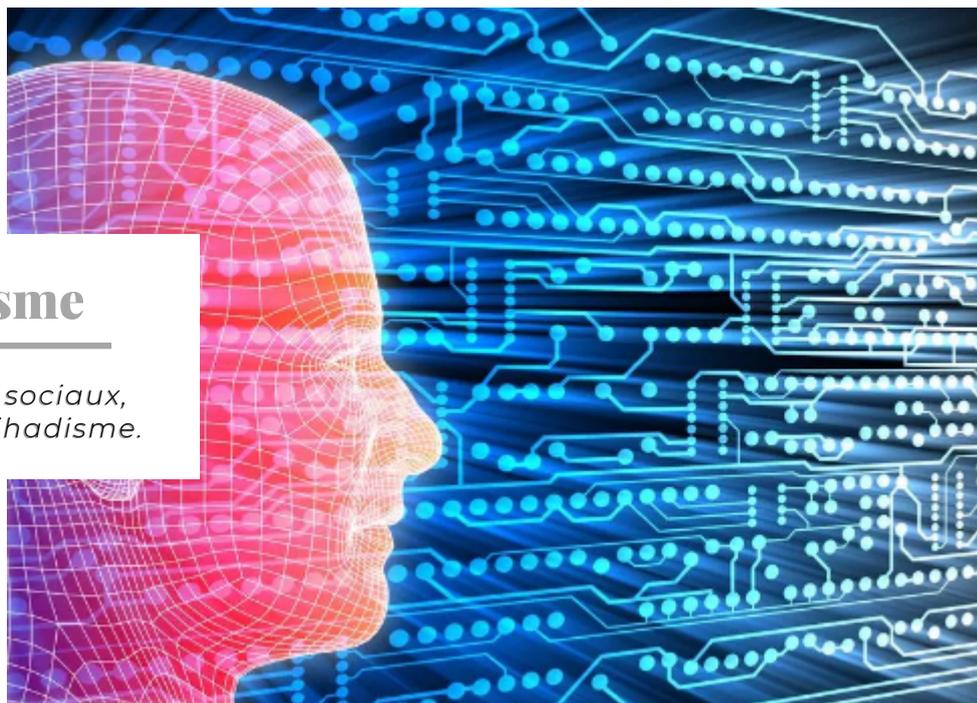


TERRORISME , INTERNET ET RÉSEAUX SOCIAUX

Fabrice LOLLIA, docteur en sciences de l'information et de la communication



Terrorisme

Internet, réseaux sociaux, radicalisation, djihadisme.

À propos de l'auteur



Fabrice LOLLIA

Docteur en sciences de l'information et de la communication.

Il est spécialiste des questions de sécurité afférentes aux nouvelles technologies.

Aujourd'hui, de plus en plus de chercheurs considèrent l'environnement numérique comme un vecteur de radicalisation, une sorte d'« incubateur à terroristes ».

Ainsi, imagine-t-on de jeunes individus vulnérables qui, exposés à des contenus numériques djihadistes, adoptent une vision du monde dite « radicale » et vont jusqu'à s'engager dans la violence politique.

Bien qu'il existe de nombreuses idéologies extrémistes, la recherche traite presque exclusivement de la radicalisation islamiste. Ce concept est « encore balbutiant, adoptant de multiples directions », mais pour autant, « il semble évident qu'internet est devenu un « espace fécond de mobilisation pour les mouvements militants extrémistes indépendamment de leur orientation idéologique et de leur situation géographique » (Ducol, 2015)p. 3).

Comment comprendre l'implication d'Internet dans la progression du terrorisme ? Quel est son impact chez les jeunes?

Une approche de terrain

Internet permet aux individus d'adopter très facilement une autre identité et de projeter une autre forme d'expression de soi, en particulier dans le cas d'affiliations identitaires idéologiquement marginales ou de croyances/opinions stigmatisées (McKenna, 2007).

Il contribue aussi à une transformation cognitive des individus en favorisant les phénomènes de « saillance identitaire » dus à l'exposition à certains contenus numériques. Il influence les mécanismes d'exposition en ligne par une sorte de « filtrage algorithmique » (Pariser, 2011) qui peut pousser certaines personnes à s'enfermer dans des visions biaisées et polarisantes du monde.

Plusieurs travaux évoquent la manière dont internet et les réseaux sociaux tendent à faciliter, plus qu'auparavant, la rencontre entre des inconnus possédant des intérêts ou des croyances marginales/déviantes communes (Lauw et al., 2010), mais qui, avant l'émergence du numérique, n'auraient sans doute pas pu interagir, ou en tout cas, plus difficilement.

Aussi, de nombreux chercheurs ont une vision instrumentaliste d'internet et de la radicalisation en ligne. Par exemple, Kiras affirme que les terroristes utilisent à leur avantage les technologies de l'information « afin de coordonner leurs actions, partager leurs informations et atteindre des auditoires auparavant inaccessibles » (Kiras, 2007a).

Il utilise d'ailleurs un vocabulaire issu des études stratégiques en expliquant que dans un conflit asymétrique traditionnel, l'état est avantagé par sa capacité à maîtriser les canaux de communication et de l'information. Mais, les nouvelles technologies de l'information brisent cette dynamique en permettant aux groupes terroristes de toucher le public par le biais de nombreux autres médias.

Dans le même ordre d'idée, il avance que la stratégie d'isolement des groupes terroristes devient obsolète avec les nouvelles technologies. En effet, il ne suffit plus de fermer les frontières pour réduire la mobilité des groupes terroristes, car avec les technologies de l'information, le message politique continue d'être diffusé auprès de la population (Kiras, 2007b). Il est donc facile d'observer qu'internet permet aux groupes terroristes de s'assurer une présence virtuelle permanente.

Pour faire face à l'émergence de contenus numériques facilitant l'organisation d'actions violentes, à l'instar de « Make a bomb in your mums kitchen » (Torok, 2010), des auteurs tentent de comprendre dans quelle mesure ceux-ci influencent le passage à l'acte du terroriste. Par exemple, il est analysé la manière dont les individus utilisent les plateformes numériques afin d'échanger des informations sur la fabrication de bombes (Weimann, 2010).

Torok et Weimann évoquent d'ailleurs à ce sujet, une problématique importante par rapport à la sécurité nationale.

Cependant, d'autres auteurs comme Holbrook (2015) estiment que la confection d'une bombe nécessite des connaissances pointues et n'est donc pas à la portée de tout le monde. Il voit une différence entre l'application théorique du concept d'apprentissage en ligne et les obstacles auxquels les individus font face en réalité. Il est intéressant de noter que les contenus numériques consultés par les terroristes ne sont pas forcément des plateformes faisant l'apologie du terrorisme. Par exemple, Holbrook (2015, p. 126), dans le cadre de ses recherches sur les terroristes, observe que les contenus souvent consultés par ces derniers sont la liste des matériaux explosifs du US Bureau of Alcohol, Tobacco, Firearms and Explosives, ainsi que la chaîne YouTube « NurdRage », spécialisée dans les expériences scientifiques en tout genre.

Aussi, on peut s'interroger sur le lien entre terrorisme et Internet.

Il est analysé (Weimann, 2008) la manière dont un groupe utilise les nouvelles technologies de l'information et de la communication comme outil tactique de guerre psychologique en diffusant, par exemple, des images de centaines d'enfants tués par des frappes israéliennes.

Il est ainsi défendu l'idée selon laquelle une guerre se gagne désormais dans les médias (télévision, Web), ce qui renvoie à une violence symbolique dont la puissance de terreur se nourrit des réseaux sociaux, notamment.

Un autre élément intéressant concerne le schéma stratégique (à long terme) mis en place lors de la construction des sites Internet par les groupes terroristes, qui correspond en tout point à une stratégie e-marketing dans le monde des affaires (Mozes & Weimann, 2010). Les auteurs suggèrent même d'alimenter une guerre psychologique dans les médias sociaux afin de contrer les idées du djihad international.

« L'arsenalisation d'Internet » (Brachman, 2006) est un autre phénomène à prendre en compte. Selon l'auteur, un groupe terroriste peut utiliser Internet à la place des camps d'entraînement djihadistes traditionnels affaiblis par les interventions américaines en Irak et en Afghanistan. Il décrit Internet comme un outil opérationnel employé par al-Qaida, et représentant un grave péril pour l'humanité. L'exemple de Haya média santé est frappant (Berger, 2015a). L'auteur explique la façon dont cet organe, qualifié comme « propagande de groupe », permet de diffuser une propagande « sur une base industrielle » (Berger, 2015b).

Un autre exemple probant est celui de l'application « The Dawn of Glad Tiding », téléchargeable sur Android et Apple Store, qui permet au responsable d'un groupe de prendre le contrôle des comptes Twitter de ses sympathisants. L'État islamique s'en est servi pour envoyer plus de 44000 tweets dans une seule journée, pendant la marche sur Mossoul, sans risque de se faire bloquer par les logiciels anti-pourriels.

Il est à noter que fin 2014, Daesh passait principalement par Twitter avec une moyenne de 72 retweets pour un tweet publié sur son compte (Grenier-Chalifoux, 2017). Notamment, la création d'une redondance sur Twitter permet de transformer un événement en fenêtre médiatique. Tel a été le cas pour la prise de Mossoul en Irak ou la Coupe du monde de la FIFA en 2014.

Le principe est simple. Par exemple, un groupe inonde de contenus djihadistes les mots-clés #Worldcup et #brazil2014, ce qui lui permet d'atteindre une audience internationale. La même tactique de communication digitale a été utilisée avec les mots-clés #Ebola en été 2014 et #jesuischarlie en janvier 2015 (Grenier-Chalifoux, 2017).

Un point de vue qui doit être modéré

D'autres auteurs estiment que l'Internet n'est pas forcément à l'origine de l'augmentation du terrorisme. Selon Benson (Benson, 2014), l'accès au Web s'est certes développé de manière substantielle, mais le nombre d'incidents terroristes internationaux n'a pas suivi cet essor. Grâce à ce média, les organisations occidentales disposent du même niveau d'information que les terroristes. Par conséquent, les États se retrouvent dans la même position vis-à-vis du terrorisme qu'avant l'arrivée d'internet

Une approche info-communicationnelle

Quel est le message des terroristes et quelle est leur stratégie de communication digitale?

Pour Bowman Grieve, un processus discret « d'engagement » se met en place (cf. note de recherche la déradicalisation, mythe ou réalité?). Des liens sociaux virtuels se forment entre les partisans, contribuant ainsi à un processus de radicalisation en ligne (Bowman Grieve, 2010, p. 33). Sivek (2013), à travers l'étude graphique de la revue numérique publiée par al-Qaida, *Inspire*, signale une interprétation étroite de l'islam ainsi que l'exploitation du registre culturel de la jeunesse occidentale afin de motiver les lecteurs à accomplir des actes de violence. Gambhir (2014), pour sa part, s'intéresse à la revue *Dabiq*. Pour l'auteur, la revue est non seulement un outil de propagande, mais aussi, et surtout, un outil tactique de guerre psychologique inscrite dans une stratégie d'influence afin d'imposer au monde la vision du califat (Gambhir, 2014).

Enfin, ces mêmes auteurs corroborent la théorie « des disséminateurs hors conflits ». Cette théorie démontre, après l'analyse de différents cas, que certains individus sont capables d'agir sur un conflit armé dans un pays en influençant la perception publique des événements à travers la diffusion de contenus numériques.

La problématique des jeunes face à internet et aux réseaux sociaux

Les médias sociaux ont un effet identitaire tant au niveau du groupe qu'au niveau individuel. Les recherches montrent en effet la présence d'un processus de « fusion identitaire » (Swann Jr & Buhrmester, 2015) par lequel l'identité de l'utilisateur se fond progressivement au profit d'une identité de groupe radicalisé. Ainsi l'individu en arrive à adopter pleinement le discours proposé par le groupe extrémiste. Cette attitude d'adoption idéologique par la sémantique groupale est d'autant plus forte chez les jeunes seul à la recherche d'attaches et qui sont donc dans une période d'influence qui les emmènerais à se laisser se séduire par le fait d'appartenir à un groupe terroriste. (Lindekilde et al., 2019)



Par exemple, en Syrie, le conflit armé, ou plus précisément sa construction sociale, se joue aussi bien au Qatar qu'au Pakistan.

Nous pouvons donc supposer qu'il en est de même pour la France.

Ducol et Campana (2015) ont étudié des sites liés aux conflits au Caucase du Nord. Ils révèlent que les réseaux qu'ils ont identifiés peuvent fortement inciter les individus à s'engager dans le terrorisme. Les auteurs reprennent un argument déjà entendu lors de l'enquête du Sénat de 2020 présidée par Mme Nathalie Delattre et conduite par la rapporteure, Jacqueline Eustache-Brinio. En effet, non seulement Internet engendre, chez certains, la volonté de devenir des djihadistes, mais surtout, il permet la diffusion de discours théologiques complexes, vulgarisés, pouvant être compris dans l'ensemble des milieux populaires (Campana & Ducol, 2015). De plus, leurs travaux démontrent que l'utilisation de la communication graphique est très répandue et efficace, car elle s'adresse à une génération de jeunes qui préfèrent les images aux textes (Klausen, 2015).

Dans le problème de la transmission par le Web, il y a également la question du prêche en arabe à l'heure des nouvelles technologies. Lors de la commission d'enquête du Sénat sus nommée en janvier 2020, de nombreux experts ont lancé ce débat. La traduction française d'un prêche en arabe ne peut pas révéler la radicalité des mots. Avec Internet, ces prêches peuvent désormais toucher un nombre considérable d'individus.

Quelle conséquence doit-on craindre pour ce nouveau type de prêche à l'ère numérique?

La problématique des jeunes face à internet et aux réseaux sociaux

Les médias sociaux ont un effet identitaire tant au niveau du groupe qu'au niveau individuel. Les recherches montrent en effet la présence d'un processus de « *fusion identitaire* » (Swann Jr & Buhrmester, 2015) par lequel l'identité de l'utilisateur se fond progressivement au profit d'une identité de groupe radicalisé. Ainsi l'individu en arrive à adopter pleinement le discours proposé par le groupe extrémiste. Cette attitude d'adoption idéologique par la sémantique groupale est d'autant plus forte chez les jeunes seuls à la recherche d'attaches et qui sont donc dans une période d'influence qui les mènerait à se laisser séduire par le fait d'appartenir à un groupe terroriste. (Lindekilde et al., 2019)

Ce processus de « fusion identitaire » trouve une explication dans le fait que la coexistence dans l'univers numérique de pléthore d'identités virtuelles peut favoriser une rupture entre l'identité de l'individu et l'adoption d'une identité de groupe. Ce phénomène a pour nom « *la désindividuation* » (Reicher et al., 1995) (Rogers et al., 2003). Cette désindividuation s'appuie surtout sur la manipulation du besoin de réunion et de rendez-vous des jeunes (extimité) pour nouer de nouveaux liens sociaux via de nouvelles rencontres virtuelles et des groupes de discussions. Au vu de la dimension affective du phénomène, il en a été constaté par une mesure un sentiment de communauté virtuel (Blanchard, 2007) ainsi qu'un « sentiment de présence » qui prend de l'ampleur dans le contexte émotionnel (Riva et al., 2007). Mais ce qui est intéressant c'est que ce sentiment de présence est plus important pour les internautes que leur réseau social hors ligne lui-même. (Courbet et al., 2015)

Enfin, de plus en plus de travaux démontrent que les réseaux sociaux qui sont fondés sur des liens émotionnels et communautaires profitent de la vulnérabilité des jeunes (Busher, 2015) et c'est la raison pour laquelle l'adhésion à ces réseaux sociaux est très souvent considérée comme une étape intermédiaire dans la radicalisation violente même si des recherches de liens de causalité restent à faire sur cette thématique pour établir le bien-fondé d'une telle affirmation

Doit-on voir un lien causal entre Internet et le passage à l'acte?

Tout d'abord, Internet joue rarement le rôle principal dans les trajectoires de radicalisation et ne constitue pas nécessairement la première exposition aux idées radicales pour les terroristes potentiels. Le site Internet entre en jeu à différents moments pour différentes personnes. Il peut renforcer des idées déjà présentes chez un individu (Ducol et al., 2016). Un sondage a été mené auprès de 6 020 jeunes Belges de 16 à 24 ans sur la corrélation entre l'adoption de comportements violents et l'exposition à des contenus numériques favorisant ces comportements.

Pour ces jeunes, ce comportement émerge lorsqu'un individu est exposé à des messages sociaux favorisant un acte criminel en le décrivant comme un apprentissage social (Pauwels & Schils, 2016). Pour ces auteurs, c'est au sein de ces communautés virtuelles que se déroule le processus de radicalisation en ligne.

Ducol (2012), dans son étude des communautés des forums djihadistes francophones, démontre que les contenus numériques djihadistes jouent un rôle dans le processus de radicalisation. Mais, il souligne également que ces sites sont consultés, dans une large majorité, sur les conseils de l'entourage physique (amis, frères...). Par exemple, dans 41 % des cas, l'utilisateur d'un tel forum a suivi la suggestion d'un autre individu dans le monde réel. La notion de bouche-à-oreille est donc essentielle.

Enfin, le rôle des femmes au sein de ces communautés virtuelles est également analysé. Le stéréotype populaire selon lequel plus un environnement est dangereux, moins les femmes y jouent un rôle important, est fortement remis en question. Certes, les hommes dominent en nombre, mais les femmes tissent des liens sociaux beaucoup plus stables, ce qui contribue à souder entre elles les communautés terroristes de l'espace virtuel (Manrique et al., 2016).

Des recherches divergentes

Les études montrent qu'internet peut effectivement être considéré comme un incubateur de radicalisation. Cependant, il est intéressant de remarquer que le fait d'être radicalisé ne mène pas forcément à une radicalisation violente, c'est-à-dire à un passage à l'acte.

D'autres auteurs, et notamment ceux de Propaganda 2.0 (Rieger et al., 2013), affirment que dans la grande majorité des cas, les individus visionnant des contenus extrémistes rejettent cette propagande. Ces contenus auraient plutôt l'effet inverse en augmentant l'animosité envers les groupes terroristes.

C'est d'ailleurs ce que développe le « slacktivism » (Manise, 2012), une théorie selon laquelle faire de l'activisme sur le terrain réduit le niveau social sur ce même terrain.

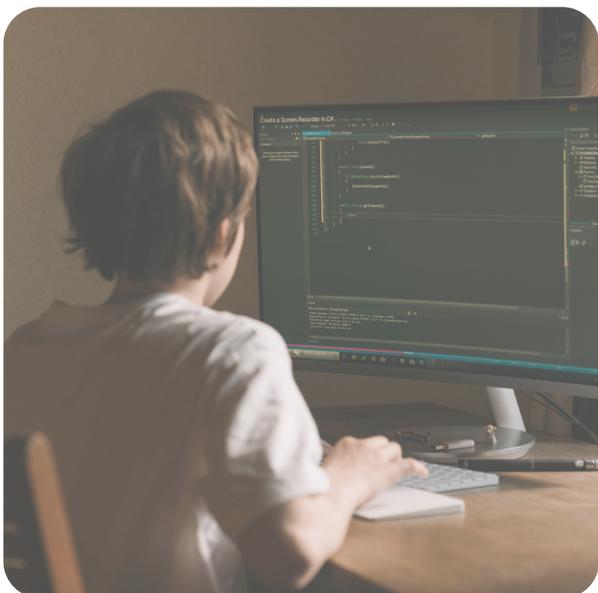
Enfin, une étude menée en 2018 sur les jeunes de 13 à 17 ans montre que les réseaux sociaux ont un impact neutre sur cette tranche. L'explication qui en ressort est le fait que nous sommes face à une génération de *digitale native*. Par conséquent leur appréhension des réseaux sociaux est maîtrisée. (Rideout & Robb, 2018)

Conclusion

Les NTIC jouent un rôle important dans l'impact symbolique du terrorisme. Cependant, il est opportun de mettre en garde contre le concept de radicalisation en ligne, qui semble discuté et discutable d'un point de vue scientifique, même si, à première vue, il paraît évident. En effet, la radicalisation ne mène pas forcément à une radicalisation violente.

Les recherches montrent clairement qu'internet et les nouvelles technologies de l'information et de la communication contribuent à l'augmentation de la radicalisation. Toutefois, il est préférable de rester prudent et d'éviter une lecture trop

« déterministe d'Internet » (Ducol, 2015). Le fait que des contenus numériques soient produits et diffusés dans l'objectif de radicaliser de recruter des individus et de faire l'apologie du terrorisme existent mais il n'est pas non plus un gage de succès... Il faut bien le comprendre, même si cette stratégie fonctionne.



PROPOSITIONS

1. Se centraliser sur la communication stratégique antiterroriste. Des experts du contre-terrorisme suggèrent de contrôler et même de réécrire les récits (narratives) diffusés par les terroristes, dans le but de contrer idéologiquement la radicalisation en ligne. Cette solution implique d'embaucher des community managers spécialisés dans le counter narrative, une forme de contre-terrorisme virtuel.

2. Commercialisation de produits idéologiques rivaux. Il faut identifier les leaders d'opinion musulmans sur les forums en ligne et les convaincre de diffuser des contre-narratifs faisant l'apologie de l'islam pacifique. Ces messages doivent provenir de la communauté musulmane, de manière subtile, pour une meilleure crédibilité du message, notamment auprès de la jeunesse.

3. Combattre l'extrémisme par l'art et la culture. Il y a par exemple la bande dessinée, la série télévisée, dont notamment Homeland.

4. Développer des évaluations plus systématiques de ces initiatives de lutte contre la radicalisation et l'extrémisme violent en ligne. Le but est de mesurer leurs effets et impacts réels. À l'instar des initiatives en ligne dans d'autres domaines d'action publique (sécurité routière, lutte contre la toxicomanie, prévention du suicide, etc.), il est essentiel de s'assurer que les dispositifs mobilisés atteignent les publics visés pour qu'ils soient efficace.

RÉFÉRENCES BIBLIOGRAPHIQUES

- Benson, D. C. (2014). Why the internet is not increasing terrorism. *Security Studies*, 23(2), 293-328.
- Berger, J. M. (2015a). The evolution of terrorist propaganda : The Paris attack and social media. The Brookings Institution.
- Berger, J. M. (2015b). The metronome of apocalyptic time : Social media as carrier wave for millenarian contagion. *Perspectives on Terrorism*, 9(4), 61-71.
- Blanchard, G. (2007). La communication politique partisane sur Internet : Des pratiques et des stratégies nouvelles?
- Bowman-Grieve, L. (2010). Irish Republicanism and the Internet : Support for new wave dissidents. *Perspectives on Terrorism*, 4(2), 22-34.
- Brachman, J. M. (2006). High-tech terror : Al-Qaeda's use of new technology. *Fletcher F. World Aff.*, 30, 149.
- Busher, J. (2015). The making of anti-Muslim protest : Grassroots activism in the English Defence League. Routledge.
- Campana, A., & Ducol, B. (2015). Voices of the "Caucasus emirate" : Mapping and analyzing north Caucasus insurgency websites. *Terrorism and Political Violence*, 27(4), 679-700.
- Courbet, D., Fourquet-Courbet, M.-P., & Marchioli, A. (2015). Les médias sociaux, régulateurs d'émotions collectives. *Hermès, La Revue*, 1, 287-292.
- Ducol, B. (2015). Devenir jihadiste à l'ère numérique : Une approche processuelle et situationnelle de l'engagement jihadiste au regard du Web. <https://corpus.ulaval.ca/jspui/handle/20.500.11794/25744>
- Ducol, B., Bouchard, M., Davies, G., Ouellet, M., & Neudecker, C. (2016). Assessment of the State of Knowledge : Connections Between Research on the Social Psychology of the Internet and Violent Extremism.
- Gambhir, H. K. (2014). Dabiq : The strategic messaging of the Islamic State. *Institute for the Study of War*, 15(4).
- Grenier-Chalifoux, W. (2017). Radicalisation hors ligne : Le rôle des réseaux sociaux dans le passage à l'acte terroriste islamiste (1990-2016).
- Kiras, J. D. (2007). Irregular warfare : Terrorism and insurgency. *Understanding modern warfare*, 224, 186-207.
- Klausen, J. (2015). Tweeting the Jihad : Social media networks of Western foreign fighters in Syria and Iraq. *Studies in Conflict & Terrorism*, 38(1), 1-22.
- Lauw, H. W., Ntoulas, A., & Kenthapadi, K. (2010). Estimating the quality of postings in the real-time web.
- Lindekilde, L., Malthaner, S., & O'Connor, F. (2019). Peripheral and embedded : Relational patterns of lone-actor terrorist radicalization. *Dynamics of Asymmetric Conflict*, 12(1), 20-41.
- Manise, J. (2012). De l'activisme numérique au militantisme de terrain.
- Manrique, P., Cao, Z., Gabriel, A., Horgan, J., Gill, P., Qi, H., Restrepo, E. M., Johnson, D., Wuchty, S., & Song, C. (2016). Women's connectivity in extreme networks. *Science advances*, 2(6), e1501742.
- Mozes, T., & Weimann, G. (2010). The e-marketing strategy of Hamas. *Studies in Conflict & Terrorism*, 33(3), 211-225.
- Pariser, E. (2011). The filter bubble : What the Internet is hiding from you. Penguin UK.
- Pauwels, L., & Schils, N. (2016). Differential online exposure to extremist content and political violence : Testing the relative strength of social learning and competing perspectives. *Terrorism and Political Violence*, 28(1), 1-29.
- Reicher, S. D., Spears, R., & Postmes, T. (1995). A social identity model of deindividuation phenomena. *European review of social psychology*, 6(1), 161-198.
- Rideout, V., & Robb, M. B. (2018). Social media, social life : Teens reveal their experiences. San Francisco, CA: Common Sense Media.
- Rieger, D., Frischlich, L., & Bente, G. (2013). Propaganda 2.0 : Psychological effects of right-wing and Islamic extremist internet videos.
- Riva, G., Mantovani, F., Capideville, C. S., Preziosa, A., Morganti, F., Villani, D., Gaggioli, A., Botella, C., & Alcañiz, M. (2007). Affective interactions using virtual reality : The link between presence and emotions. *CyberPsychology & Behavior*, 10(1), 45-56.
- Rogers, P., Lea, M., & Spears, R. (2003). Social processes in electronic team work : The central issue of identity. Swann Jr, W. B., & Buhrmester, M. D. (2015). Identity fusion. *Current Directions in Psychological Science*, 24(1), 52-57.
- Torok, R. (2010). "Make A Bomb In Your Mums Kitchen" : Cyber Recruiting And Socialisation of 'White Moors' and Home Grown Jihadists.
- Weimann, G. (2008). Hezbollah Dot Com : Hezbollah's Online Campaign. *New Media and Innovative Technologies*, 17-38.
- Weimann, G. (2010). Terror on facebook, twitter, and youtube. *The Brown Journal of World Affairs*, 16(2), 45-54.