MODULE 7

Combatting online abuse: when journalists and their sources are targeted

by Julie Posetti

Synopsis

The problem of disinformation and misinformation[196] undermining credible journalism and reliable information has escalated dramatically in the social media era. Consequences include the deliberate targeting of journalists and other online publishers, along with their sources, who are seeking to verify or share information and commentary. The associated risks can further undermine trust in journalism, along with the safety of journalists and their sources.

In some instances, journalists have been targeted in acts of 'astroturfing'[197] and 'trolling'[198] - deliberate attempts to "mislead, misinform, befuddle, or endanger journalists"[199] with the sharing of information designed to distract and misdirect them, or their potential sources. Alternatively, journalists might be targeted to trick them into sharing inaccurate information which feeds a false interpretation of the facts or, when it is revealed as fake, diminishes the credibility of the journalist (and the news organisation with which they are affiliated). In other cases, they face digital threats designed to expose their sources, breach their privacy to expose them to risk, or access their unpublished data.

There is also the phenomenon of governments mobilising 'digital hate squads' to chill critical commentary and quash freedom of expression.[200] Then, there is the serious problem of online harassment and violence (sometimes problematically labelled as 'trolling'[201]) disproportionately experienced by women and frequently misogynistic in nature. This can see journalists, their sources, and commentators subjected to torrents

196 For definitions, see: Wardle, C. & Derakhshan, H. (2017). *Information Disorder: Toward an Interdisciplinary Framework for Research and Policymaking* (Council of Europe). https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-researc/168076277c [accessed 30/03/2018].

197 'Astroturfing' is a term derived from a brand of fake grass used to carpet outdoor surfaces to create the impression it is natural grass cover. In the context of disinformation, it involves spreading fake information, targeting audiences and journalists with an intention to redirect or mislead them, particularly in the form of 'evidence' of faux popular support for a person, idea or policy. See also Technopedia definition: https://www.techopedia.com/definition/13920/astroturfing [accessed 20/03/2018].

198 Coco, G. (2012). *Why Does Nobody Know What Trolling Means? A quick reference guide for the media* at Vice.com. https://www.vice.com/en_au/article/ppqk78/what-trolling-means-definition-UK-newspapers [accessed 30/03/2018].

199 Posetti, J. (2013). *The 'Twitterisation' of investigative journalism* in S. Tanner & N. Richardson (Eds.), Journalism Research and Investigation in a Digital World (pp. 88-100): Oxford University Press, Melbourne. http://ro.uow.edu.au/cgi/viewcontent.cgi?article=2765&context=lhapapers [accessed 30/03/2018].

200 Riley M, Etter, L and Pradhan, B (2018) *A Global Guide To State-Sponsored Trolling*, Bloomberg: https://www.bloomberg.com/features/2018-government-sponsored-cyber-militia-cookbook/ [accessed 21/07/2018].

201 Note: 'Trolling' in its internet-related application refers to acts that range from gentle teasing, tricking and goading to deliberate deception. However, it is increasingly deployed as a term to cover all acts of online abuse. This is potentially problematic as it conflates a wide range of activities and potentially underplays the seriousness of online harassment.

of online abuse, false claims about their conduct, misrepresentation of their identities, or threats of harm designed to humiliate them and undermine their confidence, discredit them, divert their attention and, ultimately, to chill their reporting.[202] Meanwhile in many places, physical world abuse designed to suppress critical reporting continues, with the added danger of now being fuelled by online incitement and intimidation.

Journalists can be direct victims of disinformation campaigns, but they are also pushing back. In addition to strengthening digital defences, many are proactively exposing these attacks and uncovering the attackers. Engaging in Media and Information Literacy initiatives along with NGOs in this space, news media are also playing a role in educating the public about why journalism is worth cherishing and protecting.

Outline

Teasing out the issues

i) Recognising and Responding to 'Trolling' and 'Astroturfing'[203]

This phenomenon includes fabrication of characters and events designed to trick journalists and audiences, along with organised social media campaigns aimed at mimicking organic public reaction. It can be difficult to differentiate breaking news and legitimate witness accounts from content that has been faked or peppered with inaccuracies to deliberately mislead or undermine the credibility of journalists and other online commentators, along with their work, by duping them into sharing false information.

Examples of this kind of behaviour include:

- The fabrication of disaster victims and terrorist attack casualties (see Manchester bombings example[204]) to fool people into sharing content that potentially damages the reputation and/or credibility of individuals, including journalists, who might be tagged in the distribution process.
- The publication of content parading as newsworthy produced by fictitious characters such as the 'Gay girl in Damascus'[205]. In 2011, the world's media clamoured to report the arrest of the blogger who was purportedly a Syrian lesbian - the author turned out to be a U.S. student based outside

202 See for example: https://www.independent.co.uk/news/world/americas/twitter-maggie-haberman-new-york-times-quits-social-media-jack-dorsey-a8459121.html

203 For an explanation of 'astroturfing' useful for teaching purposes, the following link is of value: https://youtu.be/Fmh4RdlwswE

204 Manchester bombing example, https://www.theguardian.com/technology/2017/may/26/the-story-behind-the-fake-manchester-attack-victims [accessed 30/03/2018].

205 Young, K. (2017). *How to Hoax Yourself: The Case of the Gay Girl in Damascus,* November 9th, 2017, in The New Yorker. https://www.newyorker.com/books/page-turner/how-to-hoax-yourself-gay-girl-in-damascus [accessed 30/03/2018].

> the country. Journalist Jess Hill was assigned to the story for the Australian Broadcasting Corporation's *PM* programme. She says traditional verification values and methods prevented her programme from amplifying a falsehood. "We didn't report her arrest, for one simple reason – we couldn't find anyone who had actually met her in person. No relatives, no personal friends. We spent two days looking for people, asking our Syrian contacts to refer us to people who may have had contact with her, but each lead became a dead end. The fact that we couldn't find anyone who had actually met her set off major alarm bells, so we didn't report it... News agencies who rushed to report that story didn't do the basic job of going back to the source. They reported news based on an entry on a blog."[206]

Other motivations include the desire to redirect or distract journalists from an investigation by prompting fruitless lines of inquiry that stymie reporting efforts and, ultimately, have a chilling effect on truth-seeking.

Examples of this style of misdirection include:

- The attempted reframing of claims about the size of the crowd at Donald Trump's inauguration in January 2017 as 'alternative facts'[207]
- Contemporary wartime propaganda, e.g. the Taliban tweeting at journalists in Afghanistan with false and misleading details of battles.[208]
- Datasets handed to journalists that provide some verifiable public interest-value information but have been corrupted by disinformation in the mix.

More recently, computational propaganda[209] has increased the risks for journalists dealing with 'astroturfing' and 'trolling'. This involves the use of bots to disseminate well-targeted false information and propaganda messages on a scale designed to look like an organic movement.[210] Concurrently, AI technology is being leveraged to create 'deepfake'[211] videos and other forms of content designed to discredit the targets, including journalists, and especially female reporters.

---

206 Posetti, J. (2013). op cit

207 NBC News (2017) Video: https://www.nbcnews.com/meet-the-press/video/conway-press-secretary-gave-alternative-facts-860142147643 [accessed 30/03/2018].

208 Cunningham, E (2011). *In shift, Taliban embrace new media*, GlobalPost. https://www.pri.org/stories/2011-05-21/shift-taliban-embrace-new-media [accessed 30/03/2018].

209 Woolley, S. & Howard, P. (2017). *Computational Propaganda Worldwide: Executive Summary,* Working Paper No. 2017.11 (Oxford University). http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/06/Casestudies-ExecutiveSummary.pdf [accessed 30/03/2018].

210 Note: Shallow reports about bot campaigns during the 2017 UK general election highlight the difficulty of reporting on these issues. C.f. Dias, N. (2017). *Reporting on a new age of digital astroturfing,* First Draft News. https://firstdraftnews.com/digital-astroturfing/ [accessed 29/03/2018].

211 The term deepfake is a portmanteau of 'deep learning' and 'fake'. It involves AI technology in the creation of fraudulent content, sometimes of a pornographic nature, that is virtually undetectable. It is used in cyberattacks to discredit people, including journalists. See: Cuthbertson, A (2018) *What is 'deepfake' porn? AI brings face-swapping to disturbing new level* in Newsweek http://www.newsweek.com/what-deepfake-porn-ai-brings-face-swapping-disturbing-new-level-801328 [accessed 17/06/2018].

Examples of these practices include:

- Independent news site Rappler.com and its largely female staff were targeted in a campaign of prolific online abuse. "In the Philippines, paid trolls, fallacious reasoning, leaps in logic, poisoning the well – these are only some of the propaganda techniques that have helped shift public opinion on key issues."[212] (see expanded discussion below)
- A wealthy family accused of capturing key state enterprises and politicians in South Africa hired UK Public Relations firm Bell Pottinger to devise an elaborate propaganda campaign. It spread its messages via a disinformation empire involving websites, media and a paid Twitter army which targeted journalists, business people and politicians with abusive, hostile messages and photoshopped images, designed to humiliate and counter their investigations into state capture.[213] Prominent editor Ferial Haffajee was targeted in a campaign of online harassment during this period, which saw her image manipulated to create false impressions of her character, alongside deployment of the hashtag #presstitute[214]
- The case of journalist Rana Ayyub elicited a call by five United Nations special rapporteurs for the Indian government to provide protection, following the mass circulation of false information aimed to counter her critical reporting. The independent journalist had been on the receiving end of a combination of disinformation about her on social media, including 'deepfake' videos that falsely suggested she had made pornographic films, as well as direct rape and death threats[215]
- The case of Finnish journalist, Jessikka Aro, discussed under 'Digital Safety Threats and Defensive Strategies' in section ii) of this module.

Other modules in this handbook deal specifically with technical verification techniques, but it is important to enable participants to identify the malicious motivation of some online operators in the creation, distribution and targeting of journalists with disinformation and misinformation as part of a pattern of abuse.

212 Ressa, M. (2016). *Propaganda War: Weaponising the Internet*, Rappler. https://www.rappler.com/nation/148007-propaganda-war-weaponizing-internet [accessed 30/03/2018].

213 Extensive dossier on the Gupta's 'fake news empire' available at https://www.timeslive.co.za/news/south-africa/2017-09-04-the-guptas-bell-pottinger-and-the-fake-news-propaganda-machine/. [accessed 30/03/2018].

214 Haffajee, F. (2017). *Ferial Haffajee: The Gupta fake news factory and me*. HuffPost South Africa. [online] Available at: https://www.huffingtonpost.co.za/2017/06/05/ferial-haffajee-the-gupta-fake-news-factory-and-me_a_22126282/ [accessed 06/04/2018].

215 *UN experts call on India to protect journalist Rana Ayyub from online hate campaign* http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=23126&LangID=E; [accessed 17/08/2018 See also Ayyub, R. (2018). *In India, journalists face slut-shaming and rape threats*. https://www.nytimes.com/2018/05/22/opinion/india-journalists-slut-shaming-rape.html [accessed 17/06/2018].

Critical questions to add to technical methods of information verification:

1. Could there be malicious intent behind this share or tag?
2. What does the person posting the content stand to gain by sharing?
3. What could be the consequences for me/my professional credibility/a news media institution or employer if I share it?
4. Have I worked hard enough to ascertain this individual's identity/affiliations/reliability/motivations (e.g. are they seeking to seed disinformation or profit from the sale of content acquired illegally without public interest justification)?
5. Is this a human or bot?[216]
6. If you receive a 'data dump' from a purported whistleblower, should you independently verify the contents before publishing the dataset in full? Is it possible that it is peppered with disinformation and misinformation designed to deliberately mislead or discredit?

ii) Digital Safety Threats and Defensive Strategies

Journalists, human rights defenders and bloggers/social media activists are increasingly vulnerable to cyber-attacks, and their data or sources may be compromised by malicious actors including through phishing, malware attacks, and identity spoofing.[217]

An example of this practice:

Award-winning investigative journalist Jessikka Aro, who works for Finland's public broadcaster YLE, has been the target of organised 'troll' campaigns since 2014. She has experienced digital safety threats including spoofing and doxing[218], with trolls disclosing her personal contact information and spreading disinformation about her, rendering her messaging apps and inboxes full of angry messages. *"I received a phone call in which someone fired a gun. Later, someone texted me, claiming to be my dead father and told me he was 'observing' me,"* she says.[219] Aro has expressed appreciation for editors who protect journalists from threats and urged journalists to investigate and expose propaganda.

216 For example, see https://botcheck.me

217 From Technopedia: Spoofing is a fraudulent or malicious practice in which communication is sent from an unknown source disguised as a source known to the receiver. Email spoofing is the most common form of this practice. A spoofed email may also contain additional threats like Trojans or other viruses. These programmes can cause significant computer damage by triggering unexpected activities, remote access, deletion of files and more https://www.techopedia.com/definition/5398/spoofing [accessed 29/03/2018].

218 From Technopedia: Doxing is the process of retrieving, hacking and publishing other people's information such as names, addresses, phone numbers and credit card details. Doxing may be targeted toward a specific person or an organisation. There are many reasons for doxing, but one of the most popular is coercion. Doxing is a slang term that is derived from the word ".doc" because documents are often retrieved and shared. Hackers have developed different ways to dox, but one of the most common methods is by obtaining the victim's email and then uncovering the password to open their account to obtain more personal information. https://www.techopedia.com/definition/29025/doxing [accessed 29/03/2018].

219 Aro, J. 2016. *The cyberspace war: propaganda and trolling as warfare tools.* European View. Sage Journals, June 2016, Volume 15, Issue 1. http://journals.sagepub.com/doi/full/10.1007/s12290-016-0395-5 [accessed 20/07/2018].

It is therefore important for journalistic actors to be alert to the following threats:

12 key digital security threats[220]

- Targeted surveillance and mass surveillance
- Software and hardware exploits without the knowledge of the target
- Phishing attacks[221]
- Fake domain attacks
- Man-in-the-Middle (MitM) attacks[222]
- Denial of Service (DoS) attacks and Distributed Denial of Service (DDOS – Distributed Denial of Service)[223]
- Website defacement
- Compromised user accounts
- Intimidation, harassment and forced exposure of online networks
- Disinformation and smear campaigns
- Confiscation of journalistic work product, and
- Data storage and mining

For defensive strategies see: *Building Digital Safety for Journalism*.[224]

For the implications for confidential sources and whistleblowers interacting with journalists and other media producers see: *Protecting Journalism Sources in the Digital Age*.[225]

Recognising and managing online harassment and violence

"I've been called a dirty whore, a bloody Gypsy, Jewish, a Muslim slut, a Greek parasite, a disgusting migrant, a stupid psycho, an ugly liar, a biased hater. They keep telling me to go home, to kill myself or they will shoot me, cut my tongue off, break my fingers

220 Posetti, J. (2015). New Study: *Combatting the rising threats to journalists' digital safety* (WAN-IFRA). https://blog.wan-ifra.org/2015/03/27/new-study-combatting-the-rising-threats-to-journalists-digital-safety [accessed 30/03/2018].

221 King, G (2014) *Spear phishing attacks underscore necessity of digital vigilance*, CPJ. https://cpj.org/blog/2014/11/spear-phishing-attacks-underscore-necessity-of-dig.php [accessed 29/03/2018].

222 Technopedia definition of Man in the Middle Attack (MITM): "A form of eavesdropping where communication between two users is monitored and modified by an unauthorised party. Generally, the attacker actively eavesdrops by intercepting a public key message exchange and retransmits the message while replacing the requested key with his own". https://www.techopedia.com/definition/4018/man-in-the-middle-attack-mitm [accessed 29/03/2018].

223 See definitions at Technopedia. https://www.techopedia.com/definition/24841/denial-of-service-attack-dos b. https://www.techopedia.com/definition/10261/distributed-denial-of-service-ddos [accessed 29/03/2018].

224 Henrichsen, J. et al. (2015). *Building Digital Safety for Journalism* (UNESCO) Paris. http://unesdoc.unesco.org/images/0023/002323/232358e.pdf [accessed 30/03/2018].

225 Posetti, J. (2017). *Protecting Journalism Sources in the Digital Age* (UNESCO). Paris. http://unesdoc.unesco.org/images/0024/002480/248054E.pdf [accessed 30/03/2018].

one by one. They keep threatening me with gang rapes and sexual torture."[226] These are the words of celebrated Swedish journalist Alexandra Pascalidou, who testified in 2016 before a European Commission session in Brussels about her experiences online.

The global proliferation of this kind of online abuse targeting women journalists and commentators has led to the UN (including UNESCO[227]) and other agencies recognising the problem, and calling for actions and solutions.

The Organisation for Security and Co-operation in Europe (OSCE) has sponsored research that demonstrates the international impact of online abuse of female journalists who are disproportionately targeted for 'hate trolling'. [228]

That research followed a study by British think tank, Demos, which examined hundreds of thousands of tweets and found journalism was the only category where women received more abuse than men, "with female journalists and TV news presenters receiving roughly three times as much abuse[229] as their male counterparts". The keywords for the abusers were «slut», «rape» and «whore».

A hallmark of this online abuse of female journalistic actors is the use of disinformation tactics – lies are spread about their character or their work as a means of undermining their credibility, humiliating them, and seeking to chill their public commentary and reporting.

The addition of threats of violence, including rape and murder, and the 'pile on' effect (organic, organised, or robotic mass attacks against a person online) worsen the impacts.

The intimate nature of these attacks, often received on personal devices first thing in the morning and last thing at night, further sharpens the impact. "There are days when I wake up to verbal violence and fall asleep with sexist and racist rage echoing in my ears. It's like a low-intense, constant warfare", Pascalidou says.

In the Philippines, *Rappler* CEO and Executive Editor, Maria Ressa[230], is a case study in combatting prolific online harassment in the context of a massive disinformation campaign with links to the State. She is a former *CNN* war correspondent but she says none of her experiences in the field prepared her for the massive and destructive campaign of gendered online harassment that has been directed at her since 2016.

---

226 Posetti, J. (2016). *Swedish journalist Alexandra Pascalidou Describes Online Threats of Sexual Torture and Graphic Abuse* in The Sydney Morning Herald, 24/11/2016. http://www.smh.com.au/lifestyle/news-and-views/swedish-broadcaster-alexandra-pascalidou-describes-online-threats-of-sexual-torture-and-graphic-abuse-20161124-gswuwv.html [accessed 30/03/2018].

227 Posetti, J. (2017). *Fighting Back Against Prolific Online Harassment: Maria Ressa* in L. Kilman (Ed) op cit See also: Resolution 39 of UNESCO's 39th General Conference which notes "the specific threats faced by women journalists including sexual harassment and violence, both online and offline." http://unesdoc.unesco.org/images/0026/002608/260889e.pdf [accessed 29/03/2018].

228 OSCE (2016). *Countering Online Abuse of Female Journalists*. http://www.osce.org/fom/220411?download=true [accessed 30/03/2018].

229 Bartlett, J. et al. (2014) *Misogyny on Twitter*, Demos. https://www.demos.co.uk/files/MISOGYNY_ON_TWITTER.pdf [accessed 30/03/2018].

230 Maria Ressa is chair of the jury of the UNESCO-Guillermo Cano World Press Freedom Prize https://en.unesco.org/prizes/guillermo-cano/jury.

"I've been called ugly, a dog, a snake, threatened with rape and murder," she says. Ressa has lost count of the number of times she has received death threats. In addition, she has been the subject of hashtag campaigns like #ArrestMariaRessa and #BringHerToTheSenate, designed to whip-up online mobs into attack mode, discredit both Ressa and Rappler, and chill their reporting. "It began a spiral of silence. Anyone who was critical or asked questions about extrajudicial killings was attacked, brutally attacked. The women got it worst. And we've realised that the system is set up to silence dissent - designed to make journalists docile. We're not supposed to be asking hard questions, and we're certainly not supposed to be critical," Ressa says.[231]

Maria Ressa's fightback strategy includes:

- Recognising the seriousness of the problem
- Recognising the psychological impacts and facilitating psychological support for affected staff
- Using investigative journalism as a weapon in the fightback[232]
- Asking loyal audiences to help repel and contain attacks
- Tightening security on and offline in response to harassment
- Publicly calling on platforms (e.g. Facebook and Twitter) to do more to curtail and adequately manage online harassment

While dealing with the rising threat of online harassment, it is also important to acknowledge ongoing offline harassment of women journalists in the context of disinformation campaigns. For example, Australian investigative journalist Wendy Carlisle was abused, heckled and jostled during a climate change denialists' rally in Australia in 2011 while making a documentary for ABC Radio. The abuse led her to leave the event to ensure her safety.[233]

Module Aims

This module will: inform participants about the risks of online abuse in the context of 'information disorder'; help participants to recognise threats; and provide skills development and tools to assist in combatting online abuse. The aims are:

231 Posetti, J. (2017). *Fighting Back Against Prolific Online Harassment: Maria Ressa* in Kilman, L. (Ed) An Attack on One is an Attack on All (UNESCO). http://unesdoc.unesco.org/images/0025/002593/259399e.pdf [accessed 30/03/2018].

232 This was also a tactic deployed by Ferial Haffajee in the 'Gupta leaks' case study referenced earlier. She used investigative journalism techniques and digital security 'detectives' to unmask some of the trolls who had been targeting her in an effort to discredit her reporting of the scandal. See: https://www.news24.com/SouthAfrica/News/fake-news-peddlers-can-be-traced-hawks-20170123 [accessed 16/06/2018].

233 Carlisle, W. (2011). *The Lord Monckton Roadshow*, Background Briefing, ABC Radio National. http://www.abc.net.au/radionational/programs/backgroundbriefing/the-lord-monckton-roadshow/2923400 [accessed 30/03/2018].

- To increase participants' awareness of the problem of malicious actors targeting journalists, their sources, and other online communicators in disinformation/misinformation campaigns;
- To enable participants to better recognise 'astroturfing', 'trolling', digital safety threats, and online abuse,
- To equip participants to be better prepared to combat 'astroturfing' and 'trolling', digital safety threats, and online abuse in a gender sensitive manner.

Learning Outcomes

By the end of this module, participants will:

1. Have a deeper understanding of the impacts of online abuse on journalistic actors, journalism, information sharing, and freedom of expression;
2. Be more aware of the problem of malicious actors targeting journalists and other online communicators in disinformation/misinformation campaigns;
3. Understand the particular safety threats confronting women doing acts of journalism online;
4. Be able to more easily recognise malicious actors online, along with incidents of 'astroturfing', 'trolling', digital safety threats, and online abuse;
5. Be better equipped to combat 'astroturfing', 'trolling', digital safety threats, and online abuse in a gender sensitive manner.

Module Format

This module is designed to be delivered face-to-face or online. It is intended for execution in two parts: Theoretical and practical.

Linking Plan to Learning Outcomes

A. Theoretical

Module Plan	Number of hours	Learning Outcomes
An interactive lecture and Q&A (90 minutes), which could be delivered traditionally, or via a webinar platform, designed to encourage remote participation. Lecture content can be drawn from the theory and examples supplied above. However, course convenors are encouraged to also include culturally/locally relevant case studies in the delivery of this module.	60 - 90 mins	1, 2, 3, 4, 5

B. Practical

Module Plan	Number of hours	Learning Outcomes
A workshop/tutorial (90 minutes) which could be facilitated in a traditional classroom setting, or via an eLearning platform like Moodle, Facebook groups or other services that enable remote online participation. The workshop/tutorial exercise could adopt the following format: • Divide tutorials into working groups of 3-5 participants each • Each working group is to be provided with an example of malicious content (Search blogs and social media channels for content created to target Maria Ressa, Jessikka Aro, and Alexandra Pascalidou, for example, whose cases are discussed in this module) connected to a dis/misinformation/trolling/astroturfing/online abuse campaign. • Each working group must: collaboratively assess the material (research the individual/group behind the material); identify risks and threats (referring to relevant research about impacts contained in recommended readings); propose a plan of action for responding to the material (this could include replying strategically, reporting the user to the platform or police if appropriate, assigning a story on the issue); write a 250 word summary of their plan of action (using Google Docs or a similar collaborative editing tool) and submit to their lecturer/tutor for review	90 - 120 mins	1, 2, 3, 4, 5

Alternative structure

For deeper treatment of the issues, this module could be expanded to run as three separate lessons (each delivered in two parts, as described above):

- Recognising and responding to 'trolling' and 'astroturfing'
- Digital threat-modelling[234] and defensive strategies
- Recognising and managing gendered online harassment and violence

234 Stray, J. (2014). *Security for journalists, Part Two: Threat Modelling*. https://source.opennews.org/articles/security-journalists-part-two-threat-modeling/ [accessed 2/03/2018].

Suggested Assignment

Write a 1200-word feature story, or produce a five-minute audio report, a three-minute video report, or a detailed interactive infographic based on an interview with one or more journalists about experiences of online abuse (e.g. being targeted with disinformation and/or facing digital security threats as part of a disinformation campaign and/or harassed or subjected to online violence). Participants should cite reputable research as part of their feature and explain the implications of the impacts of these phenomena for journalism/freedom of expression and the public's right to know.

Reading

Aro, J. 2016. *The cyberspace war: propaganda and trolling as warfare tools*. European View. Sage Journals, June 2016, Volume 15, Issue 1. http://journals.sagepub.com/doi/full/10.1007/s12290-016-0395-5 [accessed 20/07/2018].

Haffajee, F. (2017). *The Gupta Fake News Factory and Me* in The Huffington Post. http://www.huffingtonpost.co.za/2017/06/05/ferial-haffajee-the-gupta-fake-news-factory-and-me_a_22126282/ [accessed 29/03/2018].

OSCE (2016). *Countering Online Abuse of Female Journalists*. http://www.osce.org/fom/220411?download=true [accessed 29/03/2018].

Posetti, J. (2017). *Fighting Back Against Prolific Online Harassment: Maria Ressa* in L. Kilman (Ed) An Attack on One is an Attack on All (UNESCO 2017). http://unesdoc.unesco.org/images/0025/002593/259399e.pdf [accessed 29/03/2018].

Posetti, J. (2016). *Swedish journalist Alexandra Pascalidou Describes Online Threats of Sexual Torture and Graphic Abuse* in The Sydney Morning Herald, 24/11/2016. http://www.smh.com.au/lifestyle/news-and-views/swedish-broadcaster-alexandra-pascalidou-describes-online-threats-of-sexual-torture-and-graphic-abuse-20161124-gswuwv.html [accessed 29/03/2018].

Reporters Sans Frontieres (2018) *Online Harassment of Journalists: Attack of the trolls* Reporters Without Borders: https://rsf.org/sites/default/files/rsf_report_on_online_harassment.pdf [accessed 20/8/18].

Riley M, Etter, L and Pradhan, B (2018) *A Global Guide To State-Sponsored Trolling*, Bloomberg: https://www.bloomberg.com/features/2018-government-sponsored-cyber-militia-cookbook/ [accessed 21/07/2018].

Stray, J. (2014). *Security for journalists, Part Two: Threat Modelling*. https://source.opennews.org/articles/security-journalists-part-two-threat-modeling/ [accessed 02/03/2018].

Online resources

VIDEO: *How to Tackle Trolls and Manage Online Harassment* – a panel discussion at the International Journalism Festival, Perugia, Italy (April 2017) with Julie Posetti (Fairfax Media), Hannah Storm (International News Safety Institute), Alexandra Pascalidou (Swedish journalist), Mary Hamilton (*The Guardian*), Blathnaid Healy (CNNi). Available at: http://media.journalismfestival.com/programme/2017/managing-gendered-online-harrassment