Cyberterrorism 2.0 or terrorist use of social media: the Islamic State case

Terrorismo cibernético 2.0 ou uso terrorista das redes sociais: o caso do Estado Islâmico

Rev. Bras. Est. Def. v. 7, nº 2, jul./dez. 2020, p. 59-80
DOI: 10.26792/RBED.v7n2.2020.75210
ISSN 2358-3932

GILLS VILAR-LOPES
MARCELO DE ALMEIDA MEDEIROS

INTRODUCTION

Cyberspace — and, more specifically, the Internet — becomes a common source of threats to national defence and international security (Brazil 2020; Costa 2012, 53–66), especially after the September 11 attacks. Besides, the rise and popularisation of so-called social media in the mid-2000s enhance the militancy of the most diverse social groups, including terrorist ones.

In this context, we problematise the international terrorism issue to point out which factors contribute to the emergence and development of new cyberterrorism 2.0. This article focuses on a particular recent aspect of cyberterrorism (thus, not about the entire phenomenon): new ways of using cyberspace, especially social media. Hence, we try to expose several inputs — and possible outputs — of social media usages by terrorists in terms of political[1]

Gills Vilar-Lopes — Lecturer in International Relations and Head of the Postgraduate Program in Aerospace Sciences (PPGCA) at the Brazilian Air Force University (UNIFA). PhD in Political Science from the Federal University of Pernambuco (UFPE). Specialised Course in Cybersecurity from the National Defense University (NDU), Washington D.C. Researcher at RedeCTIDC/Pró-Defesa IV (CAPES/MD), GEESI/UFPB and NEPI/UFPE. Editorial Advisor of the RBI/ABIN. This article is a result of research carried out in the Volunteer Service Program (PSV) of the Brazilian Ministry of Defence's Pandiá Calógeras Institute and complemented by discussions about "Terrorism and cyber threats in the 21st century" at a public hearing of the Foreign Relations Commission (CRE) of the Federal Senate in 2017.
Marcelo de Almeida Medeiros — Ph.D. in Political Science from the Institut d'Études Politiques de Grenoble and Habilitation Thesis from the Institut d'Études Politiques de Paris – Sciences Po. Full Professor of Comparative International Politics at the Federal University of Pernambuco – UFPE (Recife, Brazil) and PQ-1C Research Fellow of the National Council for Scientific and Technological Development – CNPq. He was Rio Branco International Relations Chair at St Antony's College, University of Oxford, Visiting Scholar at the Sciences Po, and Simon Bolivar Political Science Chair of the Institut des Hautes Études de l'Amérique Latine – Université Sorbonne Nouvelle – Paris III.

proposes, provided that we can better understand the complex current scenario of international security. Therefore, we do not ponder how and why terrorist groups use cyberspace or the Internet as a whole, but rather how they use specific and recent networks such as Facebook, Twitter, and YouTube.

Briefly, our main objective is to analyse the recent manifestations of cyberterrorism — which is an international phenomenon by itself — in the light of International Security Studies. In this regard, we try to promote a dialogue between specific data methods of collecting and analysing, as follows:

> Case study. Given the extraordinary international evidence the Islamic State (IS)[2] terrorist group has provoked the media, academy, and foreign policy of major great powers, we delve into a specific category of terrorist groups: paramilitary Islamic radicals/extremists. Here, we research and analyse the period between June 2014 and April 2015. The first period marks the IS self-proclamation, and the moment great powers start to pay more attention to the transnational claim of a caliphate in the Middle East. The second period (early 2015) is the apex of the terrorist use of social media worldwide.
>
> Discourse analysis. After monitoring social media during the cut time, as mentioned above, we sought to build an overview of the main subjects — Trending Topics (TTs) and hashtags — related to the terrorist activity on social media.

To bring the discussion of terrorism into cybersecurity, we describe and apply the qualitative framework so-called Stakeholders, Activities and Motives in the realm of cybersecurity (SAM), proposed by Kremer and Müller (2014, 41-58). we seek to understand the inputs around social media use by Islamic extremist groups, notably the IS case.

Accordingly, this work has three parts. The first one defines cyberterrorism 2.0 and social media, focusing on international relations. Subsequently, the inputs of cyberterrorism 2.0 are analysed; that is to say, we seek to identify by whom (Stakeholders), how (Activities), and why (Motives) social media are used with terrorist intentions. Social media use by specific terrorist groups has eventually engendered certain outputs in the secret services and National Defence bodies. In other words, we claim that states seek to combat such groups with the same virtual tools used to spread terror on the Internet and beyond, namely social media.

CYBERTERRORISM 2.0

As Hoffman (2017, 22) observed, "Like social media — another grossly overused term that has similarly become an indispensable part of the ar-

got of the early twenty-first century — most people have a vague idea or impression of what terrorism is [...]".

There is no consensus about terrorism, although some essential elements in these definitions are more common: political goals (Hoffman 2017, 25); violent unlawful acts or threats and actions to produce effects beyond the victims (Gonçalves and Reis 2017). The most classical definition comes from Hoffman (2017, 109), who stated that terrorism is "the deliberate creation and exploitation of fear through violence or the threat of violence in the pursuit of political change."

Nevertheless, to illustrate this conceptual difficulty, the United Nations (UN) itself struggles to define what terrorism is (Annan 2005). However, what we have is an old UN official statement that indirectly provides the following meaning to terrorism:

> criminal actions designed or calculated to provoke a state of terror in the general public, in a group of people or certain people, which have political ends and which are unjustifiable, regardless of their political, philosophical, ideological, racial, ethnic, religious claims or otherwise. (United Nations 1995, free translation).

As our work is directly related to the Internet — one of the main cyberspace facets — the analyses presented throughout this study refer specifically to the so-called cyberterrorism, a term made up in the 1980s by Barry Collin, a senior researcher at the Institute for Security and Intelligence in California (Cavelty 2007, 19-36).

In the same way, the term terrorism uncovers multiple definitions (Hoffman 2017, 22–5), and the concept of cyberterrorism is sometimes comprehensive and vague (Cavelty 2007, 20; Gercke 2009). Nevertheless, this theme's political and academic interest grows significantly, especially from the 2000s, when conceptual differences between policymakers and academics emerge (Crosston 2014, 253–67). However, there is practically a consensus about the most accepted meaning referred to as cyberattacks,[3] which generate fear and direct against national strategic structures,[4] such as hydroelectric, gas, energy, and air transport networks (ATN).

On the one hand, cyberspace promotes a high degree of decentralised, instantaneous, and sometimes anonymous sharing of information, which positively marks many societies' quotidian societies. On the other hand, it raises technical, logistical, and strategic risks for international security professionals and scholars (Demchak 2014, v-x). Regarding national security issues, this Manichaean trait of the Web lies in the fact that the concepts of internal and external enemies are merging more and more in this new domain. Otherwise stated, even though the era of social media has

emerged in the fields of humanitarian action, social activism, and development (Karlsrud 2014, 141–60), it also ends up being transformed into a strategic, operational environment for terrorists and jihadists influence (Kuehl 2014, 24–42).

In a global sense, social networks are not an exclusive issue to the Information Age. They have existed for centuries since they consist of many social groups whose individuals/elements interrelate by affinity. Nonetheless, with the spread of the Internet, especially in the mid-2000s, the term "social media" referred exclusively to websites and virtual applications that simultaneously support several social networks. Information sharing is one of the main particularities (Ferreira 2011, 208–31).

Despite the countless definitions of social media found in the most diverse areas of knowledge, there is still confusion related to them. An example of this conceptual imprecision is in Sterne's (2010) proposal, which differentiates six broad social media categories, precisely: (i) microblogs, (ii) media sharing, (iii) social media, (iv) blogs, (v) forums, (vi) bookmarking, and (vii) websites for opinions and recommendations. By separating the first three categories, the author also classifies different subcategories of websites and apps that have practically the exact characteristics of content sharing — such as Facebook, Twitter, and YouTube.

Aiming to standardise our analysis[5], we suggest a unique category of "social media", bringing together websites and applications such as Facebook, Twitter, and YouTube in the same group. Since these three web services perform practically the same tasks, differentiating one from the other only by technical limits — e.g., the number of characters or bytes. In conclusion, cyberspace incorporates the Internet because it is the only social media "many-to-many" (Sterne 2010, xvi) and is an interconnected digital infrastructure (Kremer and Müller 2014, 42).

As the years go by, social media leave the fields of leisure and work and incorporate more political aspects, i.e., creating a situation in which people and social groups can agree with their governments[6] and go against them (Karlsrud 2014, 154). Nevertheless, social media in the 21st century is not just about social revolutions and government repressions, as we usually see in papers and news, for instance, 2010/2012 Arab Spring and the 2019 Hong Kong Umbrella Movement.

Within the strategic uses of these tools, the term cyberterrorism is becoming popular in the scope of Defence and International Security Studies (Kuehl 2014, 5). Before putting them into context, it is necessary to remember the very definition of terrorism to understand how both terms apply to International Security Studies. From this, it is possible to assimilate the meaning of cyberterrorism 2.0.

Considering the association of cyberterrorism with cyberattacks, Cavelty (2010, 2) creates a hierarchical typology of cyber conflicts widespread in studies on the topic. Among the five types, cyberterrorism — involved in producing fear through some infrastructural damage — is in second place among cyber conflicts that can generate more potential damages to people, businesses, and states.

This mainstream position in the international security literature — which culmination is Cavelty's typology — does not entirely satisfy our objectives here. The reason for this is that, for instance, social media use by terrorist groups does not fit as an act of cyberterrorism in the eyes of this restricted meaning. Consequently, a broad enough concept is needed to, on one side, frame the extremist use of social media as a terrorist act along the lines of the UN definition; and, on the other, incorporate cyberattacks by terrorists to cause damage to strategic structures.

In this regard, our contribution intends to update the concept of cyberterrorism to what was practised by terrorist groups in cyberspace during the 2010s — now named cyberterrorism 2.0, that is, criminal cyber activities caused by a group or individual linked to a terrorist group, whose reasons or motivations are unjustified, to cause a state of terror to one or more people, *through psychological or physical damage.*

Typifying the crime of cyberterrorism 2.0 must comply with the judicial principle of the legal reserve. Hence, it must be previously defined as illegal; therefore, it is necessary to cultivate a law that guides it. Gagnon (2008, 46–65) recalled this when he stated that terrorism comprises both national security and criminal issues. Conversely, to legislate in an environment as unusual as cyberspace is complex, as reminded at (i) the 2001 Budapest Convention on Cyber Crimes and (ii) the fact that "several worrying criminal acts not officially defined by the authorities as terrorism may have been influenced, at least in part, by online terrorist propaganda" (Adl 2015a).

For instance, from this perspective, a posting of the video with decapitations of 21 Coptic Christians by an Islamic extremist group, as a direct message to other followers of that religion (*Folha de S. Paulo* 2015), for us, is an act of cyberterrorism 2.0. Additionally, the act of sharing and liking this type of content will also constitute a crime, even if practised by individuals who are not part of the original group of the post, if the justification/reason for this (cyber) action is the same as the original.

This forewarning is necessary because media outlets generally illustrate their reports with excerpts from videos posted by terrorist groups. In rare exceptions, these mass media provide links to videos and photos in full, under the argument of informing and often intentionally shocking

the public to call more attention to the reported case. In the Copts execution example, the act of liking or sharing the original post can be framed as a type of crime: an apology to terrorism or another correlate, but it is not defined as cyberterrorism 2.0 in the terms we defend here. Only those who encourage and support the message shared initially to cause psychological damage to a specific person or group are those who practice the act of cyberterrorism in its updated version 2.0.

Therefore, we define cyberterrorism 2.0, which analyses how terrorists or terrorist groups use social media to spread fear inside and, mainly, outside the Internet. Thus, it is a type of the cyberterrorism 2.0 genre that can cover other subareas, such as encrypted means — e.g., mobile telephone, electronic mail, and SMS services, to articulate terrorist cells. Along with the mapping of potential terrorist targets using geolocation software and online maps, the terrorist performance on the Deep Web; and financial support received via cryptocurrency.

In this sense, Terrorism Studies involve different areas and fields of knowledge to explain this violent phenomenon. At the international security level, we can see how cyberspace and specifically social media have boost terrorist activities such as recruitment and propaganda (Ford 2020) to achieve the main goal of spreading terror. Figure 1 shows the logic behind our argument, situating, at the same time, both the epistemic and operational position around cyberterrorism 2.0.

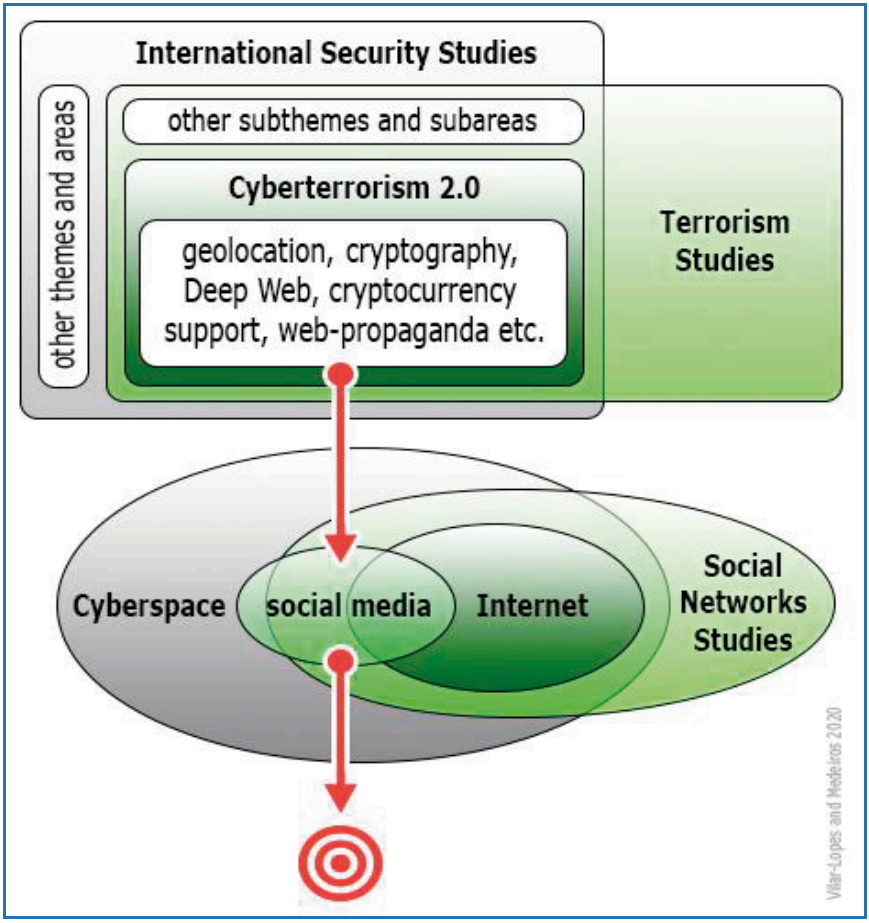

Figure 1 — Cyberterrorism 2.0 definition.
Source: the authors.

As Figure 1 shows, cyberterrorism 2.0 has its logic, explicitly: to demonstrate that social media can also be used for non-peaceful purposes. An example of this is comparing such a negative form of operation with a positive defence one in peacekeeping processes:

> There is a mushrooming of efforts to make use of big data and social media in countries in crisis. [...]Concurrently, social media is strengthening the opportunities of rebels to communicate their mes-

> sage internally, to domestic and external supporters, and directly to traditional media outlets. (Karlsrud 2014, 147).

When analysing the idea behind cyberterrorism 2.0, we see that it is contrary to Karlsrud's. In other words, while there are efforts to operate social media constructively, for example, in countries experiencing conflict, it becomes a means for terrorist groups to spread their message to the whole world through social media to bring terror to their targets. This is the hypothesis that the analyses of the following section seek to corroborate.

INPUTS OF CYBERTERRORISM 2.0 IN THE LIGHT OF THE SAM FRAMEWORK

This section seeks to highlight (i) who cyber terrorists are, (ii) how they act, and (iii) what leads them to use social media to promote cyberterrorism 2.0. These three issues are in strict accordance with the three variables set of the qualitative analysis tool named Stakeholders, Activities and Motives (SAM), by Kremer and Müller (2014), which applies to specific cybersecurity and international relations cases.

As seen in the previous section, most of the literature tends to associate cyberterrorism with cyberattacks by terrorists. Accordingly, the link between cybersecurity and international relations seems clear. As we advocate, it is necessary to broaden the concept of cybersecurity when discussing studies on terrorism, including logical/informational and psychological attacks — such as the publication of content on social media. Radical religious groups have recognised, for years, the multifaceted role that images, audio and videos play in psychological warfare (Katz 2015).

Even though the SAM's creators indicated that it aims to deal with the conceptual challenges of categorising stakeholders, activities, and motives within the scope of cybersecurity (Kremer and Müller 2014, 44), such a framework fits perfectly into this section's objectives, as it has a holistic character. However, when we deal with cybersecurity, the authors are more concerned with property and political damage caused to strategic structures — e.g., cyberattacks and intrusions into networks and computers.[7]

This thinking is very similar to the scholars' first cyberterrorism conception (cyberterrorism 1.0) seen in the previous section. Also, as with cyberterrorism 2.0, we adapt SAM to make it fit into the terrorist use of social media problems — and not the other way around — and involve cyber incidents (Kremer and Müller 2014, 45) as well as an international

phenomenon related to cyberspace, as the cyberterrorism 2.0 case shows us. In this sense, Table 1 presents three dimensions behind SAM.

Table 1
SAM framework

Stakeholder	Who?	Who is mandating, who is executing and who is affected?
Activities	What?	What activities they carried out, and what are the results in terms of defects?
Motives	Why?	Why have the activities been carried out, what are the underlying motivations and intentions?

Source: Kremer and Müller 2014, 46.

As we notice, the three sets of SAM responses correspond, essentially, to the three inputs of cyberterrorism 2.0. The research design excels in this endeavour, and we divide it into three smaller parts. The first one aims to find out who the stakeholders of cyberterrorism 2.0 are, through a quantitative survey of the profiles of terrorist groups on social media, and with the help of Webometrics methodology. The second part investigates the actions and effects on the terrorist targets through discourse analysis (DA) of the leading virtual profiles in the first phase of the research. Finally, the third part seeks to list the reasons for these activities. In doing so, we could complete the SAM framework.

Accordingly, we consider Webometrics, which includes all content accessible from the Internet and its web search engines — such as Bing, Google, Yahoo! — and other online tools. One of the webometric species is big data, which refers to the large volume of publications on virtual social media websites, videos, and blogs (Demchak 2014, viii; Karlsrud 2014, 142).

Although less than half of the terrorist groups had websites in 1998, almost all of them, including Al-Qaeda, had a space on the Internet around five years later. Shortly after that milestone, YouTube starts to function as a tool favouring fundamentalist advertisements (Gercke 2009, 53). In June 2014, the terrorist group that calls itself the Islamic State (IS) acts in an even more radical way concerning those opposed to creating a caliphate in parts of Iraq and Syria. One way to draw the world's attention and supporters to its cause is social media use. Other groups quickly followed this way of acting. The three main paramilitary Islamic fundamentalist groups operating in the Middle East and Africa — Al-Shabab, Al-Qaeda and Boko Haram — began to copy it.

Therefore, chart 1 shows the interest of Internet users in these groups between 2014 and 2015. It provides accurate data regarding the general research interest of four terrorist groups, ranging from 0 to 100 in that period. Nevertheless, we take into account the relative interest rather than the absolute. That is why, even though it does not appear in Chart 1, in relative terms, Al-Qaeda is by far the most searched terrorist group in the last 15 years. For this reason, it is natural that the peak (100) remained with that group in May 2004 — a few weeks after the attacks on the Madrid Metro, which allegedly attributed to it. However, once the research is from June 2014, it is noted that Al-Qaeda lost prominence on the Internet for Boko Haram and IS, and only in mid-April 2015, for example, it regained prominence.

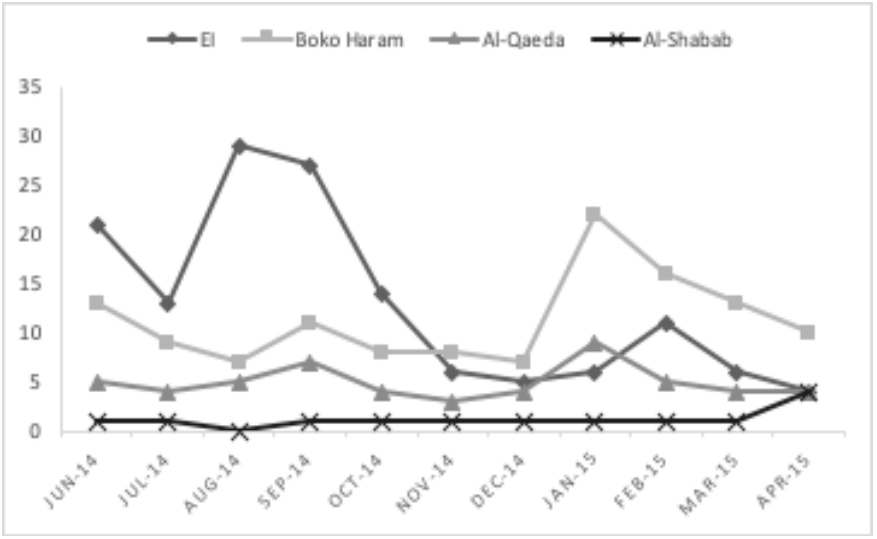

Chart 1 — Internet interest in terrorist groups (2014-2015)
Source: the authors based on data obtained in Google (2015)

Based on the first SAM variable, Stakeholder, we aim to identify who is in charge of cyberterrorism 2.0 between 2014 and 2015. For this purpose, we carry research out on the social medium used mainly by extremist Islamist groups such as IS, namely, Twitter (Adl 2015a, 10; 2012).[8] Through this aggressive social media strategy, IS transforms how terror-

ist groups and their supporters reach, influence, and recruit worldwide (Adl 2015a, 10).

IS Twitter numbers are impressive. In 2014, more than 12 official accounts were just for the organisation's central leadership, with the @alItisam account gaining over 50,000 followers. To get a comparative idea, the website Topsy (2015) shows the list of tweets per day on a given topic or over the last month. Consequently, we verify that between March 27 and April 26, 2015,[9] IS maintained its position as the most mentioned terrorist group on Twitter, according to Chart 2.

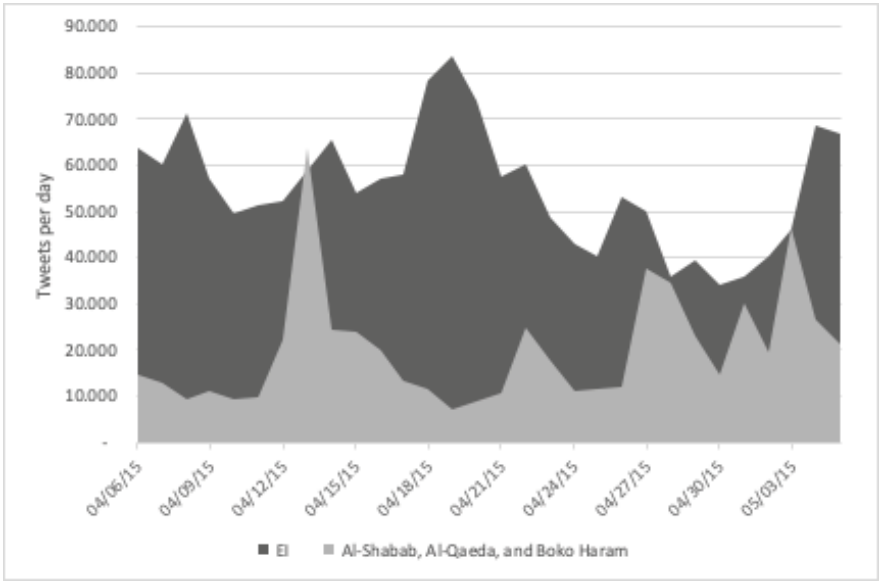

Chart 2 — Daily tweets about terrorist groups (April 6.- May 5, 2015).
Source: the authors based on data obtained in Topsy (2015).

Chart 3, in turn, shows the hashtags that refer to each of the four terrorist groups under analysis, in one month, between April 6 and May 5, 2015.

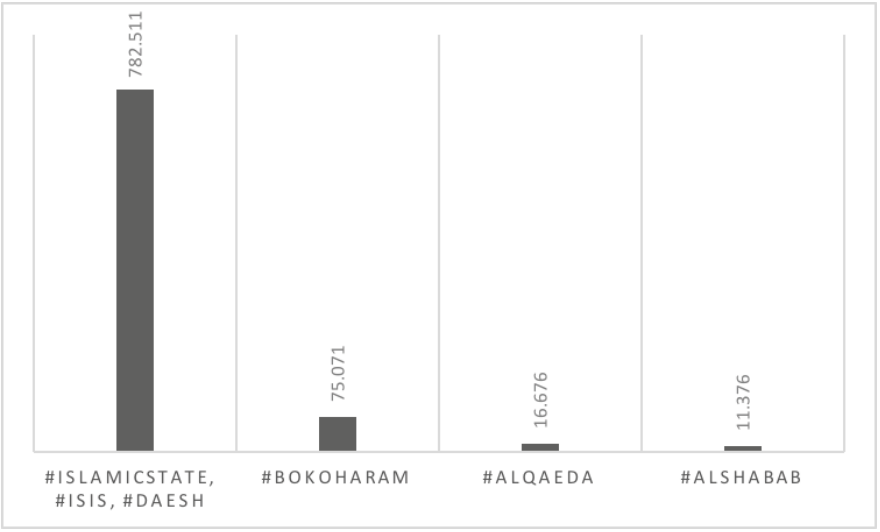

Chart 3 — Hashtags from terrorist groups on Twitter (April 6. — May 5, 2015).
Source: the authors, based on data obtained in Topsy (2015).
Note: Once IS is best known for ISIS and DAESH, the following amounts of hashtag citations are combined: #ISIS (605,670), #DAESH (113,510) and #ISLAMICSTATE (63,331).

Through Charts 2 and 3, it is possible to highlight two critical findings. Firstly, both the tweets and the hashtags about IS alone surpass all three other terrorist groups together within the proposed interval.[10] Secondly, as in the real world, the reactions of Twitter users follow the repercussions of the activities and physical attacks of these terrorist groups. For example, the only time IS loses its first position in the ranking shown in Graph 2 is on April 14, 2015, when Amnesty International reports — and the mainstream media reflects — that Boko Haram has already kidnapped at least 2,000 women (*Al Jazeera* 2015) — including 270 Nigerian Catholics in 2014.[11] Another example is the summit (49,721 tweets per day) of this time series that happened precisely on April 19, 2015, when ISIS releases a video about the execution of 30 Ethiopian Christians in Libya (*Folha de S. Paulo* 2015).

Significantly, we can say that one of the main objectives of these groups, which is to attract attention, is being achieved. However, it is challenging to measure the extent to which the contents (videos, texts, and images) shared on social media by such groups cause psychological damage, especially because Twitter, for example, is more used in Western countries. Nonetheless, it is possible to measure some perception or feeling from this

medium. For instance, the Topsy Sentiment Score[12] seeks to define how Twitter users react to specific subjects on a 0-to-100 scale. The closer a subject or hashtag is to 100, the more well-received or approved by social media. In other words, above 50 points, a positive score is attributed to the subject or hashtag.

When searching for the scores of the hashtags listed in Chart 3,[13] we observe there is a negative feeling towards all terrorist groups, as shown in Chart 4.

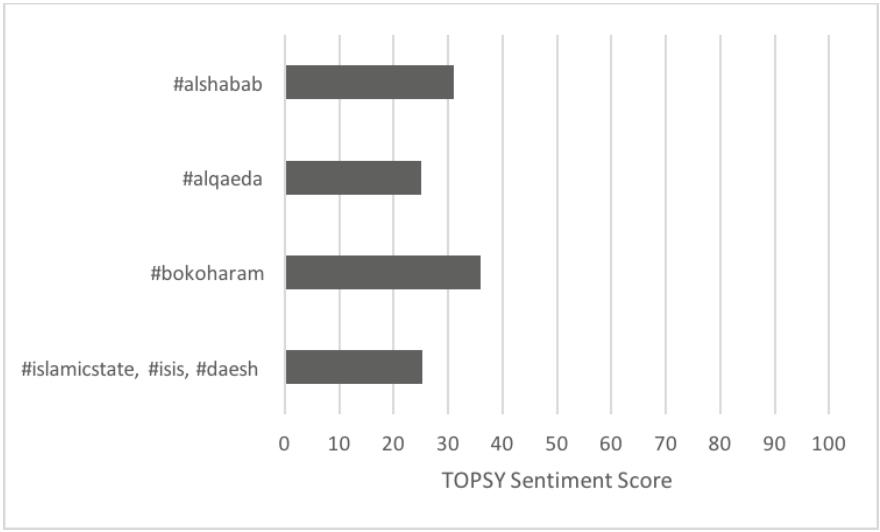

Chart 4 — "Sentiment" towards terrorist groups on Twitter on April 6 — May 5, 2015)
Fonte: the authors, based on data obtained in Topsy (2015).
Note: As IS is well known by ISIS and DAESH, the average score of its hashtags is taken, namely: #ISIS (26), #DAESH (32) and #ISLAMICSTATE (18).

Based on the cyberterrorism 2.0 definition, Chart 4 does not point out to whom and what psychological damage the contents posted by terrorist groups on Twitter causes. However, it demonstrates, in a way, that there is a tendency for users affected by the messages to disapprove of those terrorist activities, such as the sharing of execution videos, slogans, information about the city taken. In this bias, we can infer the score proposed by Topsy, which reflects the rejection of the shared content or aversion to terrorist groups by most Twitter users. Therefore, the score shown in

Chart 4 dialogues with SAM framework points to the disapproval of the messages' content by most affected users (stakeholders).

As stated, Islamic State is the terrorist group that best manages social media, especially Twitter and YouTube, to spread its messages, recruit followers, including Westerners, and encourage its supporters to take part in this process. However, it is impossible to say social media play a sufficient role in this recruitment (Adl 2014).

There are several motivations behind the terrorist use of the Internet, such as: disseminating advertisements, describing and publishing the reason for its activities, and recruiting or contacting members and donors for their cause (Gercke 2009, 53). However, the following question arises concerning recruitment: is it possible to have such activity on the Internet?

Aiming to clarify this doubt, the European Convention on the Prevention of Terrorism, signed in 2005 and applicable since 2009, must be referred. This international treaty defines *recruitment* for terrorism as the request for someone to commit or participate in a terrorist act or participate in an association or group to contribute to the practice of one or more terrorist acts on behalf of that association or group (European Council 2005).

As above-mentioned, many Westerners nations, including American (Adl 2015a, 16–7), have enlisted in the paramilitary forces of these groups, mainly in IS, whose propaganda machine not only attracted thousands of recruits but also helped Syria and Iraq to emerge as the preferred destinations of this new generation of extremists (Adl 2015a, 1).

This new generation of future terrorists permits closing the panorama of the inputs of cyberterrorism 2.0. Table 2 presents the final version of the SAM adapted and filled with what we expose so far.

Table 2
SAM Framework applied to cyberterrorism 2.0

Stakeholder	*Who* is ordering the use of social media for terrorist purposes?	*terrorist* groups such as: - Al-Shabab - Al-Qaeda - Boko Haram and, mainly, - IS
	Who is executing the terrorist activities on social media?	- *individuals* directly linked to terrorist groups. - *individuals* supporting the causes contained in messages shared on social media.
	Who is affected by the terrorist use of social media?	- even though it is challenging to measure psychological damage on social media, it can be said that the majority (approximately 70%) of *individuals* who have Twitter accounts disapprove of such groups.
Activities	*What* activities the terrorist use of social media carries out?	*non-destructive*, to *influence* public opinion and potential recruits.
	What are the results in terms of damage from the terrorist use of social media?	- *empirically*, Westerners will fight on the field and funding is sent to terrorist groups. - *psychologically and inductively*, about 70% of tweets show a high sense of disapproval for the four groups analysed. - *physically*, no strategic structure was damaged directly or indirectly.
Motives	*What* motivations lead carrying terrorist activities out on social media?	- *ideologically*: proliferating the Islamic faith. - *psychologically*: recruiting followers. - *financially*, empower supporters to take part in their activities. - *politically*, support the idea of the foundation of an Islamic State between Iraq and Syria.

Source: the authors.

CONCLUSION

The terrorist use of social media has engendered, in addition to the inputs seen in this work, some technological and political outputs. A technological example is that companies that own social media websites, such as Twitter, blocked (Garcia 2015) and closed (Adl 2014b) accounts that supported followers and even members of Al-Shabab and IS. However, by excluding accounts associated with terrorist groups, companies seem to stimulate a sort of Procrustean dilemma applied to cyberterrorism 2.0;

namely, the fewer accounts there are, the fewer potential intelligent sources of terrorist activity will exist (Adl 2012).

We can speculate that the mimicry the military will use is in two stages. The first is the observation of how terrorist groups use social media for massive recruiting. The second stage concerns a needed blend between different methods of espionage and sabotage, something very close to a junction between social[14] and reverse engineering, in what we can call "reverse social engineering". This seems to be a very complex task since the Internet — an environment in which social media are inserted — has a potential not yet measurable and in self-expansion. This seems to be the ideal scenario for the proliferation of cyber benefits and ills — the case of cyberterrorism 2.0.

Briefly and strategically speaking, there are some motivations for the use of social media by terrorist groups that we can summarise:

Make it impossible, in most cases, the consecutive charge for the content and publication, since the publisher's anonymity can be guaranteed with a simple fake profile or by use of more technical devices to mask or even hide the actual upload location where a post is.

Make it possible to reach many people practically across the globe.

Transmit various media types for free and instantaneously (text, image, voice, and video).

By applying the SAM framework in the IS case, we could have a big picture about who is responsible for manipulating social media to promote terror for political purposes, what are the results in terms of damage from the terrorist use of social media and, finally, what motivations lead terrorist activities out on these online tools.

Therefore, it is evident that the terrorist use of social media — the inputs this article sought to discuss — by paramilitary fundamentalist groups, such as IS, prove to be quite effective in their attempts, despite the strategic action of civilian and military intelligence services have emerged as an output that sates have found out to fight against cyberterrorism 2.0.

REFERENCES

Adl. 2011. "Al Shabab launches apparent Twitter campaign". http://www.adl.org/combating-hate/international-extremism-terrorism/c/shabaab-launches-twitter.html.

_____. 2012. "Tweeting for terror". http://www.adl.org/combating-hate/international-extremism-terrorism/c/tweeting-for-terror.html.

_____. 2014a. "Hashtag Terror: how ISIS manipulates social media". http://www.adl.org/combating-hate/international-extremism-terrorism/c/isis-islamic-state-social-media.html.

_____. 2014b. "ISIS faces resistance from social media companies". https://www.adl.org/blog/isis-faces-resistance-from-social-media-companies.

_____. 2015. "Homegrown Islamic Extremism in 2014: the rise of ISIS & sustained online recruitment". https://www.adl.org/sites/default/files/documents/assets/pdf/combating-hate/homegrown-islamic-extremism-in-2014-the-rise-of-isis-and-sustained-online-recruitment.pdf.

Al Jazeera. 2015. "Report: At least 2,000 women abducted by Boko Haram". http://www.aljazeera.com/news/2015/04/nigeria-boko-haram-150414043301574.html.

Annan, Kofi. 2005. "Uma estratégia mundial de combate ao terrorismo." *Público*, Lisboa, 12 Mar, http://www.publico.pt/espaco-publico/jornal/uma-estrategia-mundial-de-combate-ao-terrorismo-10842.

Barreto, Eduardo M. 2007. "Terrorismo Cibernético e cenários especulativos". *Revista Brasileira de Inteligência* 3, no. 4: 63–76.

Brazilian Institutional Security Office, GSI. 2019. "Glossário de Segurança da Informação." *Brazil's Republic Presidency*, https://www.in.gov.br/en/web/dou/-/portaria-n-93-de-26-de-setembro-de-2019-219115663.

_____. 2020. "National Cybersecurity Strategy." *Brazil's Republic Presidency*, http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10222.htm.

Cavelty, Myriam D. 2007. "Cyber-Terror — Looming Threat or Phantom Menace? The Framing of the US Cyber-Threat Debate". *Journal of Information Technology & Politics* 4, no. 1: 19–36.

_____. 2010. "Cyberwar: concept, status quo, and limitations". *CSS Analysis in Security Policy* 71: 1–3.

Costa, Carlos E. B. 2012. "Tendências mundiais e seus reflexos para a defesa brasileira". *Revista Brasileira de Inteligência* 7: 53–66.

Crosston, M. 2014. "Phreak the speak: the flawed communications within cyber intelligentsia". In *Cyberspace and International Relations: theory, prospects and challenges*, edited by J. Kremer and B. Müller, 253–67. Heidelberg: Springer.

Demchak, Chris C. 2014. "Foreword". In *Cyberspace and International Relations: theory, prospects and challenges*, edited by J. Kremer and B. Müller, v–x. Heidelberg: Springer.

European Council. 2005. "Convention on the prevention of terrorism". https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/196.

Ferreira, Gonçalo C. 2011. "Redes sociais de informação: uma história e um estudo de caso." *Perspectivas em Ciência da Informação* 16, no. 3: 208–31.

Folha de S. Paulo. 2015. "Estado Islâmico divulga vídeo que mostra a execução de cristãos etíopes". *Folha de S. Paulo* (Abr.). http://www1.folha.uol.com.br/mundo/2015/04/1618601-estado-islamico-divulga-video-que-mostra-a-execucao-de-cristaos-etiopes.shtml.

Ford, Peter. 2020. "Combatting terrorist propaganda". *Journal of Policing, Intelligence and Counter-Terrorism* 15, no. 2: 175–86. DOI: 10.1080/18335330.2020.1780298.

Gagnon, Benoît. 2008. "Cyberwars and cybercrimes". In *Technocrime: technology, crime and social control*, edited by Stéphane Leman-Langlois: 46–65. London: Willan Publishing.

Garcia, Gabriel. 2015. "Estado Islâmico ameaça de morte fundador do Twitter". *Info* (Mar.). https://exame.com/tecnologia/estado-islamico-ameaca-de-morte-fundador-do-twitter.

Gercke, Marco. 2009. *Understanding cybercrime: a guide for developing countries*. Geneva: UN/ITU.

Gonçalves, Joanisval Brito, and Marcus Vinícius Reis. 2017. *Terrorismo: conhecimento e combate*. Niterói: Ímpetus.

Google. 2015. "Google Trends." http://goo.gl/3fh9Wd.

Hoffman, Bruce. 2017. *Inside terrorism*. 3rd ed. New York: Columbia University Press.

Karlsrud, J. 2014. "Peacekeeping 4.0: harnessing the potential of Big Data, social media, and cyber technologies". In *Cyberspace and International Relations: theory, prospects and challenges*, edited by J. Kremer and B. Müller, 141–60. Heidelberg: Springer.

Katz, Rita. 2015. "Follow ISIS on Twitter: a special report on the use of social media by jihadists". *SITE Intelligence Group*. http://news.siteintelgroup.com/

blog/index.php/entry/192-follow-isis-on-twitter-a-special-report-on-the-use-of-social-media-by-jihadists.

Kremer, J., and B. Müller. 2014. "SAM: a framework to understand emerging challenges to states in an interconnected world". In *Cyberspace and International Relations: theory, prospects and challenges*, edited by J. Kremer and B. Müller: 41–58. Heidelberg: Springer.

Kuehl, Daniel T. 2014. "From cyberspace to cyberpower: defining the problem". In *Cyberspace and International Relations: theory, prospects and challenges*, edited by J. Kremer and B. Müller: 24–42. Heidelberg: Springer.

Nicol, Mark. 2015. "We can't find enough whizzkids, says British Army as it struggles to recruit technical experts for secret unit intended to combat ISIS". *Daily Mail* (April). http://www.dailymail.co.uk/news/article-3035191/We-t-whizzkids-says-British-Army-struggles-recruit-technical-experts-secret-unit-intended-combat-ISIS.html.

Raposo, Álisson C. 2007. "Terrorismo e contraterrorismo: desafio do século XXI". *Revista Brasileira de Inteligência* 3, no. 4: 39–55.

Sterne, Jim. 2010. *Social media metrics*. New Jersey: John Wiley & Sons.

Topsy. 2015. "Topsy Sentiment Score". http://topsy.com.

United Nations. 1995. "A/RES/49/60". http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/49/60.

Wendt, Emerson. 2011. "Ciberguerra, inteligência cibernética e segurança virtual: alguns aspectos." *Revista Brasileira de Inteligência* 6: 15–26.

NOTAS

1. When we talk about political meanings social media use by terrorist groups, we are bringing the classic Hoffman (2017)'s terrorism conception.
2. It is also known as the Islamic State of Iraq and the Levante (ISIS) or its Arabic version DAESH.
3. A cyberattack can be defined in many ways. One of the most famous in Brazil is provided by the Republic Presidency: a deliberate and unauthorized attempt to access or manipulate information or make a system inaccessible, non-integral, or unavailable (Brazilian Institutional Security Office 2019).
4. See Barreto (2007, 63–76), Cavelty (2007, 19–20; 2010, 1–3), Gercke (2009, 51), Raposo (2007, 39–55) and Wendt (2011, 15–26).
5. It is also considered that Sterne's reference work on social media is from 2010. Since then, all online sharing and relationship websites and services have incorporated each other's functions. For example, Facebook and Instagram share videos, as well as being used as a microblog.
6. Google Transparency Report can measure some results of this bias change in social media use.
7. Cybersecurity turns to best practices to prevent the security attributes of information — availability, integrity, confidentiality, and authenticity — from being put in check. However, when such a subfield of Computer Science is brought to the analysis of International Relations, its concept ought to be extended to examine issues other than computational — for example, policies — in the same sense that the Copenhagen School proposes the extension of the Security concept.
8. Facebook and YouTube have acted quickly to delete content published by such groups, making it difficult to investigate these two social media accurately.
9. This is one of the limitations of that website: it allows comparative research in a short period; between the day it is researched and exactly 30 days before.
10. The website Topsy allows checking such information only for the last 30 days.
11. The reaction of the international media was the creation of the #BringBackOurGirls campaign on social media, calling the attention of political leaders to the fact that the case had been neglected.
12. Such a score can only be seen and measured in the last thirty days, individually for each of the hashtags, at www.topsy.com. That is why the limitation of this part of the research and why the analysis was restricted to the period from April 6 to May 5, 2015. However, the index proposed by Topsy is quite accurate, especially when comparing the negative scores of the groups analyzed with those of other more "accepted" international

themes, such as certain sports teams, which have, on average, positive scores above 75.

13. #slamicstate, #isis, #daesh, #alshabab, #bokoharam and #alqaeda, the first three are combined into one for the same reasons listed in the note of Chart 3.
14. In the scope of Information Security, social engineering is the ability to access denied information through persuasion; that is, it is presumed that the asset that most exposes Information Security to risks is the human element.

CYBERTERRORISM 2.0 OR TERRORIST USE OF SOCIAL MEDIA:
THE ISLAMIC STATE CASE

ABSTRACT

Cyberspace has become a common source of international security threats, especially after September 11. The emergence and popularisation of so-called social media have enhanced the militancy of the most diverse groups, including terrorist ones. This article problematises international terrorism, pointing out the causes and effects of this 21st-century phenomenon that we name cyberterrorism 2.0. Thus, we focus on the cyberterrorism studies that analyse social media usage's inputs and outputs by terrorist groups. Through Webometrics and the framework Stakeholders, Activities and Motives in the realm of cybersecurity (SAM), we aim to explain, in the light of International Security Studies and through the Islamic State case study, how cyberterrorism 2.0 arises, develops and impacts national security.

Keywords: Cyberterrorism; International Politics; International Security; Social Media.

RESUMO

O ciberespaço tem se tornado uma fonte corriqueira de ameaças para a segurança internacional, sobretudo após o 11 de setembro de 2001. O surgimento e a popularização das chamadas redes sociais *on-line* potencializaram a militância dos mais diversos tipos de grupos, inclusive terroristas. Este texto problematiza o tema do terrorismo internacional, no sentido de apontar quais as causas e efeitos desse fenômeno inerente ao século XXI que aqui nominamos de Terrorismo Cibernético 2.0. Foca-se, assim, na vertente dos estudos sobre Terrorismo Cibernético voltada para a análise dos *inputs* e *outputs* da utilização das redes sociais pelos grupos terroristas. Por meio da webometria e da ferramenta de análise *Stakeholders*, Ações e Motivos na Segurança Cibernética (SAM), objetivamos explicar, à luz dos Estudos de Segurança Internacional e por meio do estudo de caso do Estado Islâmico, como esse fenômeno surge, desenvolve-se e se reflete na segurança internacional.

Palavras-chave: Mídias Sociais; Relações Internacionais; Segurança Internacional; Terrorismo Cibernético.

Recebido em 01/07/2020. Aceito para publicação em 21/04/2021.