Rethinking Online Radicalization

by Joe Whittaker

Abstract

This article seeks to re-ontologize online radicalization. Individuals becoming terrorists after being exposed to online content have become a prescient concern for academics, policy makers, and journalists. Existing theoretical contributions to the concept have assumed that there are two ontological domains—online and offline—that can be meaningfully separated. This article will draw from several arguments from other fields which critique this position; the contemporary information environment enmeshes the two inseparably. This argument is then advanced to demonstrate that online radicalization is a redundant concept by drawing on empirical research as well as recent case studies of terrorism. Instead, scholars should consider holistic theories which account for a range of other factors beyond online communication technologies.

Keywords: Terrorism; radicalization; social media; extremism

Introduction

The threat of online radicalization has been highlighted as a key policy priority by a range of stakeholders, including: governmental organizations,[1][2] law enforcement,[3][4] and the media.[5] Recent years have seen an increase in data-driven studies on this topic. However, much of the theoretical work is older and focuses on previous iterations of online technologies, as well as on previous terrorist threats. This article addresses this by offering theoretical insights which account for the advancements in communications technologies, drawing from recent research and terrorist case studies. The argument is simple: dichotomizing between "online" and "offline" realms is not ontologically defensible and can lead to missing important factors in radicalization trajectories.

The article consists of three parts: to begin, an overview of the theoretical research on online radicalization is presented, which mostly assumes that the online domain is distinct and separable from the offline. This is followed by a discussion of the work of scholars who challenge this dichotomy (mostly on topics besides terrorism), suggesting that the two spaces are inseparably intertwined. Finally, this argument is applied to recent research and terrorist case studies from the author's existing research[6] to demonstrate why it is both empirically and ontologically unsound to rely on this dichotomy. The use of these case studies—focused specifically on the so-called Islamic State (IS) within the US—are not intended to be representative, but rather used as exposition to demonstrate the ways in which terrorist activities protrude over both domains. The article argues that scholars should attempt to understand the wider information environment rather than fixating solely on one domain. Existing theoretical work, such as Situational Action Theory, as proposed by Wikström and Bouhana[7] offer a more complete picture in understanding how environments affect individuals' norm-based motivations than the theories that focus explicitly on online radicalization.

Just as Borum encouraged readers to "*Rethink Radicalization*,"[8] this article argues that we should reconsider how online radicalization is conceptualized. Borum and others have asserted that the notion of radicalization has become too ambiguous, particularly as it relates to whether it is a process of developing extreme beliefs (i.e., becoming an extremist) or engaging in extreme actions (e.g., committing an act of terror).[9][10] Although there is substantial merit to these arguments, for the sake of conceptual clarity, this article will adopt a working definition of "radicalization" which focuses on terrorist behaviors as an end point, similar to Borum's "action pathway" understanding: "the process of being involved in terrorism or engaging in violent extremist actions."[11] This does not downplay the importance of adopting extreme beliefs but rather defines the end point as behavioral.

Theorizing Online Radicalization

Since the emergence of the concept of online radicalization, scholars have attempted to theorize the process. Sageman argues there are several differences between acting online and offline, including: anonymity; younger populations; vitriolic views being expressed; easier exit ramps; nonhierarchical structures; and a lack of incentives to evolve.[12] These factors dramatically transformed jihadist terrorism from the early 2000s, in which most terror networks relied on face-to-face interactions between friends. Famously, he argued that "face-to-face radicalization has been replaced by online radicalization."[13]

Neumann offers six dynamics drawn from the academic literature which help to explain online radicalization.[14] The first two relate to exposure to extremist propaganda: *mortality salience* can lead to individuals considering their own death and increase support for violence[15] and videos from conflict zones which portray Muslims suffering which create *a sense of moral outrage.*[16] The third and fourth mechanisms relate to online communities. The Internet can act as a *criminogenic environment* in which deviant behaviors are learned and normalized,[17] which he links to the concept of an "echo chamber". Like Sageman, Neumann points to the proliferation of vitriolic views due to the *Online Disinhibition* effect.[18] The fifth process relates to the interplay between the social and interactive nature of the Internet; individuals *role-play* an idealized version of themselves online which is more zealous and supportive of violence.[19] The final dynamic is simpler; it relates to the Internet's ability to *link up with terrorist structures* and connect individuals with similar interests across great distances and no previous interactions; offering a far larger recruitment pool from previous generations.

Ducol *et al.* derive several potential radicalization dynamics from the social psychology literature, positing factors that differentiate acting online from offline.[20] The Internet may provide an opportunity for individuals to participate in new groups and the anonymity may trigger a process of deindividuation—aligning behaviors with the group and creating a diffusion of responsibility.[21] They also note that online activity may amplify attraction to a specific in-group while increasing hostility toward out-groups, which may trigger a perceived threat to the individual's identity.[22] They argue that selective exposure may create a cognitive bias which promotes polarization, as well as providing an outlet for individuals to express their "true self" by sharing their stigmatized identities with like-minded people.[23][24] Ducol and colleagues also state that online relationships may take longer to build but could result in more intimacy and connection than offline ones.[25] Moreover, individuals tend to seek out homophily, which social media platforms are specifically designed to facilitate, potentially creating an environment in which deviant subcultures can form. These subcultures are aided by secrecy and anonymity that the Internet can provide, as well as offering more settings which are prone to collective dynamics by leading to more agreement amongst members.

Radicalization is conceptualized by Koehler as a process of depluralization from political concepts and values (such as justice, freedom, and democracy) toward a specific ideology. He argues that the Internet is a main facilitator of this process as it provides an ideological pillar with the infrastructure of a radical social movement. It provides cheap and efficient communication where individuals can share crucial information, as well as being a constraint-free space with anonymity in which individuals can become "more" than their offline personas.[26] It also gives a perception of a larger critical mass of the movement, and an opportunity for individuals to directly reflect on the effects on propaganda. Koehler argues that the Internet is the most important space to learn the necessary skills to join offline groups and advance within the social hierarchies and therefore is a major driving factor to establish and foster the development of what he calls "radical contrast societies" which transmit violent ideologies and transmit them into political activism.

Scholars have attempted to "model" the process by sequencing multiple dynamics to explain how they develop into online radicalization. Saifudeen argues that the Internet has unique attributes, noting that it is akin to a buyers' market in which individuals can pick and choose the interactions and communities that best suit them.[27] He uses an analogy of a planetary orbit with five levels: *Scepticism, Validation, Activism, Extremism, Violent Extremism*. The individual remains in the orbit of their chosen online counterculture which reinforces their current mindset while "gravity wells" can pull individuals further inward. Online dynamics

can cause individuals to jump orbits very quickly given the speed of information absorption and resonance in cyberspace. Neo offers a similar approach, positing a five-stage model of *Reflection, Exploration, Connection, Resolution,* and *Operational.*[28] Like Saifudeen, Neo argues that the wide array of ideas available offer many opportunities for cognitive openings to occur and an individual's worldview can be challenged. Moreover, the Internet's anonymity facilitates an environment where an individual can experiment with an array of ideas with little consequence while having limitless access to propaganda. Combined, such exposure can help to frame and prime individuals to a new potential worldview which can exacerbate radicalization.

Drawing from their empirical research into Canadian foreign fighters, Bastug, Douai and Akca propose a four-step model to explain how online radicalization occurs.[29] It begins with the *Accessibility and Proliferation* of content, such as propaganda or contact with sympathizers. The social and psychological factors—*Susceptibility and Predisposition* —help to explain why this content may resonate with some audiences. This can move toward *Terrorist Mobilization,* in which social media plays an active role, which leads to individuals *Sharing* their own experiences on the Internet, which creates a feedback loop to the beginning by creating more content to be accessed. Weimann and Von Knop propose a model, beginning with the *Searching* phase in which individuals seek information online to fulfill their personal or spiritual needs, followed by *Seduction* where they are introduced to radical ideologies.[30] From here, users enter *Captivation*, which they argue is the most important because users begin to visit blogs, fora, and chat rooms and become attracted to seductive messages. Individuals then become integrated with their online community as part of the *Persuasion* phase and for most, this is where the road ends. However, only a select few will enter the *Operative* phase in which they gain access to contacts and materials and could be invited to join a terrorist organization. They suggest that there are several factors which cause the Internet to exacerbate radicalization, including the anonymity of the Internet, the fact that websites cater to alienated diaspora communities, and the acceptance and approval that members gain when interacting in the online milieu.

Offering a post-structuralist model, Torok likens the Internet to a Foucauldian institution in which networked powers operate and radicalize, suggesting that the online environment is a "Castle" which represents self-imposed isolation which individuals enter willingly and breeds ideological homophily.[31] In these environments, radical beliefs and behaviors become normalized and individuals become polarized as they identify as part of an in-group and therefore disparage a targeted out-group. Importantly, social media represents the "battleground" for the hearts and minds of the vulnerable and disaffected as it can replace moderate beliefs with extreme ones.

Several inferences can be drawn from these theories and models. Rather than suggesting a distinct cause-and-effect relationship, the literature suggests potential dynamics—none of which are necessary or sufficient—that may be either exclusive to, or a prominent feature of the Internet. This is analogous with radicalization research more broadly, which highlights the complexity of the process and the diversity from case to case.[32][33][34] Another prominent feature is the lack of theory derived from empirical research. Aside from Bastug, Douai and Akca's model,[35] the above research is derived either from anecdotal data or imported from other parts of social science and has not yet been tested on terrorist populations. This too, is like radicalization research—Jensen, Atwell Seate and James argue that a lack of rigorous empirical testing makes it difficult to judge how well theories work as general explanations of radicalization.[36] Instead, they argue that most theories in the field are supported by anecdotal evidence with nebulous selection criteria.

Theories also purport that engagement with propaganda is an important aspect of online radicalization. Some make this a key component,[37][38][39][40][41] while for others, such as Koehler, Neumann, and Ducol *et al*., this position is offered with a note of caution, noting that this relationship is unproven.[42][43][44] The effects of terrorist propaganda on users is still a young field with a dearth of data-driven research. Experimental studies have indicated that individuals may be more likely to engage with, or be persuaded by, extremist propaganda if they have certain characteristics like a preference for hierarchically organized societies with dominant groups within it;[45] display manipulative "Machiavellian" personality traits;[46] engage in subversive online activities such as abuse, harassment, or engagement on problematic platforms;[47] or if uncertainty or existential threat is primed.[48][49] While these studies are valuable as starting points,

experimental research struggles to recreate the complex personal and social dynamics that go into engagement with terrorism.[50] Previous research into terrorism has often assumed that propaganda will resonate and radicalize their audience with little empirical basis, akin to the now discredited "Hypodermic Needle" model of mass communication.[51][52][53]

Most importantly for what follows immediately below, theories and models assume that the online domain is distinct and separable from the offline one. By its nature, theorizing "online radicalization" implicitly suggests that a meaningful dichotomy can be drawn to show how the Internet can provide a markedly different radicalization process. Several scholars refer to the "real world" which may be dynamically connected to the Internet, but is clearly distinct.[54][55][56][57][58] Others do not explicitly use the phrase, but still imply that the two domains can be separated.[59][60] This framing of two distinct ontological realms is, it is argued here, not defensible and results in a narrow understanding of the role of communications technologies in the radicalization process.

Ontological Challenges

In the mid-2000s, Floridi predicted that in the future, the threshold between the online and offline worlds would disappear, noting that the "infosphere"—i.e. the whole information environment, the entities that exist within them, their properties, interactions, processes, and mutual relations—was being re-ontologized because of the convergence between digital resources and tools.[61] He argues that there is no longer a substantial difference between the processor and the processed, causing a gradual erasure of friction between the two ontological domains. Human beings will turn into "inforgs"—connected informational organisms, who exist in the infosphere, which is not merely supported by a material world, but will be interpreted and understood as part of an entire, singular environment, made up of both the processors and processed, online and offline.

The dichotomy of "digital dualism" is challenged by Jurgenson who argues that communications technologies have effectively linked the two domains; both spaces now enmesh to form an augmented reality.[62] Social media supplements, rather than replaces, our offline lives. Offline factors affect our friends, our social location, demographics, and epistemological standpoints, which in turn, affect our posting behaviors. Conversely, social media affects our offline activity; we are conditioned to look for the perfect photo, check-in, or status update, even when we are not logged in (if there is even a state of "not being logged in" in 2022). Jurgenson argues that nothing on the Internet exists outside of longstanding social constructions, but rather we implant these into our new augmented reality. Rey and Boesel advance and develop this into the concept of "augmented subjectivity," noting that both domains are co-produced, and experiences exist over one single, unified reality. Humans are now embodied by organic flesh and "digital protheses"—in which they can perceive, and act in, the world; neither of which can ever be isolated from experience and are inextricably enmeshed.[63] They point to a naturalistic fallacy in which the offline domain is considered as the primordial state, which in turn encourages normative judgment that gives primacy to the "real world" at the expense of digital interactions.

A group of scholars, including Floridi, have described this new hyperconnected reality as "Onlife", arguing that it no longer makes sense to dichotomize between the two domains because communication technologies have become environmental forces that affect self-conception, mutual interactions, as well as concepts of reality and interactions with it.[64] Rather than artifacts operating according to human instructions: "data are recorded, stored, computed and fed back in all forms of machines, applications, and devices in novel ways, creating endless opportunities for adaptive and personalized environments".[65] This has led to four major transformations: a blur between reality and virtuality; an unclear distinction between human, machine, and nature; a reversal between information scarcity and abundance; and a shift from the primacy of stand-alone things, properties, and binary relations to the primacy of interactions, processes, and networks.

We no longer simply "go online". This notion is a relic of the 1990s in which a user needed to make a delib-

erate decision to dial up a modem on a personal computer. Today, mobile data and devices mean that we are online almost all the time. The average person worldwide spends just under seven hours online per day, with 5.2 billion unique mobile phone users accessing the Internet for an average of four hours. Activities are split between messenger apps, social media, streaming videos, and games.[66] However, even when we are not actively online, we are not unplugged given the proliferation of push notifications, in which devices send notifications to users' home screens. This transcends the divide between purposeful and incidental exposure and has been shown to increase Internet usage.[67] Most people are either online or in a state of online readiness 24/7.

One consequence of this blurred information environment is that the distinction between public and private communications has transformed. Thorseth notes that the ubiquity of social media has changed the nature of "public space." Topics that were considered intimate (such as sexual relations or political affiliations) are now disclosed prominently on public platforms.[68] Concepts such as "public" and "private" should be now considered complementary categories, rather than mutually exclusive, which are challenged by communications technologies. The new hyperconnected world has affected our social relations; we used to have few friends with convivial relations who were mostly located near us, but now the social fabric has dramatically evolved, and people are now connected with up to (and beyond) thousands of "friends" or "followers" around the world.[69]

Another significant change is the level of information that is available to individuals within the information environment. Previously, information was considerably much more scarce than it is today and held by gatekeepers (editors of television, print media, etc.). It was also more difficult to access and disseminate than in the contemporary world, and because of the smaller economy of attention, individuals had a large internal capacity to receive it.[70] Today the opposite is true, there is an abundance of information, but we have little capacity to attend to it. Social media companies have attempted to exploit the economy of attention by designing platforms designed to retain users, which has resulted in volatile and piecemeal identities that lack empathy and capacity to read other persons' intentions. Thorseth argues that the information environment has led to wide access to information, but that we lack the capacity to incorporate diverging opinions.[71] She draws on Sunstein's concept of the *Daily Me*, in which individuals only have access to a narrow range of information that coheres to their existing worldview.[72]

This perspective has typically focused on broader sociopolitical issues rather than specifically on political violence. However, some have warned of the risks of this re-ontologized world. Jurgenson argues that it is a flammable space, referring to the Arab Spring and the Occupy Wall Street protests, which highlight the intersection between digital technologies and physical space.[73] He noted that protesters took photos and videos and were able to spread them quickly around the world to a greater audience. Rather than merely shouting in the wind, the content was met by an interested network, which in turn gave the protesters more motivation to continue. Thorseth's discussion of individuals' inability to incorporate diverging opinions briefly touches on the case of the Norwegian white supremacist terrorist attacker, Anders Behring Breivik's manifesto to demonstrate the vast quantity of information available but also a failure to incorporate the perspectives of his targeted out-groups.[74]

Re-Ontologizing Online Radicalization

Several scholars have pointed to a false dichotomy between online and offline radicalization. Gill and colleagues argue that their empirical investigation into terrorists' use of the Internet shows that "there is no easy offline versus online violent radicalization dichotomy to be drawn….Plotters regularly engage in activities in both domains."[75] These findings and sentiments are mirrored by Whittaker, whose research into the online behaviors of US-based Islamic State (IS) terrorists also found that their behaviors were spread over both domains, noting that the "melding of the online and offline environment lends further credence to the argument that it is a false dichotomy."[76] Using the same data set, Herath and Whittaker expanded on this by creating four "ideal type" pathways of terrorist engagement which describe different patterns of online

and offline behaviors. Rather than a simple dichotomy of "online" versus "offline" radicalization, their findings showed that each of the pathways exists on a spectrum.[77] These findings are supported by research conducted by Kenyon and colleagues, who used closed-source data on convicted UK terrorists. They found that although the use of the Internet was increasing, it was not replacing offline interactions—rather individuals tended to operate in both domains.[78]

Research conducted across eight countries by Hamid & Ariza found that of 439 terrorists, the majority (238) were radicalized "mostly offline", while 77 were "mostly online" and 8 were classified as "online asocial radicalization".[79] In their study of lone actor terrorists, Lindekilde, Malthaner and O'Connor highlight that behavioral patterns exist across both domains simultaneously, and as a result are mutually reinforcing.[80] Ducol offers a theoretical approach to radicalization based on Situational Action Theory in which he critiques existing theoretical discussions that assume there are two worlds, "virtual" and "real," that do not affect each other, suggesting instead that theory should conceptualize different "life spheres" in both domains (such as friends, family, social media, websites) that can become intertwined and lead to a cognitive monopoly which can radicalize.[81]

Each of these authors argues that there is a false dichotomy, but they still assume (in some cases implicitly by their coding system) that online behaviors can be meaningfully separated from offline. This section will push these arguments further by demonstrating that many of the behaviors that one might consider belonging to one domain cannot be easily demarcated. Rather than showing that terrorists tend to operate in both, it will, using the arguments laid out in the previous section, re-ontologize the debate and question the utility of considering this simplistic demarcation. To do this, this section will draw on existing empirical and theoretical research, as well as case study examples of terrorists for the purpose of exposition.

The largest existing contribution to this argument is made by Valentini, Lorusso and Stephan, who develop the Onlife thesis to radicalization. They argue that scholars in the field have conceptualized virtual spaces as distinct from the "real world"—which this article has demonstrated above. Rather, in contemporary extremism, such spaces are not clearly defined, and the two domains conflate in unprecedented ways: "radicalization processes evolve, and develop, by integrating elements that pertain to both."[82] They make this argument by discussing an online environmental dynamic—content-sharing algorithms—to demonstrate why scholars ought to rethink this dichotomy. These algorithms draw heavily on factors from both domains, such as online history, and tracked information such as location, recent purchases, and phone calls. Moreover, time spent away from social media platforms and unposted comments also affect how algorithms operate.[83] They also highlight the importance of portable devices, which help platforms to structure accurate information on users, even in the offline domain. They reconceptualize the notion of an "echo chamber"—featured in almost every online radicalization theory above—as an "echo system" which incorporates both domains in a constant and seamless feedback loop with each other. This is in keeping with previous research, which highlights the importance of offline homogenous groups as well as online ones.[84][85]

Propaganda Engagement

The blurry intersection between online and offline extremist behavior is further exemplified by Baugut and Neumann's interviews with 44 convicted and former German and Austrian Islamists. Their participants consumed propaganda online, then discussed it with their peers and preachers face-to-face. The converse was also true; individuals would have face-to-face discussions at mosques in which peers would recommend content, which they would watch later online.[86] Moreover, participants watched online propaganda *with* their offline networks, sitting together and watching radical preachers on YouTube and discussing afterward. They were also drawn further into radicalization by the platform's recommendation system. They noted that in their sample, the two modes of communication were strongly intertwined, lending further weight to the notion that there is a false dichotomy.

Terrorist cells in the US have also held "viewing parties" in which they would congregate at co-ideologues' houses and watch radical content together. In a group of would-be travelers to IS in Minneapolis/St. Paul:

"the men would spend hours watching a YouTube channel called Enter the Truth…all slick Islamic State productions, focused on the suffering of Syrian children and the moral corruption of the West."[87] The group would also sit in a circle, swapping devices with each other to share and recommend propaganda.[88] The cell responsible for the attack in Garland (Texas), watched content together, expressing their pleasure while watching execution videos and being visibly excited after the Charlie Hebdo attack.[89] Other small cells displayed similar behaviors, including Jaelyn Young and Mohammed Daklalla[90], Munther Omar Saleh and Fareed Mumuni,[91] Mahmoud Elhasssan and Joseph Farrokh[92], and Sixto Ramiro Garcia and Asher Abid Khan.[93]

These case studies and the interview research by Baugut and Neumann help to demonstrate that engagement with terrorist propaganda is more than a unidirectional relationship in which the content can radicalize its audience like a hypodermic needle injection. Instead, there is a complex information environment that protrudes over both domains. Rather than audiences being passively radicalized by propaganda, content is a topic of conversation or an activity between like-minded friends. After watching IS's video *Healing the Believers' Chests* which depicts the immolation of Jordanian pilot Muath Safi Yousef al-Kasasbeh, several terrorists discussed it and drew justifications from IS propaganda. Arafat Nagi told an unnamed co-ideologue "do to them as they do to you…they drop bombs and burn people,"[94] while Terrance McNeil took to Facebook and said "This is what happens when you bomb women and children and get caught. Alhumdullilah I was worried for a while they might let that murderer go."[95] Many others shared the video with their followers, such as Islam Said Natsheh,[96] David Wright,[97] or Khalil Abu Rayyan,[98] while others expressed explicit support amongst their peers.[99][100][101] Some of these instances took place online, others took place offline, but they both demonstrate that there is a complex information environment. Rather than mere consumption of propaganda, these cases demonstrate active dialectical engagement.

Terrorists as Prosumers

Online radicalization theories tend to focus heavily on the consumption of radical propaganda. Far less attention is paid to them as "prosumers," who are at the same time *pro*ducers and con*sumers* of violent extremist materials.[102] This is also an activity that straddles both domains; terrorists regularly take and upload photographs of themselves for their audience on social media. Jalil Aziz donned military gear, an AR-15, a knife, fingerless gloves, and a balaclava and uploaded it to his contacts on Twitter,[103] while Gregory Lepsky uploaded photos to Facebook holding a semi-automatic rifle and a pistol with the comment "look at these sick photos of me yooo."[104] Others adopted symbols of IS in their uploaded content—e.g., the tawheed gesture, such as Harlem Suarez[105]—or posed with the group's black standard flag.[106][107]

Terrorists also create and share videos for their audiences; Haris Qamar visited several tourist sites around Washington DC with a confidential FBI source to create a video for IS which encouraged lone actor attacks. As they drove past the Pentagon, Qamar shouted "bye bye DC, stupid ass kufar, kill 'em all."[108] Zakaryia Abdin uploaded a video to social media of himself shooting an AK-47 at a local gun range in South Carolina.[109] Other terrorists planned to make videos if their plots were successful, such as Munir Abdulkader and John T. Booker, whose respective plots involved abducting military officers or veterans and executing them on camera.[110][111] Each of these activities was designed to be uploaded and shared on the Internet, yet they fundamentally relied on actors' non-virtual activity in risky or noteworthy places to create the content.

These outward expressions of ideology on public social media platforms seem to be counterintuitive. Research has demonstrated that terrorists who act online are less likely to be successful than those who do not, possibly because they announce their intentions, allowing law enforcement to open investigations against them.[112][113] Understanding these behaviors within the re-ontologized information environment helps to offer a clearer picture. As discussed above, the traditional distinction between public and private has become blurry and individuals negotiate and manage identity for their perceived audiences.[114][115][116] This type of reputation management has been called "staged authenticity"[117] in which individuals create an ultra-pious and zealous jihadist avatar for their audience.[118] These activities are not merely confined to

the online domain; individuals broadcast to their contacts who are often made up of offline networks; chose to take photos in hostile physical spaces; or with terrorist symbols because, as argued above, the infosphere trains users to look for the perfect photo, check-in, or status update in physical spaces.[119]

Understanding Radicalization Environments

If the online and offline domains are ontologically inseparable, then "online radicalization" becomes a redundant concept. As Gill and colleagues argue, we should not fixate on a simple location of radicalization but instead need to "understand the drives, needs, and forms of behavior that led to the radicalization and attack planning and why offenders chose that environment rather than purely looking at the affordances the environment produced."[120] The frame of a binary dichotomy tends to result in the Internet being given radicalizing agency, which overlooks other important factors such as vulnerabilities, stressors, or how online and offline factors combine. For example, in research conducted by Reynolds and Hafez, they tested three hypotheses to best explain the recruitment of German foreign fighters, including ones that emphasise the importance of online radicalization and offline networks.[121] However, as argued above, we must understand that being situated in (and around) radical communities affects propensities to engage online. Offline proximity is an important factor in determining how social media content-sharing algorithms prioritize interactions.[122] Users are more likely to be shown or recommended materials if they come from an individual that is part of their local network.

Therefore, the question should not be "do terrorists radicalize online?" but instead "what role do information environments play in radicalization?" This reframing forgoes an online/offline dichotomy, which is neither empirically nor ontologically defensible. Individuals' environments are made up of interactions that span across both domains in ways which are not easy to separate. One existing framework that is well suited to doing this is Situational Action Theory (SAT) which assesses how an individual's propensity to radicalization (such as their vulnerabilities or stressors) interacts with their environment to affect their norm-based motivations. In other words, why do some individuals see terrorism as an acceptable (and often the *only* acceptable) form of action?[123] SAT does not assume propaganda will influence its audience, nor does it preclude it, but instead attempts to understand why it may resonate with some, but not others, based on the individual and their environment. The theory highlights the importance of socialization within certain settings, regardless of whether they are offline or online.[124] Taking the example of the "viewing parties" discussed above, it is not relevant whether this is an example of online radicalization or not, it merely attempts to understand how environments affect norm-based motivations.

One might reasonably argue that there are practical applications to an online/offline dichotomy, particularly when considering behaviors (such as assessing whether someone has radicalized entirely online or offline) or the benefits and challenges of counter-extremism interventions, such as counter-messaging or signposting toward services. However, it is argued here that there is greater utility in *more* specificity rather than relying on a simplistic dichotomy. Taking a more holistic view also offers an opportunity to attempt to understand the environmental differences between platforms and how they may affect radicalization. Rather than grouping a range of distinct behaviors as "online" (such as posting on Twitter; watching videos on YouTube; communicating visually on Skype; or interacting anonymously on Telegram), these platforms offer entirely different user experiences and have a different set of rules and realities. For example, when comparing political discussions on Facebook and YouTube, Halpern and Gibbs found differences in user deliberation. The former's interconnectedness and lack of anonymity expands the flow of information and allows for symmetrical discussion, while the latter, which is more anonymous and deindividuated, results in less polite discourse.[125] Rather than saying "this terrorist acted online," or "this is an example of an online intervention," there is greater utility in speaking specifically about the affordance of the platform in question.

Conway identified this as a major knowledge gap, suggesting that research should compare the different functionalities of platforms and how extremists exploit them.[126] Presently, we do not know how Twitter users' experience of 280-character posts, public audiences, and algorithmically sorted timelines com-

pares with Telegram's invite-only groups, self-destruct messages, and relative lack of content moderation. Therefore, when groups like IS migrated from the former to the latter,[127] we have little idea of how each platform's environment affected radicalization. If there is an "online disinhibition" effect that could exacerbate radicalization,[128][129] we do not know if platforms do so uniformly. Moreover, research has suggested that platforms' recommendation systems are not uniform when it comes to promoting extremist content,[130] which suggests environmental differences when it comes to algorithmic amplification. Rather than grouping all platforms as "online", it is more analytically useful to understand these user experiences in relation to each other as part of a wider environment. It is possible that there are more differences between some types of online communication than between online and face-to-face communication.

Conclusion

This article has sought to demonstrate that online radicalization is a redundant concept. Academic theories have hypothesized dynamics to explain that acting on the Internet may exacerbate radicalization. The purpose of this article was not to rebut these dynamics; given the weight of evidence, concepts such as disinhibition, echo chambers, or deindividuation could indeed play an important role. Instead, the argument is that it is not analytically useful to dichotomize between an online and offline domain. Not only has existing research shown that terrorist behaviors tend to spill across both, but existing critiques demonstrate that it is not an ontologically defensible position. Many behaviors that would be considered evidence of online radicalization—such as streaming propaganda; posting pictures on Facebook; or being recommended content on YouTube—cannot be easily attributed to a single domain. Rather, terrorists engage in an ongoing socialization process within their environment that often protrudes this simple dichotomy. As noted above, the examples offered were intended merely as exposition and a jumping-off point to explain this critique. Future research should analyze and begin to theorize this ontological framework in a more rigorous way. In particular, it will be fruitful to compare different ideologies who may have different norms when it comes to communications—for example, to assess whether "very online" communities such as incels or QAnon interweave the two domains in a comparable manner.

It seems advisable to avoid theories which attempt to explain how *online* radicalization works, instead focusing on more holistic theories that account for individuals' predispositions, stressors, their engagement with their environment, and systemic level factors. This article proposes that theories such as SAT offer a clearer road to understanding the role of communication technologies in their wider context, rather than focusing merely on the technologies themselves. While policy makers may opt for monocausal explanations of radicalization that fixate on a specific location, holistic theoretical understandings will be a key tool in explaining the complexity of radicalization to decision makers.

About the Author: **Joe Whittaker** *is a lecturer in cyber threats in the Department of Criminology, Sociology, and Social Policy at Swansea University. He completed his joint PhD at Swansea University and Leiden University's Institute of Security and Global Affairs on the topic of online radicalization. He also researches extremism in the context of recommendation algorithms, video games, and counter-messaging. You can contact him via email (j.j.whittaker@Swansea.ac.uk) or follow him on Twitter (@CTProject_JW).*

Notes

[1] HM Government. (2019): "Online Harms White Paper," London: The Stationery Office. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/793360/Online_Harms_White_Paper.pdf.

[2] Wiktorowicz, Q. (2013): "Working to Counter Online Radicalization to Violence in the United States," White House Blog, URL: https://obamawhitehouse.archives.gov/blog/2013/02/05/working-counter-online-radicalization-violence-united-states.

[3] Federal Bureau of Investigation. (n.d.): "What We Investigate – Terrorism." URL: https://www.fbi.gov/investigate/terrorism.

[4] Europol. (2018): "TE SAT: European Union Terrorism Situation and Trend Report," The Hague.

[5] New York Times Editorial Board. (2018): "The New Radicalization of the Internet," *New York Times*, November 24. URL: https://www.nytimes.com/2018/11/24/opinion/sunday/facebook-twitter-terrorism-extremism.html.

[6] Whittaker, J. (2021): "The Online Behaviors of Islamic State Terrorists in the United States," *Criminology and Public Policy*, 20, pp. 177–203.

[7] Wikström, P. O. H. and Bouhana, N. (2017): "Analyzing Radicalization and Terrorism: A Situational Action Theory"; in: LaFree, G. and Freilich, J. D. (Eds.) *The Handbook of the Criminology of Terrorism*. Chichester: John Wiley & Sons, pp. 175–186.

[8] Borum, R. (2011): "Rethinking Radicalization," *Journal of Strategic Security*, 4(4), pp. 1–6. URL: https://digitalcommons.usf.edu/jss/vol4/iss4/1/.

[9] Horgan, J. (2008): "From Profiles to Pathways and Roots to Routes: Perspectives from Psychology on Radicalization into Terrorism," *The Annals of the American Academy of Political and Social Science*, 618(1), pp. 80–94.

[10] Schuurman, B. and Taylor, M. (2018): "Reconsidering Radicalization: Fanaticism and the Link Between Ideas and Violence," *Perspectives on Terrorism*, 12(1), pp. 3–22.

[11] Borum, R. (2011): "Rethinking Radicalization," p. 2.

[12] Sageman, M. (2008): *Leaderless Jihad: Terror Networks in the Twenty-First Century*. Philadelphia: PA: University of Pennsylvania Press.

[13] Sageman, M. (2008): "The Next Generation of Terror," *Foreign Policy*, (March/April), pp. 36–42.

[14] Neumann, P. (2013): "Options and Strategies for Countering Online Radicalization in the United States," *Studies in Conflict & Terrorism*, 36(6), pp. 431–459.

[15] Pyszczynski, T. *et al.* (2006): "Mortality Salience, Martyrdom, and Military Might: The Great Satan Versus the Axis of Evil," *Personality and Social Psychology Bulletin*, 32(4), pp. 525–537.

[16] Sageman, M. (2008): *Leaderless Jihad*, op. cit.

[17] Sutherland, E. H. (1947): *Principles of Criminology*, 4th ed. Chicago: Lippincott.

[18] Suler, J. (2004): "The Online Disinhibition effect," *CyberPsychology & Behavior*, 7(3), pp. 321–326.

[19] Brachman, J. M. and Levine, A. N. (2011): "You Too Can Be Awlaki," *The Fletcher Forum of World Affairs*, 35(1), pp. 25–46.

[20] Ducol, B. *et al.* (2016): "Assessment of the State of Knowledge: Connections Between Research on the Social Psychology of the Internet and Violent Extremism," *Canadian Network for Research on Terrorism, Security and Society*, (16).

[21] Spears, R. et al. (2002): "Computer-Mediated Communication as a Channel for Social Resistance: The Strategic Side of SIDE," *Small Group Research*, 33; pp. 555–574.

[22] Harris, K., Gringart, E. and Deirdre, D. (2014): "Understanding the Role of Social Groups in Radicalisation," *7th Australian Security and Intelligence Conference*, Edith Cowan University, Perth, Western Australia, 1–3 December.

[23] Slater, D. (2002): "Social Relationships and Identity Online and Offline"; in: Lievrouw, L. and Livingstone, S. *Handbook of New Media: Social Shaping and Consequences of ICTs*. London: Sage, pp. 553–546.

[24] McKenna, K. Y. and Bargh, J. A. (1998): "Coming Out in the Age of the Internet: Identity "Demarginalization" Through Virtual Group Participation," *Journal of Personality and Social Psychology*, 75(3), pp. 681–694.

[25] Walther, J. B. (1996): "Computer-Mediated Communication: Impersonal, Interpersonal, and Hyper-personal Interaction," *Communication Research*, 23(1), pp. 3–43.

[26] Koehler, D. (2014): "The Radical Online: Individual Radicalization Processes and the Role of the Internet," *Journal for Deradicalization*, (1), pp. 116–134.

[27] Saifudeen, O. A. (2014): "The Cyber Extremism Orbital Pathways Model," *RSIS Working Paper*.

[28] Neo, L. S. (2016): "An Internet-Mediated Pathway for Online Radicalisation: RECRO"; in: Khader, M. (Ed.) *Combating Violent Extremism and Radicalization in the Digital Era*. Hershey, PA: Information Science Reference, pp. 197–224.

[29] Bastug, M. F., Douai, A. and Akca, D. (2018): "Exploring the 'Demand Side' of Online Radicalization: Evidence from the Canadian Context," *Studies in Conflict & Terrorism*. DOI: 10.1080/1057610X.2018.1494409.

[30] Weimann, G. and Von Knop, K. (2008): "Applying the Notion of Noise to Countering Online Terrorism," *Studies in Conflict & Terrorism*, 31, pp. 883–902.

[31] Torok, R. (2013): "Developing an Explanatory Model for the Process of Online Radicalisation and Terrorism," *Security Informatics*, 2(6), pp. 1–10.

[32] Hafez, M. M. and Mullins, C. (2015): "The Radicalization Puzzle: A Theoretical Synthesis of Empirical Approaches to Homegrown Extremism," *Studies in Conflict & Terrorism*, 38(11), pp. 958–975.

[33] Borum, R. (2017): "The Etiology of Radicalization"; in: LaFree, G. and Freilich, J. D. (Eds.) *The Handbook of the Criminology of Terrorism*. Chichester: John Wiley & Sons, pp. 17–32.

[34] Jensen, M., Atwell Seate, A. and James, P. (2020): "Radicalization to Violence: A Pathway Approach to Studying Extremism," *Terrorism and Political Violence*, 32(5), pp. 1067–1090.

[35] Bastug, M. F., Douai, A. and Akca, D. (2018): "Exploring the 'Demand Side' of Online Radicalization," op. cit.

[36] Jensen, M., Atwell Seate, A. and James, P. (2020): "Radicalization to Violence," op. cit.

[37] Weimann, G. and Von Knop, K. (2008): "Applying the Notion of Noise to Countering Online Terrorism," op. cit.

[38] Torok, R. (2013): "Developing an explanatory model for the process of online radicalisation and terrorism," op. cit.

[39] Saifudeen, O. A. (2014): "The Cyber Extremism Orbital Pathways Model," op. cit.

[40] Neo, L. S. (2016): "An Internet-Mediated Pathway for Online Radicalisation: RECRO," op. cit.

[41] Bastug, M. F., Douai, A. and Akca, D. (2018): "Exploring the 'Demand Side' of Online Radicalization," op. cit.

[42] Koehler, D. (2014): "The Radical Online," op. cit.

[43] Neumann, P. (2013): "Options and Strategies for Countering Online Radicalization in the United States," op. cit.

[44] Ducol, B. et al. (2016): "Assessment of the State of Knowledge," op. cit.

[45] Reeve, Z. (2019): "Engaging with Online Extremist Material: Experimental Evidence," *Terrorism and Political Violence*, pp. 1–34.

[46] Braddock, K., Schumann, S., Corner, E. and Gill, P. (2022): "The Moderating Effects of 'Dark' Personality Traits and Message Vividness on the Persuasiveness of Terrorist Narrative Propaganda," *Frontiers in Psychology*, 13.

[47] Braddock, K., Hughes, B., Goldberg, B. and Miller-Idris, C. (2022): "Engagement in Subversive Online Activity Predicts Susceptibility to Persuasion by Far-right Extremist Propaganda," *New Media & Society*.

[48] Rieger, D., Frischlich, L. and Bente, G. (2013): *Propaganda 2.0: Psychological Effects of Right-Wing and Islamic Extremist Internet Videos*. Köln: Wolters Kluwer.

[49] Frischlich, L. *et al.* (2015): "Dying the Right Way? Interest in and Perceived Persuasiveness of Parochial Extremist Propaganda Increases after Mortality Salience," *Frontiers in Psychology*, 6(August), pp. 1–11.

[50] Braddock, K. (2022): "Vaccinating Against Hate: Using Attitudinal Inoculation to Confer Resistance to Persuasion by Extremist Propaganda," *Terrorism and Political Violence,* 34(2), pp. 240–262.

[51] Sageman, M. (2014): "The Stagnation in Terrorism Research," *Terrorism and Political Violence*, 26(4), pp. 565–580.

[52] Archetti, C. (2015): "Terrorism, Communication and New Media: Explaining Radicalization in the Digital Age," *Perspectives on Terrorism*, 9(1), pp. 49–59.

[53] Aly, A. (2017): "Brothers, Believers, Brave Mujahideen: Focusing Attention on the Audience of Violent Jihadist Preachers," *Studies in Conflict & Terrorism*, 40(1), pp. 62–76. DOI: 10.1080/1057610X.2016.1157407.

[54] Weimann, G. and Von Knop, K. (2008): "Applying the Notion of Noise to Countering Online Terrorism," op. cit.

[55] Neumann, P. (2013): "Options and Strategies for Countering Online Radicalization in the United States," op. cit.

[56] Torok, R. (2013): "Developing an Explanatory Model for the Process of Online Radicalisation and Terrorism," op. cit.

[57] Koehler, D. (2014): "The Radical Online," op. cit.

[58] Neo, L. S. (2016): "An Internet-Mediated Pathway for Online Radicalisation: RECRO," op. cit.

[59] Sageman, M. (2008): *Leaderless Jihad,* op. cit.

[60] Bastug, M. F., Douai, A. and Akca, D. (2018): "Exploring the 'Demand Side' of Online Radicalization," op. cit.

[61] Floridi, L. (2007): "A look into the future impact of ICT on our lives," *Information Society*, 23(1), pp. 59–64.

[62] Jurgenson, N. (2012): "When Atoms Meet Bits: Social Media, the Mobile Web and Augmented Revolution," *Future Internet*, 4(1), pp. 83–91.

[63] Rey, P. J. and Boesel, W. E. (2014): "The Web, Digital Prostheses, and Augmented Subjectivity," *Routledge Handbook of Science, Technology, and Society* (January 2014), pp. 173–188.

[64] Floridi, L. (2015): "Introduction"; in: Floridi, L. [Ed.] *The Onlife Manifesto: Being Human in a Hyperconnected Era*, London: SpringerOpen, pp. 1–7.

[65] Floridi, L. et al. (2015): "The Onlife Manifesto"; in: Floridi, L.[Ed.] *The Onlife Manifesto: Being Human in a Hyperconnected Era*, London: SpringerOpen, p. 10.

[66] Kemp, S. (2021): "Digital 2021: Global Overview Report," *DataPortal*, 27 January. URL: https://datareportal.com/reports/digital-2021-global-overview-report.

[67] Stroud, N. J., Peacock, C. and Curry, A. L. (2020): "The Effects of Mobile Push Notifications on News Consumption and Learning," *Digital Journalism,* Vol. 8(1), pp. 32–48

[68] Thorseth, M. (2015): "Commentary of the Manifesto"; in: Floridi, L.[Ed.] *The Onlife Manifesto: Being Human in a Hyperconnected Era*, London: SpringerOpen, pp. 37–40.

[69] Ganascia, J. (2015): "Views and Examples on Hyper-Connectivity"; in: Floridi, L.[Ed.] *The Onlife Manifesto: Being Human in a Hyperconnected Era*, London: SpringerOpen, pp. 65–88.

[70] Broadbent, S. & Lobet-Maris, C. (2015): "Towards a Grey Ecology"; in: Floridi, L.[Ed.] *The Onlife Manifesto: Being Human in a Hyperconnected Era*, London: SpringerOpen, pp. 111–124

[71] Thorseth, M. (2015): "On Tolerance and Fictitious Publics"; in: Floridi, L.[Ed.] *The Onlife Manifesto: Being Human in a Hyperconnected Era*, London: SpringerOpen, pp. 245–260.

[72] Sunstein, C. R. (2001): *Republic.com.* Princeton, NJ: Princeton University Press.

[73] Jurgenson, N. (2012): "When Atoms Meet Bits," op. cit.

[74] Thorseth, M. (2015): "On Tolerance and Fictitious Publics," op. cit.

[75] Gill, P. et al. (2017): "Terrorist Use of the Internet by the Numbers: Quantifying Behaviors, Patterns, and Processes," *Criminology and Public Policy*, 16(1), p. 114.

[76] Whittaker, J. (2021): "The Online Behaviors of Islamic State Terrorists in the United States," op. cit. p. 195.

[77] Herath, C. and Whittaker, J. (2021): "Online Radicalisation: Moving beyond a Simple Dichotomy," *Terrorism and Political Violence.*

[78] Kenyon, J., Bender J. and Baker-Beall, C. (2022): "Understanding the Role of the Internet in the Process of Radicalisation: An Analysis of Convicted Extremists in England and Wales," *Studies in Conflict and Terrorism*.

[79] Hamid, N. and Ariza, C. (2022): "Offline Versus Online Radicalisation: Which is the Bigger Threat?" *Global Network on Extremism & Technology*.

[80] Lindekilde, L., Malthaner, S. and O'Connor, F. (2019): "Peripheral and Embedded: Relational Patterns of Lone-Actor Terrorist Radicalization," *Dynamics of Asymmetric Conflict: Pathways toward Terrorism and Genocide*, 12(1), pp. 20–41.

[81] Ducol, B. (2015): "A Radical Sociability: In Defense of an Online/Offline Multidimensional Approach to Radicalization"; in: Bouchard, M. (ed.) *Social Networks, Terrorism, and Counter-Terrorism: Radical and Connected*. London: Routledge, pp. 82–104.

[82] Valentini, D., Lorusso, A. M. and Stephan, A. (2020): "Onlife Extremism: Dynamic Integration of Digital and Physical Spaces in Radicalization," *Frontiers in Psychology*, 11(March), p. 12.

[83] Cohen, J. N. (2018): "Exploring Echo-Systems: How Algorithms Shape Immersive Media Environments," *Journal of Media Literacy Education*. Vol. 10, pp. 139–151.

[84] Gentzkow, M. and Shapiro, J. M. (2011): "Ideological Segregation Online and Offline," *Quarterly Journal of Economics*,

126(4), pp. 1799–1839.

[85] Pattie, C. and Johnston, R. (2016): "Talking With One Voice? Conversation Networks and Political Polarisation," *The British Journal of Politics and International Relations*, 18(2), pp. 482–497.

[86] Baugut, P. and Neumann, K. (2020): "Online Propaganda Use During Islamist Radicalization," *Information Communication and Society*, 23(11), pp. 1570–1592.

[87] Koerner, B. I. (2017): "Can You Turn a Terrorist Back into a Citizen?" *Wired*, 24 January. URL: https://www.wired.com/2017/01/can-you-turn-terrorist-back-into-citizen/.

[88] Temple-Raston, D. (2015): "He Wanted Jihad. He Got Foucault," *New York Magazine*, 27 November. URL: http://nymag.com/intelligencer/2017/11/abdullahiyusuf-isis-syria.html?gtm=bottom.

[89] *USA v. Abdul Malik Abdul Kareem,* Government's Sentencing Memorandum, Case: 2:15- cr-00707-SRB, United States District Court for the District of Arizona, 2016.

[90] Green, E. (2017): "How Two Mississippi College Students Fell in Love and Decided to Join a Terrorist Group," *The Atlantic*, 1 May. URL: https://www.theatlantic.com/politics/archive/2017/05/mississippi-youngdakhlalla/524751/.

[91] *USA v. Munther Omar Saleh and Fareed Mumuni,* Government's Sentencing Memorandum, Case: 1:15-cr00393-MKB, United States District Court for the Eastern District of New York, 2018.

[92] *USA v. Mahmoud Amin Mohamed Elhassan,* Government's Sentencing Memorandum, Case: 1:16-cr-0064- AJT, 2017.

[93] Goldman, A. (2015): "An American Family Saved Their Son from Joining the Islamic State. Now He Might Go to Prison," *Washington Post*, 6 September.

[94] *USA v. Arafat: M. Nagi,* Criminal Complaint, Case 1:15-cr-00148, United States District Court for the Western District of New York, 2015.

[95] *USA v. Terrence Joseph McNeil,* Affidavit, Case: 5:15-mj-01176-KBB, United States District Court for the Northern District of Ohio, 2015.

[96] *USA v. Islam Said Natsheh,* Government's Sentencing Memorandum, Case: 3:16-cr-00166-RS, United States District Court for the Northern District of California, 2016.

[97] Hughes, S. Meleagrou-Hitchens, A. and Clifford, B. (2018): "A New American Leader Rises in ISIS," *The Atlantic*, 13 January. URL: https://www.theatlantic.com/international/archive/2018/01/isis-americahoxha/550508/.

[98] *USA v. Khalil Abu Rayyan,* Criminal Complaint, Case: 2:16-mj-30039-DUTY, United States District Court for the Eastern District of Michigan, 2016.

[99] *USA v. Alaa Saadeh,* Criminal Complaint, [Unknown case #], United States District Court for the District of New Jersey, 2015. URL: https://extremism.gwu.edu/sites/g/files/zaxdzs2191/f/Saadeh%2C%20A.%20Criminal%20Complaint.pdf.

[100] *USA v. Laith Waleed Alebbini,* Motion to Revoke Detention Order, United States District Court for the Southern District of Ohio, Case: 317-cr-00071-WHR, 2017.

[101] *USA v. Ahmed Mohammed el Gammel,* Criminal Complaint, Case: 1:15-cr-00588-ER, United States District Court for the Southern District of New York, 2015.

[102] Conway, M. (2017): "Determining the Role of the Internet in Violent Extremism and Terrorism: Six Suggestions for Progressing Research," *Studies in Conflict & Terrorism*, 40(1), pp. 77–98.

[103] *USA v. Jalil ibn Ameer Aziz*, Government's Sentencing Memorandum, Case: 1:15-cr-00309-CCC, United States District Court for the Middle District of Pennsylvania, 2017.

[104] *USA v. Gregory Lepsky*, Criminal Complaint, Case: 3:18-cr-00114, United States District Court, District of New Jersey, 2017.

[105] *USA v. Harlem Suarez*, Government's Sentencing Memorandum, Case: 4:15-cr-10009-JEM, United States District Court for the Southern District of Florida, 2017.

[106] *USA v. Sajmir Alimehmeti*, Criminal Complaint, Case: 1:16-cr-00398, United States District Court for the Southern District of New York, 2016.

[107] *USA v. Joseph Jones and Edward Schimenti*, Criminal Complaint, Case: 1:17-cr-00236, United States District Court for the Northern District of Illinois, 2017.

[108] *USA v. Haris Qamar*, Statement of Facts, Case: 1:16-cr-00227-LMB, United States District Court for the Eastern District of Virginia, 2016, p. 10.

[109] *USA v. Zakaryia Abdin*, Criminal Complaint, Case: 2:17-mj-00081-MCRI, United States District Court for the District of South Carolina, 2017.

[110] *USA v. Munir Abdulkader*, Sentencing Proceedings, Case: 1:16-CR-019, United States District Court for the Southern District of Ohio, Western Division, 2016.

[111] *USA v. John T. Booker Jr.* Criminal Complaint, Case: 5:15-mj-05039-KGS, United States District Court for the District of Kansas, Topeka Docket, 2015.

[112] Jensen, M. et al. (2018); "The Use of Social Media by United States Extremists," National Consortium for the Study of Terrorism and Responses to Terrorism. URL: https://www.start.umd.edu/publication/use-social-media-united-states-extremists.

[113] Whittaker, J. (2021): "The Online Behaviors of Islamic State Terrorists in the United States," op. cit.

[114] Thorseth, M. (2015): "Commentary of the Manifesto," op. cit.

[115] Ess, C. (2015): "The Onlife Manifesto: Philosophical Backgrounds, Media Usages, and the Futures of Democracy and Equality"; in: Floridi, L.[Ed.] *The Onlife Manifesto: Being Human in a Hyperconnected Era*, London: SpringerOpen, pp. 89–110.

[116] Hildebrandt, M. (2015): "Dualism is Dead. Long Live Plurality (Instead of Duality)"; in: Floridi, L.[Ed.] *The Onlife Manifesto: Being Human in a Hyperconnected Era*, London: SpringerOpen, pp. 27–30.

[117] Uimonen, P. (2013): "Visual identity in Facebook," *Visual Studies*, 28(2), pp. 122–135. DOI: 10.1080/1472586X.2013.801634.

[118] Brachman, J. M. and Levine, A. N. (2011): "You Too Can Be Awlaki," op. cit.

[119] Jurgenson, N. (2012): "When Atoms Meet Bits," op. cit.

[120] Gill, P. et al. (2017): "Terrorist Use of the Internet by the Numbers," op. cit. p. 114.

[121] Reynolds, S. C. and Hafez, M. M. (2019): "Social Network Analysis of German Foreign Fighters in Syria and Iraq," *Terrorism and Political Violence*, Vol. 31 (4), pp. 661–686.

[122] Valentini, D., Lorusso, A. M. and Stephan, A. (2020): "Onlife Extremism," op. cit.

[123] Wikström, P. O. H. and Bouhana, N. (2017): "Analyzing Radicalization and Terrorism," op. cit.

[124] Bouhana, N. (2019): "The Moral Ecology of Extremism: A Systemic Perspective," *Commission for Countering Extremism*. URL: https://www.gov.uk/government/publications/the-moral-ecology-of-extremism-a-systemic-perspective.

[125] Halpern, D. and Gibbs, J. (2013): "Social Media as a Catalyst for Online Deliberation? Exploring the Affordances of Facebook and YouTube for Political Expression," *Computers in Human Behavior*, 29(3), pp. 1159–1168.

[126] Conway, M. (2017): "Determining the Role of the Internet in Violent Extremism and Terrorism," op. cit.

[127] Conway, M. (2016): "Violent Extremism and Terrorism Online in 2016: The Year in Review," *Vox Pol*. URL: https://www.voxpol.eu/download/vox-pol_publication/Year-In-Review-WEB.pdf

[128] Suler, J. (2004): "The Online Disinhibition Effect," *CyberPsychology & Behavior*, 7(3), pp. 321–326

[129] Neumann, P. (2013): "Options and Strategies for Countering Online Radicalization in the United States," op. cit.

[130] Whittaker, J. et al. (2021): "Recommender Systems and the Amplification of Extremist Content," *Internet Policy Review,* 10(2).