CCSSII), Università degli Studi di Firenze*, 2017.

Singer, Peter W. “The Cyber Terror Bogeyman.” Brookings, July 28, 2012. https://www.brookings.edu/articles/the-cyber-terror-bogeyman/.

United Nations Office on Drugs and Crime (UNODC). *Counter-Terrorism in the International Law Context*. Publishing and Library Section, United Nations Office at Vienna, 2021.

United Nations Office on Drugs and Crime (UNODC). ”Cybercrime Module 14 Key Issues: Cyberterrorism.” UNODC. Accessed June 10, 2023. https://www.unodc.org/e4j/zh/cybercrime/module-14/key-issues/cyberterrorism.html.

Vigneri, Fabio. “Cyberterrorismo: Realtà O Finzione? Profili Problematici Di Definizione e Contrasto.” Opinio Juris, July 26, 2021. https://www.opiniojuris.it/cyberterrorismo-realta-o-finzioneprofili-problematici-di-definizione-e-contrasto/.