Narratives of Risk: Assessing the Discourse of Online Extremism and Measures Proposed to Counter It*

Matti Pohjonen and Reem Ahmed

Abstract: The discourse surrounding digital technologies is rapidly changing, namely from an entity with the potential to generate positive political change to one that can be abused by extremists. In light of this, a new "dispositif" of risk has emerged whereby governments are seeking to address the imagined dangers posed by digital technology through a series of pre-emptive measures. By examining how the relationship between digital technology and violent extremism has been articulated in the EU's counter-terrorism policy, this article argues that critical distance is now needed from both these utopian and/or dystopian conceptualisations of digital technology and conflict.

Keywords: Internet, violent extremism, EU IRU, risk theory
Stichwörter: Internet, gewalttätiger Extremismus, EU IRU, Risikotheorie

1. Introduction

The discourse surrounding the internet and new media is rapidly changing. Where there once was a more enthusiastic rhetoric regarding the "promises" of digital technology as a harbinger of citizen participation, open and accountable governance and democracy globally, the debate has now increasingly shifted to its "dark" side: new media as a platform for violent online political extremism. Indeed, critical security scholars have argued that a new "dispositif" of risk has emerged whereby these imagined dangers of digital technologies need to now be contained and controlled through the development of new political, legal and technological mechanisms, such as surveillance and censorship, predictive policing, and cooperation with internet intermediaries to monitor and remove extremist content (see Amoore and de Goede 2008; Argomaniz 2015; Grusin 2010; Nouri and Whiting 2014).

Given the complex nature regarding the role digital technologies play in occurrences of violent extremism, this article argues that a different approach is needed. Instead of asking *what* role new media plays in facilitating violent radicalisation, we need to examine the context *in which* it has been imagined as something in the first place and with what consequences. To this end, the article examines how the relationship between digital technology and violent extremism has been articulated in the European Union's (EU) counter-terrorism policy and specifically around the creation of the EU Internet Referral Unit (IRU). In the first section of this article, we explore the debates surrounding digital technology and the recent shift of the discourse to its "dark" side. Following this, the analytical framework will be outlined, and in the final section we critically examine recent EU documents that detail the perceived growing threat posed by online violent radicalisation and responses to it.

2. The many "risks" of digital technology

Assumptions regarding the political significance of new digital technologies have historically tended to oscillate between a kind of techno-utopianism, in which digital technologies have been seen as instrumental in bringing about positive democratic change, and a more techno-pessimist approach, which has correlated digital technology with increased government control over the public sphere. This imposition of political value onto a diverse set of different "media-related practices" (Hobart 2010, Couldry 2014) is perhaps best exemplified by the labelling of the events during the so-called Arab Spring in 2010-2012 as "Twitter" or "Facebook" revolutions (see Johnson et al. 2013; Ghomin 2012; Oh et al. 2015). Christensen (2010) writes that this kind of enthusiasm has usually been followed by a critical inquiry regarding the extent of what the perceived benefits of the technology actually were:

> In the first camp, we find those who trumpet the virtues of new technologies such as Twitter and YouTube, linking, for example, the erosion of oppressive state power with access to and use of social media. In the latter camp, the techno-dystopians (or debunkers), we find those who consider techno-utopianism as nothing more than technological determinism (Christensen 2010: 155-156).

The ensuing "Arab Winter" has since provided a bleak reminder that these digital revolutions were perhaps not all that they seemed. There has been a violent backlash against youthful eruptions of democratic fervour at the hands of entrenched political elites in Egypt, often using the same digital technologies to suppress dissent that were used to inspire it. Moreover, a bloody civil war in Syria has had profound ramifications on the rest of the world, and perhaps most notably facilitated the rise of the so-called Islamic State (IS), a terrorist group that has become known as much for its ruthless territorial expansion on the ground as it has for its savvy use of new digital technology for recruitment and violent propaganda.

Indeed, following the Arab Spring, there appears to have been an analytical shift in focus to what some have called the "dark side" of internet freedoms – namely, to the many imagined dangers or risks now associated with new digital technologies (see Morozov 2012; see also Mosco 2005). Where previously there was greater emphasis on the positive democratic potential of new media (see Castells 2012; Gerbaudo 2012; Bruns 2016), governments have turned their attention to a wide range of alarming online

* This article has been double blind peer reviewed.

DOI: 10.5771/0175-274X-2016-4-236

activities: sophisticated social media recruitment strategies by IS and their supporters; "home-grown" terrorists finding inspiration for attacks; individuals learning to build bombs from YouTube videos or online manuals; the coordination of terrorist networks in the murky underworld of encrypted communication and the dark web; and the spread of hate speech online around the so-called "migrant crisis" (see Carter et al. 2014, Edwards and Gribbon 2013; Briggs, 2011, Neumann 2012, von Behr et al. 2013, Wojcieszak 2010).

Nowhere has this shift been more evident as in the emerging field of research on violent online political extremism. Yet, despite such growing fears of online radicalisation – and the increased pressures governments face to act – there still seems to be insufficient empirical research that has systematically examined this assumed causal or quasi-causal relationship between online and offline activity. In their overview of existing literature, for instance, Gill et al. (2015) argue that the existing research suffers from lack of conceptual clarity about how this relationship between online activity and offline behaviour (such as radicalisation) should be assessed. On the one hand, theories in circulation subsume a wide range of online behaviour such as "accessing information on overseas events via the Internet, to accessing extremist content and propaganda, to detailing attack plans in a blog post" (ibid: 5) into this general category. On the other hand, there is an absence of empirical research that would substantiate this link in a wide variety of different settings and contexts (ibid):

> Even for a field as bereft of empiricism as terrorism studies, the striking lack of data is surprising. Of the 200 abstracts analysed, only 6.5% utilised any form of data. Primary data was utilised in just 2% of the studies, but this mostly focused on extremist forums and social media and, therefore, largely captured radicalised individuals (and not necessarily individuals prepared to conduct terrorism) … Instead, the literature assumes virtual space is a good substitute for physical interactions, but fails to tell us why and in what contexts in particular (ibid: 6).

Along the same lines, Conway (2016: 5) argues that "basic descriptive research is largely missing from this field, along with more complex theory-informed approaches seeking to show causal connections". The literature on violent online extremism thus seems to suggest that online activity can, indeed, be a facilitator of radicalisation but it remains unclear what the differentiated role of "online" activity is and how its causal relationship to offline activity can be theorised (see Grey and Head, 2009; Archetti 2013; von Behr et al. 2013; Benson 2014; Pauwels and Schils 2016).

Given these epistemic uncertainties, we propose to adopt a different approach in this article. Firstly, instead of questioning how digital technology contributes to political expression – whether positively or negatively – we have chosen to approach this relationship as "overdetermined" (Laclau and Mouffe 1984). By this we suggest that currently there are more theories in circulation than factual evidence would warrant. Therefore, we argue that it makes sense to temporarily recoil from trying to understand what this relationship is (by positing, for instance, some underlying causal relationship between online behaviour and extremism offline) and rather first ask *how this relationship has been imagined in the first place*. Secondly, in order to distance ourselves from some of these impositions of political value onto digital technologies, we have instead chosen to look at it as symptomatic of a broader risk discourse around the war on terrorism. This allows us to move away, albeit temporarily, from the more theoretically difficult question of how digital technology contributes to violent political extremism and rather ask the more straightforward question of how and by whom these dangers have been imagined as something in the first place.

Risk theory has been used to comprehend how uncertainties of modern societies have been approached in academic, policy and public debates (see Beck 1992; Giddens 1999). What is interesting about debates on risk is that the "dark" sides of digital technologies also seem to be increasingly understood in terms of the risks they pose: in the vulnerable youths who could potentially be recruited by terrorist propaganda; in finding new ways to prevent violent attacks that could be facilitated or inspired by online activity; and in the dangers of racist, xenophobic and misogynist hate speech. Amoore and de Goede (2008) further argue that the discourse around terrorism in the US and Europe has allowed new practices of governance to emerge through which these imagined risks are managed, including new methods of online surveillance and monitoring of online material that could be flagged as extremist or potentially violent. They write that "the proliferation of risk techniques in the war on terror, then, is essentially about a particular mode of governing – a means of making an uncertain and unknowable future amenable to intervention and management" (Amoore and de Goede 2008: 9). Martin (2015) similarly argues that what matters in theories of radicalisation is not only gathering empirical evidence about a given situation, but it is also a way of using this research to *prevent* such dangers through policies linked to it. The majority of the academic literature on the topic has, as a consequence, tried to "model this process towards violence, such that it can be understood, predicted and acted upon" (Martin 2015: 63).

3. The many metaphors of digital technology and conflict

This shift in focus (between what this relationship is versus how it has been articulated) thus allows us to explore how these imagined dangers of digital technologies have been foregrounded in political debates. The analytical framework developed in this article reflects this shift of focus. In particular, in order to distance ourselves from what we consider to be a set of overdetermined debates about digital technology's many dangers, we draw instead on a "paradigmatic research framework" developed in conflict studies to explore different ways this relevance has been articulated as a part of political discourse. Coleman (2003, 2004, 2006) has argued that, in order to understand how any given conflict situation is understood by its participants, we need to first ascertain how its basic premises have been framed by the different theories and methods used to understand it. Coleman (2004: 197) writes that "these frames help to organise our thinking about our work, but also constrain our understanding of the full complexity of the situations that we engage".

Moreover, Coleman proposes that we should look both at what has been both *implicitly* presupposed by these approaches as well as what has been *explicitly* presupposed. By implicit frames he refers to those types of often unconscious structures that shape our understanding of the world. He writes that: "Our metaphors of conflict are packed with a set of basic, often unexamined, assumptions that further guide our perception and information processing... These images and assumptions provide the backdrop for our implicit framing of intractable conflicts, which helps to determine our sense of our own role in the conflict" (Coleman 2004: 197). These implicit frames consist of the kinds of basic assumptions regarding how we organise our understanding of what reality is, ideas of human nature, what power is, what the nature of conflict is, and who the stakeholders are. Besides these implicit frames, Coleman argues that we need to additionally look at how the theories and methods we use have been explicitly framed in our research. These explicit frames consist of theories and methods that researchers consciously adopt to make sense of conflict situations, such as key causal variables and levels of analysis (ibid: 200).

Furthermore, Coleman (2004) points to five different paradigms through which conflicts have been historically understood. These are: (1) the *realist paradigm*, which relies on a political metaphor that sees "conflicts as dangerous, high-stakes games won through strategies of domination, control, and countercontrol" (ibid: 203); (2) the *human relations paradigm*, which is based on a social metaphor "of destructive relationships where parties are locked in an increasingly hostile and vicious escalatory spiral from which there appears to be no escape" (ibid: 207); (3) the *medical paradigm*, which views humans and social systems as basically health-oriented entities where pathological illnesses or destructive tendencies can nonetheless develop (ibid: 212); (4) the *postmodern paradigm*, which sees conflict as consisting of the different way parties "interact with one another to construct a sense of meaning, responsibility, and value in that setting" (ibid: 217); and, finally, (5) the *systems theory paradigm*, which sees conflicts as "entities made up of a variety of interdependent and interactive elements nested within other, increasingly complex environments" (ibid: 222).

Each of these paradigms, Coleman continues, also creates a set of possible solutions to how the conflict could be resolved based on how its basic premises are implicitly and explicitly understood. The realist paradigm thus prefers deterrence, force and legal frameworks to mitigate the problems of conflict (Coleman 2004: 203). The human relations paradigm, on the contrary, leans towards softer methods such as increasing social interdependence and cooperation, as well as fostering reconciliation (ibid: 207). The medical paradigm sees conflicts as anomalies in a healthy system and thus, as a result, proposes to target them by identifying malignant social processes and cultural patterns that maintain these negative patterns (ibid: 212). The postmodern paradigm, in turn, looks towards finding ways to transform the collective identities and narratives behind conflicts more egalitarian and sustainable (ibid: 217). Finally, the systems theory paradigm employs a multi-layered analysis whereby the solution is found in a heuristic understanding of the complex interactions that cause destructive patterns in society (ibid: 222-223).

Our argument builds on this framework to explore how the relationship between digital technology and violent extremism has been framed in European counter-terrorism policy, and, in particular, in the EU Terrorism Situation and Trend Reports (TE-SATS) and documents chronicling the creation of the EU Internet Referral Unit (IRU), which has been created to address growing concerns regarding online radicalisation. Two issues are assessed in these documents: (1) how digital technology has been linked to violent extremism, and (2) the nature of the specific counter-measures that have been suggested to mitigate the risks of online radicalisation. We will analyse, in particular, some of the presuppositions, implicit and explicit, through which the relationship between digital technology and violent extremism in Europe is currently understood in these documents, what the stakes behind it might be, as well what potential alternative frameworks could be developed for understanding this relationship. While digital technology arguably poses a new dynamic in conflict, we argue in this paper that the way we comprehend it nonetheless still relies on pre-existing paradigms of understanding that need to be critically examined.

4. Analysis

4.1 The creation of the EU Internet Referral Unit

Over the past decade, the EU has increasingly asserted that the internet plays a significant role in the radicalisation of individuals towards acts of terrorism. This is evident in Europol's annual TE-SAT reports, as well as the EU's broader Counter-Terrorism Strategy. The 2014 TE-SAT report, for instance, states clearly that:

> Terrorists and violent extremists of all affiliations make adamant use of the Internet, in particular social media, as pivotal tools for planning, targeting, recruitment, communication, bonding, instruction, training and propaganda. Social media are believed to have contributed to the acceleration of (self-) radicalisation among EU nationals (Europol 2014: 9).

The 2015 TE-SAT report similarly states that: "The nature of terrorist communication on the Internet is constantly changing as a result of new technologies that become available. Terrorist groups have continued to adapt their approaches to communication, exploiting new methods for interaction and networking on the Internet" (Europol 2015:12). Both these documents explicitly suggest that the internet and social media have become "pivotal" for groups planning to carry out politically violent acts and that the internet provides "new opportunities" for terrorists to target audiences with their messages, accelerating the process of radicalisation as a result. Furthermore, within the EU Counter-Terrorism Strategy, which was revised in June 2014 in light of "evolving trends" such as the growing number of foreign fighters and the increasing potential of the internet for the recruitment of terrorists,[1] one of the key priorities for the prevention of terrorism is to tackle the misuse of the internet by terrorist groups (Council

1 For further information on this revision see: http://www.consilium.europa.eu/en/policies/fight-against-terrorism/

of the European Union 2005: Article 13). This is most visibly reflected in the creation of the EU IRU, which was launched on 1 July 2015. This initiative aims to pool together resources and best practices to monitor violent extremist content online, as well as to work together with the internet industry and relevant competent authorities to remove content where necessary (Council of the European Union 2015a: 3).[2] Whilst the creation of the EU IRU was formally announced in March 2015, the founding rationale for the unit is explained by the EU Counter-Terrorism Coordinator, Gilles de Kerchove, in a document dated 17 January 2015:

> Europe is facing an unprecedented, diverse and serious terrorist threat. The horrific attacks that took place in Paris between 7 and 9 January 2015 were followed by an unprecedented show of unity by millions of citizens in France and across Europe as well as a show of solidarity and political will by many EU and world leaders. In addition to action from the national governments, citizens are looking to the European Union to provide an ambitious response. Core European values have been attacked, in particular freedom of speech. The EU has to respond with meaningful action. Failure to do so could result in disillusionment of citizens with the EU (Council of the European Union 2015b: 1).

The Coordinator goes on to outline four areas in which to "amplify and accelerate" existing policy to prevent radicalisation – one of which is the internet (ibid: 2).

What is evident in the documents is a sense of urgency in adopting these proposed measures for monitoring and removing extremist content in order to prevent potential future terrorist attacks. The EU IRU concept note states that terrorist use of the internet has "increased *dramatically* over recent years. Jihadist groups have shown a *sophisticated* understanding of how social networks operate and have launched *well organised* social media campaigns to recruit followers, promote or glorify acts of terrorism and violent extremism" (Council of the European Union 2015a: 1, emphasis added). Thus, the EU recognises that terrorist groups could conceivably (mis-)use the internet with a high degree of competence and such exploitation is potentially dangerous. Faced with this construction of digital technology and its associated risks, the EU thus needs a strong multi-national police force – Europol – to control and manage these "dark" sides of internet freedom. Furthermore, the measures infer a form of continued governance over "vulnerable audiences" who are more likely to be susceptible to such material. Even though recent TE-SAT reports have acknowledged that the internet is abused by all kinds of extremist groups (see for example Europol 2013, 2014, 2015), and Europol refers to addressing the use of social media by terrorist organisations and violent extremists in general, the EU IRU appears to be primarily targeted at jihadi material as the concept note specifically cites internet usage by jihadi groups and the rising numbers of claimed supporters of IS on Twitter (Council of the European Union 2015a: 1). As the 2015 TE-SAT report outlines, propaganda material espoused by IS is targeted specifically at Muslims in Europe with the aim to construct an ...in-group/ out-group dichotomy, [where there is] "a strong emphasis on group solidarity and emotional bonds among Muslims" (Europol 2015: 21) as opposed to broader European values. Thus, within this context, the Muslim community are viewed as the most vulnerable to jihadi content online by groups that threaten Europe with violence. This further exemplifies how this initiative was triggered by events in Paris in January 2015[3] and the need to show EU citizens that something was being done about the perceived increasing threat of jihadi terrorism in Europe.

4.2 Discussion: implicit and explicit frames in the EU counter-terrorism policy?

While this only scratches the surface of the abundant discourse, we can nonetheless extrapolate from these documents some of the ways that the debates on digital technology have been framed. For instance, if we look closely at current EU counter-terrorism policy from the perspective of Coleman's (2004) model, it is clear that the dominant paradigm through which the imagined dangers of digital technology are framed is the realist one. This is reflected both in how digital technologies are imagined (through their propensity to be used for propaganda and for the planning of violent attacks by terrorist groups) and through the measures that need to be taken to prevent these imminent attacks (prioritising measures such as legislation and the policing of online behaviour). Concurrent with Coleman's realist paradigm, the EU is asserting its strength in the form of Europol and bestowing the illusion of control over a situation that is, in reality, unpredictable and ultimately complex. Ultimately then, the backdrop of the EU's narrative is to defend core European norms and values from being attacked and abused by terrorist groups who use, among other things, the internet and social media to do so. Such strong and emotive discourse effectively frames the conflict into two parties – those who respect these values and those who do not – thus establishing a strict division between those who belong to this European in-group and those who are outside it. As suggested in the concept note, "tackling this phenomenon efficiently requires the EU Member States to … ensure that [the] Internet remains a public good, free of terrorist and violent extremist propaganda while respecting fundamental principles such as the freedom of speech" (Council of the European Union 2015a: 3). This line is particularly significant as the EU is demonstrating a strong will to defend these freedoms, even if, as critics have suggested, many of the practical measures proposed to counter online violent political extremism can have questionable ramifications on the same principles of freedom of speech that EU seeks to protect, such as through advocating measures of online surveillance and censorship to contain these imagined threats.

2 The EU IRU builds on the earlier capabilities of the "Check the Web" project, a project where the "monitoring and evaluating terrorist websites" for intelligence purposes was seen as paramount to prevent new kinds of terrorist attacks from taking place (Council of the European Union 2007: 2). Thus, the EU IRU is an extension of this as it aims to respond more pro-actively by taking down terrorist content.

3 From 7-9 January 2015, 17 people were killed in attacks on the Charlie Hebdo headquarters, a kosher supermarket, and in a Paris suburb. Al-Qaeda in the Arabian Peninsula claimed the attacks.

It is also important to consider that the realist paradigm is not the only way the relationship between digital technology and conflict could be understood. As Coleman has suggested, depending on the framework we find most useful for understanding conflict, we could as well view violent extremism as the outcome of destructive social relationships between different groups in society, in which case more interdependence and reconciliation would be a more suitable remedy to counter it. Or, we could approach radicalisation as a phenomenon rooted in questions of social identity, which, in turn, would require us to diagnose the reasons for this (such as social alienation and disenfranchisement) and take measures to treat the root causes of the problem. In other words, this shift of focus would place emphasis on addressing the reasons why individuals choose to seek out extremist material on the internet in the first place, rather than approaching the problem through realist metaphors of propaganda and war and as a result through methods of control and counter-control.

We could equally argue that there is an urgent need to create new narratives in Europe that are not exclusionary, but rather consist of ways of renegotiating what it means to be European in a multicultural society and thus prevent some of the polarised identities resulting from the profiling of Muslims as a group especially vulnerable to online radicalisation. New research has begun to examine possible ways of fostering online spaces of engagement and counter-speech as conflict mediation mechanisms; however, more needs to be done to make such approaches inclusive and not just another form of counter-propaganda (see Bartlett and Krasodomski-Jones 2015; Ferguson 2016). These new ways of understanding online extremism as a symptom of an underlying conflict, and partially also the metaphors we use to frame this conflict, could thus potentially help us move beyond the realist paradigm and instead engender new innovative solutions to address the issue of online radicalisation. Indeed, if new digital technologies are increasingly framed as dangerous, and as a result governments resort to using strategies of propaganda and control to prevent these dangers from manifesting, perhaps the policies we adopt also contribute to the problems that we are trying to prevent by, for instance, alienating "vulnerable audiences" through their stigmatisation as potential enemies or as risks to be managed (see Ericson 2008).

5. Conclusion

This article has looked critically at how we frame the relationship between digital technology and violent extremism, focusing especially on the contemporary debates on violent online political extremism and European counter-terrorism strategy. Given the current lack of conceptual clarity and empirical evidence, we argued that it makes sense to temporarily step back from the existing debates and look instead at what has been presupposed by these debates and how they have been framed. Ericson writes that "terrorism is the politics of uncertainty … terrorists are in the business of uncertainty, playing on randomness to keep whole populations in fear, anticipation and disestablishment" (Ericson 2008: 58). This way, the debates could perhaps be seen as reflective of the growing concerns regarding online radicalisation that the political establishment and public share, and the increasing urgency to do something about it, as it is about some ontological "object" out there. This does not mean that the internet does not play a significant role in violent radicalisation, but the way in which this (assumed) causal relationship has been constructed is potentially problematic. Whilst the EU certainly does not view the internet in isolation when dealing with the issue of violent extremism, there is an implication within the documents studied that there has been a radical shift in the way that the internet presents new challenges to security. However, terrorist groups have existed long before the internet, and although the internet is a new medium through which terrorists communicate, the internet has not necessarily altered the reasons why individuals choose to engage in terrorism. Looking critically at the metaphors through which this relationship between digital technology and conflict has been imagined, rather than accepting it at face value, can thus help us gain distance from both the utopian and, increasingly, dystopian impositions of political value on technologies that themselves are neutral.

Matti Pohjonen (PhD) is VOX-Pol* research Fellow for 2015-16. His research focuses on different kinds of conflict mediation mechanisms through which social media communities have tried to counter hate speech and extremism online. He currently leads a research project mapping the social media activities of the far right in the EU.

Reem Ahmed (MA) is a Researcher and PhD student at the Institute for Peace Research and Security Policy at the University of Hamburg (IFSH). She works within the framework of VOX-Pol*. Her research is focused on terrorism, radicalisation, and the role of women in jihadi and right-wing movements.

Bibliography

Amoore, L. (2008). "Consulting, Culture, the Camp: On the Economies of Exception." In Risk and the War on Terror, edited by L. Amoore and M. de Goede, 112–129. London: Routledge

Amoore, L. and *M. de Goede*. (2008). Risk and the War on Terror. New York: Routledge.

Aradau, C., and *R. van Munster*. (2008). "Taming the Future: The Dispositif of Risk in the War on Terror." In Risk and the War on Terror, edited by L. Amoore and M. de Goede, 23–40. London: Routledge

Archetti , C. (2013). Understanding Terrorism in the Age of Global Media: A Communication Approach, Basingstoke: Palgrave

Argomaniz, J. (2015). European Union responses to terrorist use of the Internet. *Cooperation and Conflict*, *50*(2), 250-268.

Bartlett, J. and *A. Krasodomski-Jones*. (2015). "Counter-speech: examining content that challenges extremism online." Demos.

Beck, U. (1992). Risk Society: Towards a New Modernity. New Delhi: Sage.

Benson, D. (2014). "Why the Internet is Not Increasing Terrorism," Security Studies 23(2), 293–328

* The VOX-Pol Network of Excellence is funded by the European Union under the 7th Framework Programme for research, technological development and demonstration under Grant Agreement No. 312827. The project focuses on researching the prevalence, contours, functions, and impacts of Violent Online Political Extremism and responses to it.

Anzeige

(Seite VI)