global-e

Hijacking Heads & Hashtags

Series | ISIS Media
August 24, 2017 | Volume 10 | Issue 56
Katerina Girginova

"In the name of Allah, the Most Gracious, the Most Merciful, the CyberCaliphate under the auspices of ISIS continues in its

> ***CyberJihad. While the US and its satellites kill our brothers in Syria, Iraq and Afghanistan we broke into your networks and personal devices and know everything about you.*"**
> - Threat from the ISIS group via hijacked CENTCOM (US military Central Command) Twitter account. Issued in 2015 as President Obama spoke to the FCC about stepping up cybersecurity efforts.

In the past few decades we have become increasingly familiar with the concept of cyberwarfare. More recently, however, we have also witnessed the rise of a new type of mediation, which could be understood as the mediated personalization of conflict. Popularized in the past few years, and largely in connection to the strategic digital efforts surrounding the group ISIS, this is a form of social media communication that bypasses traditional media and official bodies to target, instead, individual users at high speed and en masse.

Hashtag hijacking, the focus of this essay, is one such tactic from ISIS' strategic communication; it produces a spectacular clashing of texts, worlds, and audiences, and results in a disorientation and virtual encroachment of space. In turn, it gives unprecedented proximity to the phones, hands, eyes, and ears of ordinary people around the world who would not necessarily have had direct and immediate exposure to messages from such groups before. While some work does exist examining the weaponization of social media (Nissen, 2015), a more thorough reading of specific tactics would expand our understanding not only of the ISIS war machine (Kraidy, 2017) but also of the role of new media technologies and practices in today's global conflicts. This essay first explores the idea of hijacking and then delves into examples of its practice.

The idea of hijacking

Hijacking is not a new practice. Etymologically, the word *hijack* itself evokes a complex tale of global appropriation, embroiled in misunderstandings and mistranslation. By some accounts, hijack is a combination of the words "hi – jack" and is thought to have emerged as a euphemism during the American prohibition era as either a code word for prohibited alcohol use or, for US highway jackrolling, a compound word, for stealing cars (Clark, Y. in The Guardian, n.d.). By other accounts, the word emerged during the French revolution as a description of the

frequent practice of robbing the rich “échaquer”, and was misunderstood and mispronounced by the English to morph into ‘hijack’ (Cryer, 2012). Échaquer as a word itself disappeared from use around this time and is said to have been replaced by the word détourner (Bowen, P. in *The Guardian*, n.d.), a term for ‘diversion’, later appropriated by the Situationists. Finally, “haiduk” is a popular Eastern European word for an outlaw, a freedom fighter in the Balkans or somewhat of a thief, which has since immigrated into the English vocabulary as ‘hijack’ (Burke, M. in The Guardian, n.d.).

In short, ‘hijack’ has a number of suggested origins but quite fittingly, no known root. Nonetheless the curious point about translating the word hijack into the digital space today is that a hashtag or a textual meaning is not a tangible good that may be hijacked like a car. What gets hijacked by the ISIS group in these cases is not simply a hashtag but rather, public *attention*, a *communicative space,* and a *particular meaning* and *social convention*. Hashtag hijacking thus becomes a convenient portmanteau that is really about subverting attention and implicit communicative rules and spaces, as established by specific social groups.

While some work does exist examining the weaponization of social media, a more thorough reading of specific tactics would expand our understanding not only of the ISIS war machine but also of the role of new media technologies and practices in today’s global conflicts.

Broadly speaking, textual hijacking can be understood as a tactic played out by a less powerful actor in order to use, manipulate, and divert the space and resources created by a more powerful one (de Certeau, 1984). In our context, the less powerful actor is ISIS, using social media as a mass channel and a way of circumventing traditional Western media and military organizations. Hijackers seize opportune moments and spaces to push messages and agendas to maximum effect. In essence, hijacking is a form of counterpower and can be situated amongst an older and wider array of practices of détournement and culture jamming (Debord, 1967; Dery, 1993).

The practice of hijacking

Beginning in 2014, ISIS started targeting social media platforms and users by hijacking a variety of hashtags. Of course, this practice is only one among a much

broader spectrum of the ISIS media spectacle, part of which is created and sustained by Twitter and the Western media themselves. As Twitter came under increasing pressure to react to the content on its platform, it systematically began to shut down ISIS Twitter accounts in late 2016 and there was a rapid decline in hashtag hijacking in the ensuing months. Nonetheless, the practice of hashtag hijacking remains—it just seems to have moved on to other platforms such as Telegram. Furthermore, the practice of digitally hijacking texts continues to be an insightful act of détournement, which is telling for the mediation of war today.

Textual hijacking takes place through a diversion of social media platforms, topics, users and conventions. In some cases it is done by association, whereas in others it takes place through digital embodiment or through mass force. The latter is typically part of an algorithmic effort which employs the help of fake accounts and bots (more on this is mentioned later). Below are some examples of each of the main hijacking tactics on Twitter: event crashing and persona poaching.

Event crashing

Event crashing exploits an existing, popular event hashtag, such as ISIS' use of #WorldCup (See Image 1). The operational logic is that using popular event hashtags opens up new opportunities and audiences for ISIS' messaging. In these cases, ISIS seizes upon diverse and popular social networks and gains attention through the shock and clash value of message juxtaposition.

Image 1. This image has been edited to hide a decapitated head that accompanied by the text “This is our ball… it is made of skin.” The account and post have since been deleted.

It is worth noting that the scale on which event crashing takes place varies. While #WorldCup is a rather global topic, much more localized hashtags have also been used to target, for instance, smaller communities around relatively unknown soccer teams.

The selection of targeted hashtags itself became a spectacular event when the method was crowdsourced among ISIS supporters online and circulated by the mass media. A man under the name Abdulrahman al-Hamid asked his 4,000 plus followers on Twitter to help him find the highest trending topics in the UK; “We need those who can supply us with the most active hashtags in the UK. And also the accounts of the most famous celebrities. I believe that the hashtag of Scotland’s separation from Britain should be the first.” (translated from Arabic from the now suspended handle @Abu_Laila – in Malik, Laville, Cresci & Gani, 2014).

Persona poaching

ISIS has not only created new accounts but they have also literally embodied old ones, by hacking and hijacking passwords and thus, digitally seeping into the persona of another’s body. In turn, persona poaching includes diverting accounts or hashtags of people and organizations in the public spotlight such as #JustinBieber, Keith Richard (Rolling Stones), Tame Impala (Australian psychedelic band), and the US Central Command’s (USCC) Twitter accounts. (The latter three include hijacking accounts, whereas the former, Justin Bieber, includes only hashtag re-appropriation.)

Image 2. #JustinBieber, and Image 3. Keith Richards -- account hacks

The Tame Impala and Keith Richards digital efforts had some real impact as a number of airplanes had to be diverted because of ISIS-related Twitter threats.

In an interesting twist on persona poaching, a number of highly publicized counter-ISIS hashtags have emerged, like the ones below (See Images 4 and 5). Of course, as the saying goes, on the Internet nobody knows if you're a dog, so issues of (re)presentation, authenticity, and validity haunt all digital practice and research (Kraidy, 2012), particularly when accounts and users are suspended, anonymized and frequently resurrected. ISIS' online presence is largely a spectacle precisely for that reason—it is a reflection and a refraction of reality without necessarily being attached to a direct referent.

Images 4 and 5.

Images 4 employs a professionally framed screenshot, hashtag, and a play on words—but this account, like many others, has since been suspended. Image 5 is an example of a reversal to persona poaching practices, whereby somebody has posted under the counter hashtag #AMessagefromUStoISIS. The person posting under the Lord Stirling account is anonymous and so further adds to the fog around the ISIS media spectacle.

the practice of digitally hijacking texts continues to be an insightful act of détournement, which is telling for the mediation of war today.

It is worth noting that algorithmic buttressing in the form of fake accounts and bots is rife in the ISIS effort for maximum visibility. In fact, according to the 2015 ISIS Twitter Census (Berger & Morgan, 2015), around 20% of all ISIS Tweets come from bots or apps. These bots and apps help to rapidly disseminate ISIS Tweets and generate traffic, retweets, and higher algorithmic visibility on the Twitter platform itself. This implies that much of ISIS' social media presence is algorithmically bolstered and thus, hashtag hijacking, event crashing, and persona poaching may also be understood as a product of technology and automation as much as of individual actors or organizations.

Summary

Hijacking serves to appropriate, re-appropriate and perhaps, mis-appropriate existing new media texts, communities and conventions. It causes a spectacular, mediated clashing of worlds, ideas and audiences; one that takes place at speed, en masse, and through increasingly personalized means. While the valence and media interest in ISIS' hashtag hijacking has died down since 2016, studying this tactic provides an example of one communicative turn in modern warfare—a mediated spectacle that has the potential to storm into personal screens, communities, and spaces, thereby exercising a spectacular psychological power that often outshines reality. Still, studying these tactics opens some difficult ontological questions about conducting research online: how do we verify actors and acts, and to what extent can we reconcile this 'reality' with the digital, unverified, and mediated mirage that a majority of people experience?

References

Berger, J. M., & Morgan, J. (2015, March 20). “The ISIS Twitter Census: Defining and describing the population of ISIS supporters on Twitter,” *The Brookings Project on U.S. Relations with the Islamic World.* Retrieved from http://www.brookings.edu/~/media/research/files/papers/2015/03/isis-twitter-census-berger-morgan/isis_twitter_census_berger_morgan.pdf

Bowen, P. (n.d.). *The Guardian*. Retrieved from http://www.theguardian.com/notesandqueries/query/0,,-1420,00.html

Burke, M. (n.d.). *The Guardian*. Retrieved from http://www.theguardian.com/notesandqueries/query/0,,-1420,00.html

de Certeau, M. (1984). *The Practice of Everyday Life* (S. Rendall, Trans.). Berkeley and Los Angeles, CA: University of California Press.

Cryer, M. (2012). *Curious English Words and Phrases: The Truth Behind the Expressions We Use*. New Zealand, NZ: Exisle Publishing.

Debord, G. (1967). *The society of the spectacle*. New York, NY: Zone Books.

Dery, M. (1993). *Culture jamming: Hacking, slashing, and sniping in the empire of signs* (Vol. 25). Westfield, NJ: Open Media.

Klatt, W. (n.d.). *The Guardian*. Retrieved from http://www.theguardian.com/notesandqueries/query/0,,-1420,00.html

Kraidy, M. M. (2012, July). *Plato's Digital Cave: The Arab Spring as a Representational Challenge*. Paper presentation at Crossroads Conference, Paris, France.

Kraidy, M. M. (2017). Terror, Territoriality, Temporality: Hypermedia Events in the Age of Islamic State. *Television & New Media*, 1527476417697197.

Malik, S., Laville, S., Cresci, E., & Gani, A. (2014, September 24). ISIS in duel with Twitter and YouTube to spread extremist propaganda. *The Guardian.* Retrieved from https://www.theguardian.com/world/2014/sep/24/isis-twitter-youtube-message-social-media-jihadi

Nissen, T. E. (2015). The weaponization of social media. *Royal Danish Defense College*. Retrieved from http://www.stratcomcoe.org/thomas-nissen-weaponization-social-media

Tags

social media

terrorism

cyberwarfare

Katerina Girginova is a doctoral candidate in the Annenberg School of Communication, University of Pennsylvania.

View PDF