ITSS
International Team
For the Study of Security
Verona

Tech Giants' Role in Countering the "Media Jihad"

by Rita Sasso

ITSS Verona Magazine, Vol. 1, n. 2

Fall/Winter 2022

Tech Giants’ Role in Countering the “Media Jihad”

Rita Sasso

To cite this article: Rita Sasso, *Tech Giants’ Role in Countering the “Media Jihad”*, ITSS Verona Magazine, Vol. 1, no. 2, Fall/Winter 2022.

Keywords: Warfare, Disinformation, Cyberterrorism, Tech Giants

ITSS Verona website: https://www.itssverona.it/itss-magazine

LinkedIn: https://www.linkedin.com/company/itss-verona/

Instagram: https://instagram.com/itss_verona?igshid=YmMyMTA2M2Y=

Twitter: https://twitter.com/itssverona

Published online: December 30th, 2022

Abstract: Since the last decades of the 20th century, war has deeply changed. New actors have entered the scene, fighting for new goals and using new methods of warfare. Particularly, scholars have conceptualised a new way of waging war based on the use of (dis)information to disrupt the morale of the enemies and gain strategic advantage. In this context, the Internet and social media are becoming increasingly effective and pervasive in shaping public opinion, providing violent groups with unprecedented tools to advance their causes. This essay seeks to analyse and assess the role of the major tech companies (Tech Giants) in preventing malicious actors from exploiting their platforms for their interests.

The essay will first examine the new relevance of cyber warfare, in particular analysing the case study of IS "Media Jihad", and the failure of tech companies in countering the threat of the "Media Jihad"; then, it will argue that there is an increasing involvement of Tech Giants, in collaboration with States, in fighting back the new cyber menaces.

In April 2016, "Media Operative, You Are a Mujahid, Too" was published online by the Islamic State (IS). This 55-page Arabic-language document represents a sort of motivational handbook, dealing with the Islamist propaganda strategy and information warfare. By asserting that "media weapons [can] actually be more potent than atomic bombs," the authors wanted to promote the idea of a "Media Jihad".[1] Through this statement, they were capable of describing a crucial fact: warfare was evolving and the adaptation to its transformations was paramount in order to succeed. As a matter of fact, starting from the last decades of the 20th century, a new type of warfare developed. Mary Kaldor describes this phenomenon with the term "new wars", pointing out that new wars are to be understood in the wider context of globalisation processes.[2] According to Kaldor, the expression "new wars" refers to a new logic of "doing war" more than to an empirical category per se. Apart from new actors, new goals, and new forms of finance, what is most interesting about new wars for the purpose of the present analysis concerns the new methods of warfare. Indeed, if old wars were fought exclusively through military means, in new wars physical encounters are rare and political means of waging war become more and more used.[3] Along the same line as Kaldor, Frank G. Hoffman, leading thinker of the "hybrid warfare" theory, emphasises the involvement of different actors and different modes of warfare in modern conflicts. Taking a cue from the debate on new wars and hybrid warfare, some scholars have attempted to enlighten the increasing importance of information warfare. Particularly, Russian military theorists and analysts highlight that the aim of "gibridnaya voyna" (hybrid warfare) is to undermine the spirit of the

[1] Charlie Winter, "Media Jihad: The Islamic State's Doctrine for Information Warfare," King's College London: ICSR (2017): pp. 1-24, https://icsr.info/wp-content/uploads/2017/02/ICSR-Report-Media-Jihad-The-Islamic-State%E2%80%99s-Doctrine-for-Information-Warfare.pdf, 17-18.

[2] See note above, 4.

[3] Mary Kaldor, "In Defence of New Wars," *Stability: International Journal of Security and Development* 2, no. 1 (March 7, 2013): pp. 1-16, https://doi.org/10.5334/sta.at, 2.

enemy by the use of economic, political and informational means, rather than the traditional military ones.[4] In the last decades, “cyberspace” has gained an enormous strategic relevance acquiring the status of alternative battlefield in many conflicts; meanwhile, the Internet and social media are becoming increasingly effective and pervasive in shaping public opinion, providing violent groups with unprecedented tools to advance their causes.[5] In this respect, many authors enlighten a process of “media weaponization”, meaning the exploitation of social media to influence the morale and the spirit of enemies, gaining strategic superiority in the case of a direct confrontation.[6] In the process of “media weaponization”, have social medias had only a passive role? Or have they tried to actively counter this process, breaking the cyber military network?

A New Warfare: Hashtags as Weapons

Cyberspace offers several strategic advantages: “high connectivity, low latency, low cost of entry, multiple distribution points without intermediaries, and a total disregard for physical distance or national borders”.[7] The exploitation of these ambiguities, particularly effective for a non-state actor as the Islamic State (IS), aims to manipulate, disinform, and confuse public opinion. As Emerson T. Brooking and Peter W. Singer argue, “Iraq had changed dramatically in the years since the 2003 United States-led invasion”, but not enough.[8] In fact, on the one hand, a process of technological modernization had widened the Iraqi users on the Internet, from 150.000 to 4 million; while, on the other hand, the ongoing conflict between the Shiite majority and the Sunni minority created a climate of suspicion and hate among the population. This context paved the way for the IS attack on the city of Mosul. Indeed, in the summer of 2014, fighters of the self-declared Islamic State invaded northern Iraq.

The offensive, organised online and launched with the hashtag #AllEyesOnISIS, was preceded by a campaign of the terror characterized by the diffusion of content, such as videos and

[4] Ofer Friedman, “Hybrid Warfare or Gibridnaya Voyna?”, The RUSI Journal, 162:1 (2017): pp. 42-49,https://doi.org/10.1080/03071847.2016.1253370, 42-45.

[5] Fabio Rugge, “Mind Hacking”: Information Warfare in the Cyber Age, Politeia, 34:132 (2018). https://www.ispionline.it/it/pubblicazione/mind-hacking-information-warfare-cyber-age-19414

[6] Peter W. Singer, “LIKEWAR : the Weaponization of Social Media”. (S.L.: Mariner Books, 2019), 4-11.

[7] See note 5.

[8] Singer, “LIKEWAR”, 4.

photos depicting tortures and executions of prisoners. A climate of terror spread among the Iraqi military forces and many soldiers defected. Thus, the IS managed to occupy Mosul without much effort.[9] The IS is broadly recognised as a large terrorist organization, but the massive use of propaganda and social media is what sets it apart from any other terrorist group. Indeed, the IS uses the method of "trend-hijacking", consisting in the spread of a certain message or narrative by a network of "bots" (automated programs that can interact with other users on the Internet), in order to reach three main goals: first, demonstrating that the international community is heavily unable to counter them, both on the virtual and the real battlefield; second, spreading fear and anxiety in the public opinion; finally, attracting and recruiting new fighters from all over the world.[10]

This pervasive presence online had disastrous consequences in the real world: "in Iraq, at least 30.000 civilians would be killed by the group; in Syria, the deaths were literally incalculable in the chaos of the civil war"; the number of terrorist attacks soared.[11] Junaid Hussain, a Britain hacker of Pakistani origin, also known with the battle name of Abu Hussain al-Britani, was one of the principal organisers of the "Cyber Caliphate" hacking group. By his death in 2015, he had managed to recruit roughly 30.000 volunteers from all around the world, mainly through Twitter.[12]

At this point, public opinion began to wonder whether tech companies in control of social media were doing something to counter this "Media Jihad". Tech Giants, the major tech companies of the Silicon Valley (Google, Facebook, and Twitter) were particularly thrust under the spotlight. Many argued that they were just looking the other way at their economic interests, or worst "facilitating terrorism"[13]. Indeed, especially Facebook and Twitter were blamed for their incapacity to cope with new responsibilities, deriving from their increasing power. In America, in 2015, a $1 billion lawsuit was filed against Facebook by terrorist attack victims' relatives, with the accuse of

[9] See note 6.
[10] Jarred Prier, "Commanding the Trend: Social Media as Information Warfare", Strategic Studies Quarterly, 11:4 (2017): pp. 50-85, http://www.jstor.org/stable/26271634, 54-62.
[11] Peter W. Singer, "LIKEWAR", 153.
[12] See note above, 147-150.
[13] "Tech Giants Are under Fire for Facilitating Terrorism," The Economist, June 8, 2017, https://www.economist.com/international/2017/06/08/tech-giants-are-under-fire-for-facilitating-terrorism.

having “knowingly provided material support”[14] to the terrorists, letting them exploit online platforms to reach their malicious intents. Even though the lawsuit was ultimately dismissed, victims continued to file lawsuits after every new act of terrorism. Thus, at least in this first phase of “media weaponization”, the Tech Giants’ role seemed to be quite passive. Attached to the visions of themselves as the realm of free speech, they were not able - or pretended not - to understand the inherent danger of a mild stand against such a pernicious phenomenon: the transformation of the Internet from the realm of free speech to the realm of “bellum omnium contra omnes”.

Tech Giants’ Reactions

Although many have criticised the passive role of Tech Giants in countering cyberwars and particularly “Media Jihad”, tech companies have experienced a significant policy shift in their relatively brief lives. In the case of Twitter, the most popular social network among “media-jihadists”, this improvement is clear: in 2012, Twitter’s general manager Tony Wang described the platform as “the free speech wing of the free speech party”[15]; five years later, in 2017, Sinead McSweeney, leader of Twitter's Public Policy team in Europe, stated that it was “no longer possible to stand up for all speech”.[16] Thus, if initially, Twitter fostered a non-intervention approach, then it started to assume a more proactive behaviour, in particular against IS-related accounts and contents.

According to Brooking and Singer, this shift in Twitter’s approach is linked to a pivotal event, the 2013 Al-Shabaab terrorist attack in Nairobi. In that occasion, 67 people were killed by four gunmen who had previously advertised the attack through the hashtag #Westgate, the targeted shopping mall in Nairobi. Right after the terrorist attack, Twitter started to delate IS-related accounts and in 2017 it announced that its internal system was able to detect 95% of terrorist accounts and eliminate most of them “before they made the first tweet”.[17] As Twitter abandoned its

[14] Peter W. Singer, “LIKEWAR”, 237.
[15] See note above, 228.
[16] Shona Ghosh, “Twitter was once a bastion of free speech but now says it’s no longer possible to stand up for all speech.” [online] Business Insider (2017), https://www.businessinsider.com/twitter-no-longer-possible-to-stand-up-for-all-speech-2017-12?IR=T.
[17] Peter W. Singer, “LIKEWAR”, 235-236.

laissez-faire approach, the IS presence on the platform progressively became less pervasive and disturbing.

In April 2017 the United Nations Counter Terrorism Executive Directorate launched the initiative Tech Against Terrorism, which aims at three main purposes: promote the collaboration between Tech Giants and governments; collect and share knowledge and tools to ensure a safe Internet environment and stop the terrorist exploitation of social media; and support tech companies in implementing their responsiveness to the threats of cyber terrorism.[18] Furthermore, on June 26, 2017, Facebook, Microsoft, Twitter, and YouTube created the Global Internet Forum to Counter Terrorism (GIFCT), joined by Dropbox, Amazon, LinkedIn and WhatsApp in 2019. Fostering the cooperation "with smaller tech companies, civil society groups and academics, governments and supra-national bodies such as the EU and the UN ", the GIFCT's main objective is to prevent malicious actors from exploiting the Internet and social media. The most important GIFCT tech innovations aimed at pursuing this objective are the Hash Sharing Consortium and the Content Incident Protocol (CIP). The former is a database containing more than 200.000 "hashes" - digital fingerprints – that can facilitate the tracking and the elimination of terrorist-related accounts and contents. The latter is a mechanism designed to stop the circulation of terrorism or extremism-related contents from real-world violent events.[19]

Furthermore, it is important to notice that social media such as Facebook, Twitter, and Google are relatively young tech companies (respectively 18, 16, 24 years old) that in a few years have drastically revolutionised every domain of human life: from sociality to war. Thus, they are just trying to find the most effective ways to address these new challenges. Obviously, when it comes to tackling these issues, strong conflicts of interest could undermine the peaceful collaboration of Tech Giants and governments; however, they have shown their will to assume a proactive role against the exploitation of social platforms by malicious actors.

[18] *About Tech Against Terrorism - Tech Against Terrorism*, [online] Available at: https://www.techagainstterrorism.org/about/

[19] www.gifct.org. (n.d.). GifCT. [online] Available at: https://www.gifct.org/

Conclusion

In the initial stages of “Media Jihad”, Tech Giants failed in setting up an adequate response to protect the Internet from malicious actors, and this had catastrophic consequences also in the real world. As a matter of fact, their commitment to the principle of freedom of speech and their laxness allowed cyber-jihadists to create a highly structured network and to coordinate terrorist attacks and recruitments. However, the new tendency is clearly positive and proactive. Indeed, states and Tech Giants are trying to cooperate in order to create a common set of rules against the exploitation of social media as tools of information warfare. The fruits of this cooperation have resulted in a great step forward in tackling the issue of cyberwars and cyberterrorism and, thanks to the tech innovations made by organizations such as GIFCT and Tech against terrorism, the presence of IS online has been less and less pervasive. Nonetheless, Twitter is still dealing with the problem of trend-hijacking, and Elon Musk’s acquisition of Twitter on 27 October 2022, cast doubt about the Company’s future efforts in countering malicious actors from its own weaponization. Indeed, Musk announced not only that “new Twitter policy is freedom of speech”[20], but also that he is willing to restore previously banned controversial accounts.[21] The online Jihadist community has apparently welcomed this turn as an opportunity to make their comeback on Twitter, as the number of IS-related account has experienced an increase of 69% in the eleven days following Musk's acquisition.[22]

The phenomenon of “media weaponization” is effectively present and persistent and, while it should be recognised that Tech Giants have been able to join forces and cooperate with governments, it is of utmost importance to keep an eye on future Tech Giants’ policies to actively counter this pernicious phenomenon.

[20] See link: https://twitter.com/elonmusk/status/1593673339826212864

[21] Clare Duffy and Catherine Thorbecke, “Elon Musk Says He Will Begin Restoring Previously Banned Twitter Accounts next Week | CNN Business,” CNN, November 24, 2022, https://edition.cnn.com/2022/11/24/tech/elon-musk-amnesty-poll/index.html.

[22] See link: https://twitter.com/MoustafaAyad/status/1589296369231335426

Bibliography

Duffy, Clare, and Catherine Thorbecke. "Elon Musk Says He Will Begin Restoring Previously Banned Twitter Accounts next Week | CNN Business." CNN, November 24, 2022. https://edition.cnn.com/2022/11/24/tech/elon-musk-amnesty-poll/index.html.

Fridman, Ofer. "Hybrid Warfare or Gibridnaya Voyna?" *The RUSI Journal* 162, no. 1 (January 2, 2017): 42–49. https://doi.org/10.1080/03071847.2016.1253370.

Ghosh, Shona. "Twitter Was Once a Bastion of Free Speech but Now Says It's 'No Longer Possible to Stand up for All Speech.'" Business Insider, 2017. https://www.businessinsider.com/twitter-no-longer-possible-to-stand-up-for-all-speech-2017-12?IR=T.

Kaldor, Mary. "In Defence of New Wars." *Stability: International Journal of Security and Development* 2, no. 1 (March 7, 2013): 1–16. https://doi.org/10.5334/sta.at.

———. *New and Old Wars : Organized Violence in a Global Era*. 3rd ed. 1999. Reprint, Cambridge: Polity, 2012.

Prier, Jarred. "Commanding the Trend: Social Media as Information Warfare." *Strategic Studies Quarterly* 11, no. 4 (2017): 50–85.

Rugge, Fabio. "'Mind Hacking': Information Warfare in the Cyber Age." ISPI, January 11, 2018. https://www.ispionline.it/it/pubblicazione/mind-hacking-information-warfare-cyber-age-19414.

Singer, P W. *LIKEWAR : The Weaponization of Social Media.* S.L.: Mariner Books, 2019.

The Economist. "Tech Giants Are under Fire for Facilitating Terrorism", June 8, 2017. https://www.economist.com/international/2017/06/08/tech-giants-are-under-fire-for-facilitating-terrorism.

Winter, Charlie. "Media Jihad: The Islamic State's Doctrine for Information Warfare." King's College London: ICSR, 2017. https://icsr.info/wp-content/uploads/2017/02/ICSR-Report-Media-Jihad-The-Islamic-State%E2%80%99s-Doctrine-for-Information-Warfare.pdf.