**INSTITUT FRANÇAIS D'ETUDES SUR L'ASIE CENTRALE**

**ФРАНЦУЗСКИЙ ИНСТИТУТ ИССЛЕДОВАНИЙ ЦЕНТРАЛЬНОЙ АЗИИ**

**IFEAC**

**USR 3140 CNRS**

# Internet security facing Jihadist propaganda in Europe: the last challenge for society?

Noemi M. Rocca

Published by IFEAC in Cahiers des IFRE, December 2017/4, pp. 75-81.

Jihadist menace is perceived by public opinions as one of the main threats states are facing with[1]. In order to deal with such a threat as well as with the increasing public concern about it, governments have developed various Countering Violent Extremism (CVE) campaigns which include, among others, measures targeting the use of cyberspace by violent radical Islamist insurgents'[2]. Because of its features - i.e., among others: easy access; little or no regulation; little or no censorship; potentially huge audiences; anonymity; fast flow of information; interactivity; cheapness[3] - cyberspace is used by Jihadists for disseminating contents and for operational purposes. There is a growing consensus in literature about the importance of the Internet for logistic operations of Jihadists[4]. The Internet's functionalities (command, coordination,

[1] See for example the Center for Strategic International Studies' survey: "*Views from around the Globe: Countering Violent Extremism*", October 18, 2016, (available at https://csis-prod.s3.amazonaws.com/s3fs-public/publication/161018_CVE_Full_Report_CSIS.pdf) and the Special Eurobarometer of the European Parliament "*Europeans in 2016. Perceptions and expectations, fight against terrorism and radicalization"*, June 2016 (available at http://www.europarl.europa.eu/atyourservice/en/20160623PVL00111/Europeans-in-2016-Perceptions-and-expectations-fight-against-terrorism-and-radicalisation ).

[2] In this paper, from now on it will be used the term "Jihadists" for violent radical Islamist insurgents.

[3] Gabriel Weimann, *Terror on the Internet: The new arena, the new challenges*. US Institute of Peace Press, 2006, p.30.

[4] See, among many others, Gabriel Weimann, quot. 2006, and, of the same author, *Terrorism in cyberspace: The next generation*. Columbia University Press, 2015; Ines Von Behr et al., *Radicalisation in the digital era. The use of the internet in 15 cases of terrorism and extremism*, Rand Europe, 2013; Garth Davies et al. "Terrorist and extremist organisations' use of the Internet for recruitment" in Martin Bouchard and Philippa Levey (ed. by), " *Radical and Connected. Social Networks, Terrorism and Counter-terrorism.* Routledge (2015).

communication and information sharing[5]) in particular have crucially supported the organizational needs of transnational Jihadism. Text and video contents available on Jihadist sites are acknowledged of very sophisticated quality from technical and communication-effectiveness points of view and the Jihadist presence on social medias is considered more dynamic than the usual average of other sites[6]. The Internet – and in particular the Web – has been turned into a propaganda-machine for the Jihadist cause.

However, the importance of the Internet in radicalizing single individuals and groups is far from being unanimously acknowledged[7]. In fact, the literature does agree in considering the Internet to play a role in the radicalization process of single individuals, but *what* exactly is its role and *how* it influences such a process has not yet been fully demonstrated[8]. What appears as a pivotal point in the radicalization process are the social interactions, both on-line and off-line. Sageman, drawing from his large-scale empirical researches, concludes that "social bonds play a more important role in the emergence of the global Salafi Jihad than ideology"[9]. Bouchard and Nash point at social networks – online as well as offline – as the main factor acting in the radicalization trajectory[10]. Von Behr et al. after testing – among others - the hypothesis according to which "the Internet allows radicalization to occur without physical contact" found that "the evidence doesn't support the claim that the Internet is replacing the need for individuals to meet in person during their radicalization process. Instead, the evidence suggests that the internet is not a substitute for in-person meetings but, rather, complements in-person communication"[11]. Neumann and Stevens stress the real-world context in which both off-line and on-line social interactions take place and underline how real-world and virtual-world experiences are entangled in individuals' multifaceted pathways toward radicalization[12]. Moreover, the high number of prisons-context radicalization cases and the acknowledged importance of the so-called "hotbeds" in Europe and in the United

---

[5] Michele Zanini and Sean J. A. Edwards, "The Networking of terror in the information age" in Arquilla, J. and D. Ronfeldt (2001), *Networks and Netwars: The Future of Terror, Crime, and Militancy* (RAND Corporation: Santa Monica, CA).

[6] Berger and Morgan in "The ISIS Twitter Census: Defining and describing the population of ISIS supporters on Twitter." *The Brookings Project on US Relations with the Islamic World* 3.20 (2015).

[7] According to Ducol, "[f]irst and foremost, empirical evidence that the Internet plays a role in facilitating radicalization and further commitment to clandestine political violence is far from being conclusive. Current understanding appears to be deeply limited by weak research methods [...]." Moreover, "[t]oo often authors uncritically assume a functionalist bias in presuming a strong causality between the exposure to extremist cybercontents and the effects that this content can produces on people who are consuming it." (p.88-89). Benjamin Ducol, "A radical sociability: in defense of an online/offline multidimensional approach to radicalization" in Martin Bouchard and Philippa Levey (ed. by), (2015) quot.

[8] For example, Bouchard and Nash note that "[w]hile the role of the internet should not be over-played as a *cause* of terrorism, its role as *facilitator* at key point in the trajectory of terrorists cannot be denied either" ("Researching Terrorism and Counter-Terrorism through a Network Lens." *TSAS 2014Working paper*, p.12). A similar conclusion is that of the 2014 *UK Home Affairs Committee Report* :"Extremist material on the internet will continue to motivate some people to engage in terrorism but will rarely be a substitute for the social process of radicalization" (p.8-9).

[9] Marc Sageman, 2004, quot. p.178.

[10] Bouchard and Nash (2015) quot.

[11] Von Behr et al.(2013) quot. (p. xii)

[12] Stevens and Neuman (2009), quot., p.12-13.

States[13], appear as additional proofs of both the "real world" context of the radicalization process and the importance of social interactions.

Given the proved importance of the Internet as a medium for Jihadists' external and internal communication (the former aimed to recruit new supporters through propaganda and the latter aimed to command, coordination and info sharing), political authorities in many Western countries are developing CVE measures which target Jihadists' use of the Internet. From a war studies' point of view, cyberspace appears as becoming a domain of confrontation between state actors and transnational non-state actors (the so-called Islamic State). Such a confrontation can be defined as a "*guerre cognitive*"[14] because its final objective is persuading and mobilizing public opinions for action by using the non-kinetic tools traditionally employed in wars for influence (i.e. propaganda, psychological operations and perceptions management) supported by innovative Information and Communication Technologies' tools (social media platforms in particular).

## I. Description of online CVE measures

Online measures for countering violent extremism can be divided into "negative" or "reactive" and "positive" or "proactive" ones[15]. The first group is aimed to unilaterally destroy web sites and online contents (destructive measures) or to compel hosting companies of such contents – typically but not only social media platforms - to remove them (digital disruption strategies). The second group is aimed to reduce the appeal of on-line Jihadist propaganda by diffusing – on all the medias, but especially on the Web - contents which counter Jihadist narratives. Such measures can be implemented by governmental agencies and also by engaging and empowering users' communities. Many authors consider negative measures as less effective than positive ones because of :

- the extremely high number of Jihadists' sites which make their control and, eventually, their removal a difficult task to achieve;

- the very high birth-rate of new sites replacing (destroyed) old ones;

- the growing "user-created" portion of the web which allows a continuous flux of contents' production;

---

[13] See for example the CEP's report "Extremist Hubs" available at https://www.counterextremism.com/extremist-hubs?utm_source=Nationbuilder&utm_medium=email&utm_campaign=Extremist%20Hubs&utm_term=.944136a7edda.

[14] The concept of "*guerre cognitive*" as well as that of "*intelligence économique*" have been developed by the French school of strategic studies. See, for example, Loup Francart (2000), *La guerre du sense*, Paris: Economica; Christian Harbulot (ed.) "*Manuel d'intelligence économique*", Presses Universitaires de France, 2015 (2nd Edition); Christian Harbulot, Nicolas Moinet and Didier Lucas (2002), *La guerre cognitive: à la recherche de la suprematie strategique*; Christian Harbulot and Didier Lucas (2002), *La guerre cognitive: L'arme de la conossaince*; François Géré (2011) *Dictionaire de la disinformation*, Paris: Armand Collin. Social connectedness, the attribution of meaning to events and information as well as the management of perceptions about events themselves are the main *foci* of the French thought.

[15] Neuman and Stevens (2009), quot.; Davies et al. (2016), quot.

- the Dark Web existence and the move of the terrorists to it[16];

- the fluid technological context in which alternative ways of communication can be easily and quickly developed and used by Jihadists[17].

Despite such difficulties, some authors proved the importance of reactive strategies in fighting online Jihadists[18]. In any case, the literature is unanimous in pointing out the need of complex, multi-faceted CVE strategies which involve both negative and positive measures.

### II.a) "Negative"/"reactive" measures: "digital destruction" and "digital disruption"

Negative measures for "digital destruction" consist basically of three types of technical options: removing, filtering and hiding[19]. They rely on online network extractors for discovering sites and collecting information about extremist activities on the web which can be temporarily or definitely destroyed by sending them "trojans" and "malawares" or through repeated "denial of service" operations. A promising tool is the "hashing" technology "capable of detecting and efficiently and permanently removing extremist images, videos and audio messages that have been determined to violate the terms of services of Internet and social media companies"[20]. Such technologies have been successfully used in the past to eradicate child pornography on the net.

At the EU level, the prevention of radicalization is considered as falling under the Member States' sovereign authority. Therefore, the EU's role is limited to that of "guidance" in inspiring the national states to develop national policies and instruments. One of the EU's initiative has been the "Clean IT" project, which was "aimed to initiate public-private partnership in order to develop a non-legislative framework to counter the unlawful use of internet by terrorists"[21]. However, it was only partially developed because of contestations about its supposed anti-freedom of speech and opinions nature. Another one has been the creation of the Commission's Radicalization Awareness Network (RAN)[22] for sharing knowledge and experience. One of its working group is expressly devoted to the delivery of both on- and offline communication that offers alternatives or that counters extremist propaganda and challenges extremist ideas. Yet, so far, the EU's action

[16] The part of the web which can't be researched by the usual engines and which account for the majority of the whole cyberspace. It hosts all kind of illicit cyber activities. See *Invisible Web or Deep Web: What It Is, How to Find It, and Its Inherent Ambiguity.* 2008. Regents of the University of California. 9 Jan. 2009. On the move of Jihadists to Dark Web and its consequences, see Gabriel Weimann, (2016), "Terrorist Migration to the Dark Web", *Perspectives on Terrorism*, Vol.10, No.3.

[17] See for example the move of Jihadists communications from some messaging apps to others.

[18] Berger and Morgan (2015), quot.; J. M. Berger, "Making CVE Work. A Focused Approach Based on Process Disruption", *ICCT Research Paper*, May 2016

[19] See Neuman and Stevens (2009), p.15-19.

[20] See Joseph Rago, "How Algorithms can help Beat Islamic State" in *The Wall Street Journal*, 16 March 2017. Available at https://www.wsj.com/articles/how-algorithms-can-help-beat-islamic-state-1489187064.

[21] Argomaniz, Javier. "European Union responses to terrorist use of the Internet" in *Cooperation and Conflict* 50.2 (2015): 250-268, p.259.

[22] Official site: https://ec.europa.eu/home-affairs/what-we-do/networks/radicalisation_awareness_network_en.

has been limited and mainly it was focusing on problem-mapping, research funding, information sharing and the delivery of best practices[23].

Many disruptive campaigns against Jihadist propaganda have been carried out by non-governmental organizations and no-profit advocacy groups[24]. Social media companies are taking some measures on their own (or because pressured to do it by public advocacy campaign) for limiting and, in some cases, removing contents considered as inciting violence[25]. In Europe some national governments - the British, the German and the French ones in particular[26]- are trying to hold private industry (in particular Google, Microsoft, Facebook and Twitter) accountable for sites hosting extremist contents and force them to remove such contents. However, so far, private industry's collaboration has been considered by political authorities as limited and not effective[27]. As a response to this "inertia", the German government has recently presented a draft bill which targets fake news, hate speech and posts considered as inciting terrorism or spreading child pornography. The envisioned measures would compel social media companies to remove in 24 hours fake news as well as other contents considered as "criminal" or facing fines as high as 50 million euros[28]. Such packet of measures is seen as pivotal from both the legal and political point of view and, if approved, can become of reference for other European states. Interestingly enough, in some Western countries they are military units in charge of countering Jihadist on-

[23] Argomaniz, Javier, quot., p.257. A 2017 study by the PWC and the International Centre for Counter-Terrorism – The Hague ("*The EU's policies on Counter-Terrorism*", available at http://www.europarl.europa.eu/RegData/etudes/STUD/2017/583124/IPOL_STU(2017)583124_EN.pdf) is quite critical regarding the RAN CoE's effectiveness (see p. 64).

[24] See for example the "Counter Extremism Project". Official site: https://www.counterextremism.com/digital-disruption#dd-social.

[25] Nick Gutteridge "Google's secret war on ISIS: . Search giant in covert bid to wipe out poisonous Jihadis" in Express, 9 September 2016. Available at http://www.express.co.uk/news/world/708732/Google-ISIS-fightback-search-engine-blitz-Islamic-State-jihadi-propaganda.

[26] Jessica Guynn "UK official: Get terrorist content off Facebook, Youtube and Twitter" in USA TODAY, March 30 2017, availble at https://www.usatoday.com/story/tech/news/2017/03/30/amber-rudd-terrorism-meeting-facebook-google-twitter/99831462/. Already in 20015 the French government was the first one to adopt a "pulling out" strategy. See Amar Toor "France can now block suspected terrorism websites without a court order", in *The Verge*, February 9, 2015 http://www.theverge.com/2015/2/9/8003907/france-terrorist-child-pornography-website-law-censorship.

[27] See, for example, in the UK: Tim Shipman, Simon Duke and Duncan Geddes, "Boris savages "disgusting" Google", in *The Times*, 26 March 2017. Available at https://www.thetimes.co.uk/article/boris-savages-disgusting-google-7kc5tbzb6..

[28] See Antony Faiola and Stephanie Kirchner, "How do you stop fake news? In Germany, with a law" in *The Washington Post*, 5 April 2017. Available at https://www.washingtonpost.com/world/europe/how-do-you-stop-fake-news-in-germany-with-a-law/2017/04/05/e6834ad6-1a08-11e7-bcc2-7d1a0973e7b2_story.html?utm_term=.76c47e6deca2.

line operations: the "Cyber Command" in the United States[29], the 77 Brigade in the UK[30], the 28th Regiment "*Pavia*" in Italy[31] and the inter-armies "*Commandement Cyber*"[32] in France.

### II.b) "Positive"/"proactive" measures: countering Jihadist propaganda

Positive measures basically consist of opposing Jihadists' propaganda on existing social platforms or devoted web-sites. At the EU level, the abovementioned EC's RAN would be "launching the EU Civil Society Empowerment Programme (ESCN) to help civil society grassroots groups and credible voices to fill the Internet with alternative narratives"[33]. In such campaigns particular attention is devoted to the development and dissemination of counter-narratives. Developing counter-narratives involves "re-narrating the events of the opposition's narrative, coopting their meaning. In other words, one tells one's narrative in a way that re-frames the opposition's and offers a bigger, better, smarter alternative of understanding, identifying and acting"[34]. The web represents the principal medium for counter-narratives' diffusion, although effective CVE campaigns require all-media strategies. Scholars unanimously state the importance of context-related and theoretically funded counter-narratives' role in fighting Jihadist propaganda. Ajit Maan – drawing on Paul Ricoeur's studies devoted to narratives' role in identity construction - argues that narratives and not assertions mobilize action[35]. Moreover, in order to be an effective counter-terrorism tool, they must relate to the every-day experience of the recipients and belong to a wider, multifaceted CVE strategy in which "soft" non-kinetic tools work together with "hard" kinetic ones for eradicating not only the enemy persuasive power but also the structural causes

---

[29] See Ellen Nakashima and Missy Ryan "U.S. military has launched a new digital war against the Islamic State", in *The Washington Post*, 15 July 2016. Available at https://www.washingtonpost.com/world/national-security/us-militarys-digital-war-against-the-islamic-state-is-off-to-a-slow-start/2016/07/15/76a3fe82-3da3-11e6-a66f-aa6c1883b6b1_story.html?tid=a_inl&utm_term=.8f83117b253d.

[30] See Ewen MacAskill, "British Army creates team of Facebook warriors", in *The Guardian*, 31 January 2015. Available at https://www.theguardian.com/uk-news/2015/jan/31/british-army-facebook-warriors-77th-brigade. See also

[31] See Alberto Scarpitta, "Il 28° Reggimento Pavia e l'evoluzione delle info-ops" ("The 28th Regiment and the evolution of info-ops.". In *Analisi Difesa*, 1 September 2015. Available at http://www.analisidifesa.it/2015/09/il-28-reggimento-pavia-e-levoluzione-delle-info-ops/.

[32] See Nathalie Guibert "L'armée française lance un exercice de cyberdéfense à grande echelle". In *Le Monde*, 16 March 2017. Available at http://www.lemonde.fr/international/article/2017/03/16/l-armee-francaise-lance-un-exercice-de-cyberdefense-a-grande-echelle_5095415_3210.html.

[33] According to Matthias Monroy in "Social Media companies launch upload filter to combat terrorism and extremism" 17 March 2017. Available at https://digit.site36.net/2017/03/17/social-media-companies-launch-upload-filter-to-combat-terrorism-and-extremism/.

[34] Jim Sisco and Ajit Maan "The "kill/capture" approach ain't working for us: Narratives do better than drones" in *Foreign Policy*, 23 April 2015. Available at http://foreignpolicy.com/2015/04/23/the-killcapture-approach-aint-working-for-us-narratives-do-better-than-drones/.

[35] Maan, Ajit, "Narratives are about "meaning" not "truth"", in *Foreign Policy*, December 3, 2015. See also, *Inter-narrative identity. Placing the Self*. University Press of America, 2010; and *Counter-terrorism. Narrative Strategies*. University Press of America, 2014.

on which such power relies on[36]. However, so far, counter-narratives' implementation in online CVE campaigns has been limited and in some cases even counter-productive[37].

## III. The dichotomy between security and fundamental rights' guarantee

Proactive CVE measures' effectiveness is uneasy to evaluate not only because their results need to be assessed in the long term but also because of the difficulties in developing qualitative or quantitative frameworks for evaluating them. At the same time, although negative measures imply a numerical dimension and therefore are easier to evaluate[38], their implementation raises more concerns because of their political significance. In fact, fighting online Jihadist threat through web sites' destruction and contents' removal risks overcoming privacy right and freedom of speech and expression producing a sort of "securitization" of cyberspace[39]. Civil and human rights associations are indeed opposing online negative CVE measures and political plans to implement new ones[40]. According to Berger and Morgan[41] "tampering with social networks is a form of social engineering, and acknowledging this fact raises many new difficult questions" (p.3), as – among others - what are the "unintended consequences" of it (p.59). In Neuman's and Stevens' words: "How far can we go in protecting democracy without jeopardizing the very liberties one wishes to protect?" [42]

As a preliminary attempt to answer such a fundamental question, it can be said that the amplitude of online CVE's pressure on fundamental rights is related to *a)* the *actual* threat (i.e. the Jihadists' violent actions and their functional exploitation of cyberspace for such actions as well as for propaganda and recruitment purposes); *b)* the public opinions' *perceptions* about such a threat; *c)* the political authorities' will to deal with such issues, opposing - on one side - private industry's

---

[36] Ajit Maan, "The Heart of the Common Man: The Battleground of Asymmetric Conflict", in *Indian Strategic Studies*, 19 Aug , 2015. Available at http://strategicstudyindia.blogspot.it/2015/08/the-heart-of-common-man-battleground-of.html#more.

[37] Bibi T. van Ginkel," Responding to Cyber Jihad: Towards an Effective Counter Narrative", *ICCT Research Paper*, March 2015; Alex Schmid (2014) quot., Davis et al (2016), quot. According to the West is losing the "War of ideas" against global Jihad because of a lack of narrative coherence while our opponents are better prepared to strategically operate on cyberspace. David Betz (2008) "The virtual dimension of contemporary insurgency and counterinsurgency", *Small Wars & Insurgencies*, 19:4, 510-540.

[38] See for example the conclusion of Neumann and Stevens (2009:6). See also Scott Higham and Ellen Nakashima "Why the Islamic State leaves tech companies torn between free speech and security", in *The Washington Post*, 16 July 2015. Available at https://www.washingtonpost.com/world/national-security/islamic-states-embrace-of-social-media-puts-tech-companies-in-a-bind/2015/07/15/0e5624c4-169c-11e5-89f3-61410da94eb1_story.html?kmap=1&tid=a_inl&utm_term=.9c8ccc95af72.

[39] For the concepts of "securitization" and security threats' construction see the works of the so-called Paris School - which develops Michel Foucault's notion of "governmentality" and Pierre Bourdieu's "field" concept - and of the so-called Copenhagen School.

[40] See for example the stance taken by the European Digital Rights association, which is made up of 35 European civil and human rights associations. Official website: https://edri.org/about/. See also the campaigns promoted by the Open Rights Group. Official website: https://www.openrightsgroup.org.

[41] Berger and Morgan (2015), quot.

[42] Neumann and Stevens (2009), quot. p.6.

interests and civil rights associations' pressure, and - on the other side - citizens' concerns about security.

Encryption - a technology which has not yet been regulated because of its value in terms of privacy protection and, therefore, its unanimous defense by tech industry - is a paradigmatic case of the complex relationship between public interest, private tech companies' search for profit and the political role of governments in providing, at the same time, security and protection of fundamental rights.

The "pulling out" approach – i.e. that one based on web sites' destruction and contents' removal - can produce also the so-called "executive aggrandizement". This is a process through which, in a state under what is considered to be (or framed as) a direct and impellent threat to national security, the executive branch enlarges its power beyond the legislative branch and the limits fixed by the constitutional act[43].

## Conclusion

Combating a cognitive war against transnational Jihadists focusing on short-term reactive tactics can be not only ineffective, but also socially and politically dangerous. Civil rights associations' recent stances against current and envisioned online CVE measures make clear the risk of political de-legitimization of governments engaged in shortsighted and poorly conceived campaigns.

Jihadists' actions, governments' re-actions, civil rights associations' counter-reactions and Internet companies' stances have to be situated and planned within a wider context which takes into account economic, social, political, technological and organizational factors. Because of the complex significance of such phenomena, any normative answer to them could not simply be of a technological kind, but implies political will, attitude and choices. It needs also a reflection on the level on which such responses have to be effectively deployed - whether it be national or supranational - as well as on the potential risk of activating structural changes which affect the distribution and the balance of powers within a state. In other terms, the political essence of the problem should not be held back or missed in developing and implementing all kind of CVE measures, not least those online.

Finally, given the fact that no clear evidence has been reached so far, further methodologically reliable studies on the Internet's role in the production of the Jihadist menace (in terms of both real and perceived threat) are urgently needed. A theoretical knowledge which could be empirically funded is essential for defeating an opponent which has demonstrated to know and to use in a very effective and sophisticated manner all the techniques and the tools of a cognitive war.

---

[43] See Hilde Eliassen Restad, "*The War on Terror from Bush to Obama: On Power and Path Dependency*", Norwegian Institute for International Affairs (NUPI) Report, (2012)

*Noemi M. Rocca is PhD Candidate in International Relations. "Centre for Social Studies" and "School of Economics", University of Coimbra, Portugal.* *The author acknowledges the support of the Institute Français d'Etudes sur l'Asie Centrale (IFEAC) in the form of a travel grant which enabled her to attend the round table.*