

SOMMAIRE Introduction 3 5 1. Online harassment, a disinformation strategy 5 Mexico: "troll gangs" seize control of the news 6 In India, Narendra Modi's "yoddhas" attack journalists online 7 Targeting investigative reporters and women Censorship, self-censorship, disconnecting and exile 10 2. Hate amplified by the Internet's virality 13 13 Censorship bots like "synchronized censorship" Troll behaviour facilitated by filter bubbles 14 3. Harassment in full force 19 19 Crowd psychology 3.0: "Anyone can be a troll" Companies behind the attacks 20 Terrorist groups conducting online harassment 20 The World Press Freedom Index's best-ranked countries 20 hit by online harassment 21 Journalists: victims of social network polarization 4. Troll armies: threats and propaganda 22 Russia: troll factory web brigades 22 24 China: "little pink thumbs," the new Red Guards 25 Turkey: "AK trolls" continue the purge online 26 Algeria: online mercenaries dominate popular Facebook pages 97 Iran: the Islamic Republic's virtual militias Egypt: "Sisified" media attack online journalists 28 28 Vietnam: 10,000 "cyber-inspectors" to hunt down dissidents 29 Thailand: jobs for students as government "cyber scouts" Sub-Saharan Africa: persecution moves online 29 5. RSF's 25 recommendations 30 **Tutorial** 33 35 Glossary

INTRODUCTION

In a new report entitled "Online harassment of journalists: the trolls attack," Reporters Without Borders (RSF) sheds light on the latest danger for journalists – threats and insults on social networks that are designed to intimidate them into silence. The sources of these threats and insults may be ordinary "trolls" (individuals or communities of individuals hiding behind their screens) or armies of online mercenaries. Harassing journalists has never been as easy as it is now. Freedom of expression and bots are being used to curtail the freedom to inform.

With the help of its 12 bureaux and sections and its worldwide network of correspondents, RSF has documented dozens of cases in 32 countries for the last six months and has for the first time classified the types of online harassment. RSF has interviewed experts in cyber-crime, newsroom editors, lawyers and, above all, journalists themselves - some of whom have been terrified by the torrents of online abuse to a scale they had never imagined possible.

The links between the masterminds and the trolls who carry out the cyberviolence against journalists are often hard to demonstrate. More research needs to be done. One thing is nonetheless clear: this phenomenon is spreading throughout the world. How should we respond to these virulent online campaigns that often have dramatic consequences? RSF offers recommendations for governments, international organizations, online platforms, media companies, and advertisers.



""'Presstitute, fuck you!'... Once or twice, you can take it.

But when you're told that hundreds of times,
it inevitably has an impact on your morale"

A JOURNALIST

"The print issue journalist was shocked by so many insults over an ordinary article. For him, it was an explosion of hate. But for us it was just another day"

A WEBSITE JOURNALIST AT A NATIONAL FRENCH RADIO STATION

"For a long time, I told myself: it's the price you have to pay. But that doesn't mean it has to go unpunished"

A COLUMBIAN JOURNALIST WHO WAS THE VICTIM OF HARASSMENT

"At a certain moment, you feel you're being run over by a steamroller"

 ${\sf A}{\sf N}$ EDITOR

"Those who say it's not a big deal, that it's just threat, have never experienced it"

AN EDITOR AT A MEDIA OUTLET WHERE JOURNALISTS ARE HARASSED

"Lots of journalists watch what's being posted on Twitter but don't dare post anything themselves because they're scared of the backlash"

 ${\sf A}$ SOCIAL MEDIA EDITOR IN A NEWSROOM

"Nothing is ever just virtual"

A WOMAN JOURNALIST TARGETED BY ONLINE HARASSMENT





ONLINE HARASSMENT, A DISINFORMATION STRATEGY

MEXICO: "TROLL GANGS" SEIZE CONTROL OF THE NEWS

Of countries not at war, Mexico is the deadliest for journalists. Eleven journalists were killed in Mexico in 2017. It is also a country where online disinformation campaigns using fake accounts and bots – programs that automatically generate posts – have reached an unprecedented level. Social networks are the new battlefield of election campaigns including, most recently, the campaign for the July 2018 elections for president, deputies and senators (and governors in some states). Troll gangs have waged battles using mass postings in support of one candidate or another with the aim of making their name a trending topic on Twitter. The virtual applause from bots and fake posts threatens the integrity of the public debate by drowning journalistic content and creating a content asymmetry. It has become increasingly difficult for Mexicans to distinguish journalistic content from promotional or manipulated content in a country where an estimated 18% of Twitter content is created by bots.

The harm caused by these troll gangs does not stop at Mexico's borders. Alberto Escorcia, a Mexican investigative journalist who has specialized in covering automated online propaganda, discovered that online accounts based in Mexico were used to try to influence the October 2017 independence referendum in Catalonia, Spain, where heightened political polarization resulted in a great deal of harassment of journalists. "These fake accounts were used to promote content opposing Catalan independence and to disseminate content from the Russian news site RT," Escorcia told RSF. It was like spam, but it was sent on a massive scale with the aim of influencing its readers during a referendum.

The dormant accounts of Mexican troll gangs have been reactivated to provide politicians with virtual applause in both Mexico and Europe.

Crédit: RSF.

Dormant accounts reactivated during political campaigns

"It's not just two or three accounts spreading a rumour, it's technocensorship," Escorcia said. Raids are orchestrated on a large scale and are sometimes organized to target and attack journalists. On his site, LoQueSigue, Escorcia revealed that an army of 75,000 bots obstructed the protests about the disappearance of 43 students in Ayotzinapa in the state of Guerrero in 2014. After being left dormant,



these accounts were reactivated during Alfredo de Mazo's campaign to be elected governor in the state of Mexico. As a result of these discoveries, Escorcia received repeated death threats which eventually drove him to flee the country for a time.



A death threat against a Mexican journalist on Twitter.

IN INDIA, NARENDRA MODI'S "YODDHAS" ATTACK JOURNALISTS ONLINE

Disinformation orchestrated from the highest level is a global phenomenon found in authoritarian regimes, but also in certain countries where democracy is crumbling. In India, trolls who have been dubbed "yoddhas" by Prime Minister Narendra Modi threaten and insult journalists and flaunt their hostility towards women, minorities, and untouchables. Calling themselves "Proud Hindu," "Bharat mata Ki Jai" ("Long Live our Mother India") or "Desh Bhakt" (Patriot"), they post pictures of Hindu divinities or Modi in their profile photos on social networks.

Sadhavi Khosla, a young businesswoman, decided to work for Narendra Modi's campaign in 2013. Arvind Gupta, who at that time ran the IT unit at Modi's Hindu nationalist Bharatiya Janata Party (BJP), received her in his office "surrounded by large screens displaying data about social network activities and trends in real time." He gave her a "hit list" of journalists to target. For nearly a year, including several months after Modi's election victory, she spent her days on social networks relaying harassment messages in accordance with the party's orders. All this was exposed in <code>I am a Troll</code>, a best-seller by Indian journalist Swati Chaturvedi that described how the authorities use social networks to circumvent the media.

Modi, who was elected with the help of well-organized online activists, is often asked why he follows the social network accounts of those who insult journalists online, but he refuses to discuss the issue. In 2015, he even went so far as to invite 150 of these account holders to a meeting organized by the BJP's technology department, which personally selected the "yoddhas." The next day, most of these online assailants posted photos of themselves with Modi.

Gujarat Files author Rana Ayyub: "I've been called a prostitute, escort girl and ISIS sex slave."

"I've been called Jihadi Jane, Islamo fascist, ISIS sex slave, porkistani [a play on pork and Pakistani]," says freelance journalist Rana Ayyub. "My face has been superimposed on a naked body and my mother's photograph has been taken from my Instagram account and photoshopped in the most objectionable manner possible." Ayyub is often targeted by trolls for criticizing Narendra Modi's nationalist discourse in her book Gujarat Files: Anatomy of a cover up. Defying the self-censorship that undermines journalism in India, she has also shed light on the anti-Sikh violence of 1984 and the massacre of Muslims in 2002.



A new torrent of hate speech was unleashed against Ayyub in April of this year after a tweet falsely quoted her as having defended the perpetrators of the gangrape of a child and as having accused the Hindu nationalist government of using the case to persecute Muslims. "I couldn't sleep for three nights, I couldn't talk," she told RSF. "The trolls posted my phone number, the address of my house online. If this is the depth of their hatred, what will stop them from coming into my house as a mob and kill me?" A Facebook post left little doubt about the source of the campaign: "Look, Rana Ayyub, what they've spread about you. Don't ever dare to speak about Hindus and Modi again." RSF asked the government and New Delhi police to do everything possible to protect Ayyub, who was nominated for the RSF Press Freedom Prize in 2017.

Rana Ayyub.
© Chandan Khanna / AFP

TARGETING INVESTIGATIVE REPORTERS AND WOMEN

Being targeted by hate speech after the publication of an article is now routine for many journalists. "It used to be the news organizations that were attacked but now it is the journalists themselves as individuals," the editor of a French media outlet told RSF.

In April 2017, the Council of Europe published a survey of harassment against journalists in its 47 member countries. Of the 940 journalists polled, 40% said they had been subjected to forms of harassment that had "affected their personal life" in the previous three years. Of these cases, 53% consisted of cyberharassment.

"Women who talk too much should be raped." Online threat received by a woman journalist.¹

^{1.} https://www.osce.org/fom/220411?download=true

Investigative journalists whose reporting aggravates authoritarian regimes or political or criminal groups are the most likely to be targeted. During the Panama Papers revelations in April 2016, then Ecuadorean President Rafael Correa named five Ecuadorean journalists who had participated in the research, accusing them of bias for exposing information involving government associates. These journalists were then targeted by a harassment campaign on social networks. One of them, Katherine Pennacchio, was insulted and a smear campaign was launched against her. Her attackers criticized the fact that she had revealed that a Protestant pastor's church was linked to the Panama Papers scandal.

A report entitled "Women's rights: Forbidden subject" that RSF published in March 2018 highlighted the fact that women journalists are also one of the leading targets of trolls. In a study of thousands of tweets, the British think-tank Demos found that journalism was one of the categories in which women



received more insults than men. "Slut," "rape" and "whore" were among the insulting words most frequently used. Danielle Keats Citron, a law professor at the University of Maryland, says that in gender-based cyberharassment, the "victims are women" and, in the case of women journalists, "the threats are sexual and degrading." The aggression includes sending explicit photos, questionable "jokes," misogynistic comments, the use of nicknames, and doctored photos. Non-consensual pornography is used as a tool to intimidate women journalists.

The International Women's Media Foundation reported in 2013 that two thirds of the women journalists polled in <u>an international survey</u> said they had been the victims of harassment. A quarter of the victims said the harassment was online. This gender-based online violence is often accompanied by racist threats.



Laura Kuenssberg, the first woman journalist to be appointed as BBC News political editor, was assigned a bodyguard in September 2017 – not because she was going to a war zone or hotspot but because she was going to cover the Labour Party congress. Labour Party supporters had been accusing her of political bias in her reporting ever since the May 2016 local elections. They even started a petition for her dismissal that got 35,000 signatures. But the criticism had in some cases been accompanied by threats and verbal abuse, mainly online.

Laura Kuenssberg, Political Editor of BBC News.

© Justin Tallis / AFP



In Pakistan, 68% of journalists have been harassed online. Women activists and feminists are trolled and branded as agents of the West. The activist Nighat Dad is one of the leading campaigners against online harassment. "I've seen blackmail, photoshopped pictures, hacking of personal accounts and rape threats," she said. In 2012, she created the Digital Rights Foundation to help Pakistani women to cope with online harassment.

Khadija Ismayilova, an Azerbaijani investigative journalist who was on RSF's 2014 list of "information heroes," is well known for covering corruption and campaigning against it. In an attempt to silence her, her enemies went so far as to conceal cameras inside her home and managed to film her in her private life. The resulting videos were then used to blackmail her: if she did not refrain from further investigative reporting, they would be released. She courageously refused and the videos were posted online. In December 2014, she was arrested and sentenced to seven and a half years in prison on trumped-up charges. After a campaign led by international organizations including RSF, she was finally released in May 2016 but remains under close surveillance and is banned from travelling abroad.



Khadija Ismayilova © : Wikimedia commons.

Nothing had prepared Philippine journalist Maria Ressa, the editor of the independent news website Rappler, for such a flood of online abuse. "I've been called ugly, a dog, a snake, threatened with rape and murder," she said. Since Rodrigo Duterte's election as president in 2016, Philippine journalists are constantly targeted if, like her, they do any investigative reporting about the government. The online threats echo the government's frequent harassment of Rappler, which is backed by RSF.



"Those who say they're not real threats have not experienced them" A journalist victim of online harassment.

Maria Ressa, CEO of Rappler.

© Noel Celis / AFP

CENSORSHIP, SELF-CENSORSHIP, DISCONNECTING AND EXILE

The impact of online harassment on journalists is psychological. "It's no good having a thick skin because at a certain moment it cracks," said Pascal Wallart, La Voix du Nord's bureau chief in Hénin-Beaumont, a French town run by the far-right National Front party. "You feel crushed by their desire to destroy other people."

A French guide to combatting sexist cyberviolence says: "Virality [...] adds to the violence suffered by victims, the feeling of humiliation and distress. The violence is reinforced by the overlapping of 'online' and 'offline,' allowing the victim no respite." This also applies to journalists.

According to a 2014 <u>survey by the Pew Research Center in the United States</u>, around 40% of adult internet users who had been harassed online decided to respond to their harassers, but only half of them responded actively by blocking the harassers or sending them a message. Many journalists choose to ignore hate messages. "I don't read this kind of message, I delete them immediately," Novaya Gazeta journalist Elena Milashina said. Others disconnect temporarily during a smear campaign. "For the sake of my mental health, and so as not to waste any more time (...) I have stayed away from social networks for a few days, but I will go back, of course," said Beatriz Navarro, La Vanguardia's correspondent in Brussels.

"I talk less about socially taboo subjects (...) you have to be strategic if you don't want to be forced into exile."



Some of the journalists who spoke to RSF decided to decrease visibility online and censor themselves after being the target of online harassment. Abdou Semmar, an Algerian journalist who received online threats, some threatening his sister with rape, said: "These online attacks affected my family life (...) I've reduced my presence on social networks, I no longer talk about gays, and I talk less about socially taboo subjects in order not to give any weapons to my enemies. It's unfortunate but you have to be strategic if you don't want to be forced into exile."

Journalists are sometimes driven to flee abroad. For many journalists, some of them assisted by RSF, the only option is to change profession or go into exile. David Thomson, a journalist who received many online death threats while covering Jihadi networks in France, had to flee to the United States in 2017.

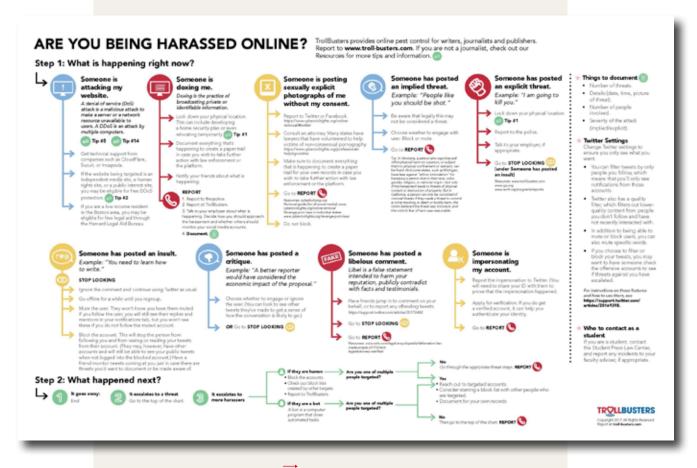
According to a Council of Europe study published in April 2017, 31% of journalists tone down their coverage of certain stories after being harassed, 15% drop the story, 23% don't cover certain stories and 57% do not report that they have been the targets of online violence.

Seeing online violence against other journalists also has a deterrent effect. Even journalists who have never been harassed may be dissuaded from covering sensitive subjects or from posting too often on social networks. The harassers send a message to all journalists, not just their victims. News organization are now starting to take stock of the scale of the online violence against their staff, but freelance journalists are particularly isolated and therefore more exposed to pressure.

Well-wishing troll community v. hate-filled troll armies

"Some journalism colleagues considered hate mail a badge of honour", said Michelle Ferrier, a Florida-based former reporter and columnist who received hate mail containing threats to herself and her children in the 2000s. A decade later, she came up with the idea of creating TrollBusters to combat online harassment. One of the services TrollBusters provides is a community of well-wishing Internet users ready to "respond" to the trolls and return the hashtags with a wave of positive messages that create a protective bubble around the targeted journalist.

Mobilizing a community of ambassadors ready to defend journalists is a method often used by the victims of online harassment. When Maria Ressa, the editor of the Philippine website *Rappler*, was threatened with murder and rape in online attacks she asked her community to help identify her harasser, who was using a Facebook account with a false name. A 22-year-old student was eventually identified and, after his university was informed, he was made to call her and apologize. The <u>resources offered by TrollBusters</u> include a step-by-step flow chart explaining what to do when you are harassed. The Tactical Technology Collective also has <u>a website with resources for women</u> who are the victims of cyberharassment. These are helpful and necessary initiatives but more are needed.



"Are you harassed online?"
A resource proposed by TrollBusters.

HATE AMPLIFIED BY THE INTERNET'S VIRALITY

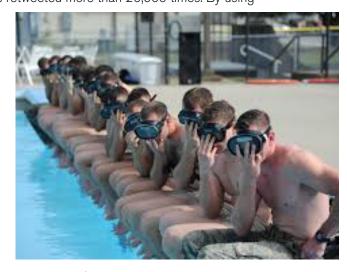
The impact of online harassment can be dramatic because new technologies are manipulated to amplify hateful messages. Artificial intelligence is used to nefarious ends. Bots automate censorship. And social networks provide press freedom's enemies with an unprecedented echo chamber for magnifying hate speech and disinformation.

CENSORSHIP BOTS LIKE "SYNCHRONIZED CENSORSHIP"

"When Bots Tweet" is the title of an article by University of South Carolina researcher Nathalie Marechal about bot activity on social networks. Imperva Incapsula, a company that provides website security services, estimates that bots were responsible for 51.2% of all Internet traffic in 2016. Some bots organize and deliver content. Other bots, the malicious ones (which steal content, for example), have accounted for most bot activity since 2013. Governments often use them against their opponents and independent observers, including journalists. Thousands of fake accounts and fake profiles can be deployed at a click. Algorithms are programmed to react to certain keywords.

Investigative journalists with the New York-based non-profit media outlet *ProPublica*, who have been the victims of online harassment, said: "We learned a sobering lesson about how easy and inexpensive it is for haters to disrupt our work." In an article entitled "The Low Cost of Internet Harassment". ProPublica's reporter Julia Angwin said the tweeted insults received by her colleagues had been coordinated: "They tweeted in formation, like synchronized swimmers." One tweet accusing ProPublica's journalists of being "presstitutes" was retweeted more than 20,000 times. By using

bots, attacks can be multiplied many times over. "Sometimes it can be smartphone factories," Louvain-based academic Nicolas Vanderbiest said. "Smartphones connected among themselves that send the same message, but adding to the complexity." Against a backdrop of polarization, the false information spread by bots is then read and shared by real activists. This is a winning formula in **astroturfing.**



Synchronized swimmers. Online attacks against journalists are synchronized.

© DR

Troll-sellers - enemies of the freedom to inform online

Companies that make <u>money from selling social network followers and retweets</u> to individuals or organizations are <u>partly to blame</u>. One of these firms, Followers and Likes, did not hesitate to sell retweets to *ProPublica*'s undercover reporters, who had created two fake Twitter accounts. The reporters were able to buy 10,000 retweets for their fake pro-Russian account for just 45 dollars and 5,000 retweets for 28 dollars for their fake English-language account.

Some firms that sell followers declined to sell to the ProPublica reporters but those that did included Devumi. These companies also assist with **"email bombing,"** another form of harassment in which the target's email address is registered as a subscriber to thousands of online services -- often porn sites -- in order to flood their inbox. Some vendors charge only <u>5 dollars for 1,000 registration emails</u>. Attacking online can be simple and cheap, say *ProPublica*'s journalists, who were themselves the targets of online harassment after writing about trolls. In RSF's view, online platforms must do more to combat such automated censorship, which <u>restricts the freedom to inform</u>.

"Social networks have become a battlefield." A journalist

TROLL BEHAVIOUR FACILITATED BY FILTER BUBBLES



On social networks, we share, like, and comment on content that reinforces our beliefs, often to the point of retreating into filter bubbles.

Online harassment is devastating because the trolls writing the hate messages have an advantage over the journalists they target – virality. The threats, insults, and false information act as clickbait, creating outrage for those living within what the Internet activist Eli Pariser calls "filter bubbles." The French sociologist Gérald Bronner, the author of Democracy of the Credulous, says: "We all have a tendency to go look for content that conforms to our ideological compulsions. This form of intellectual comfort ensures that our beliefs endure." According to the Massachusetts Institute of Technology, fake news spreads six times faster online than real news. Content distribution algorithms reward troll behaviour.

The new rules of the game push journalists – whose stories are drowned in social network newsfeeds, as RSF has condemned – to make themselves more visible online, where the frontier between private and professional life is becoming ever more porous. Journalists will resort to using their personal accounts to increase their visibility. The harassers then exploit the personal data gleaned online to hijack the accounts of these journalists in order to discredit them.

Hard for journalists to abandon social networks

Although social networks are a minefield, journalists cannot abandon them because they have become essential for their work. When the PR company Cision polled 357 French journalists, it found that 94% of them use social networks, especially Facebook and Twitter, in the course of their work.

Of these, 77% use them for posting or promoting their content, 73% for following other media or their favourite websites, and 70% for interacting with their readers, listeners, or viewers. Their presence on social networks makes them more exposed to online harassment, but they cannot imagine doing without social networks even when they are overrun by trolls waiting to pounce. "We embrace the challenge, but it's a new one," a newsroom editor said. Many journalists criticize Facebook and Twitter for not doing what it necessary to effectively combat online harassment of journalists. Some online platforms are trying to take action. For example, the discussion website Reddit has scrapped it subsidiary pages ("subreddits") in order to eliminate trolls.

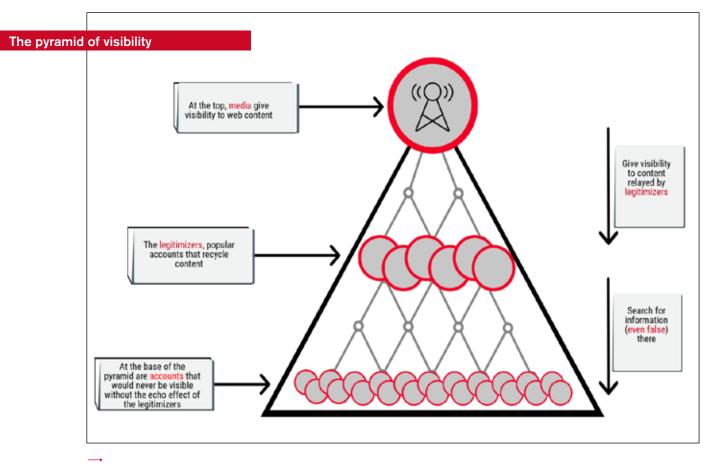


What starts these online conspiracies? It is often no more than a terse tweet from a well-followed account. Dominique Cardon, a French sociologist and author of *What Algorithms Dream About*, calls them *"launderers"*. These popular accounts relay the most slanderous allegations, which – without social network virality – would sink into Internet obscurity instead of spreading like wildfire. They play a key role in what Cardon calls the *"visibility pyramid"* by *"laundering"* content found on social network accounts with relatively few followers at the lowest level of the pyramid and making it available to the media at the top of the pyramid.

Social networks provide journalists with visibility, information sources, and access to readers. But they can also become a trap.

© Pixabay/DR

^{*} Speech at Assises du Journalisme, March 2017 (Tours, France)



Based on our interview with Dominique Cardon.

© RSF

40% of the world's population on social networks

A total of 3.81 billion individuals were online in April 2017, with more that 80% of users located in Northern Europe and the United States, 33% in South Asia and 29% in Africa. This explosion in the number of internet users in the past decade has been accelerated by mobile use. Since 2016, more than half of the world's online traffic has been via smartphones. Social networks have become the universally-used medium for accessing readers: 40% of the world's population have social media accounts and 67% of Americans get their news on social networks, according to the Washington-based Pew Research Center.

With their repeated attacks on journalists, politicians such as Donald Trump have given free rein to those who feed the hatred of journalists, offline and online. The Vocativ site has established a link between the peak moments of online harassment of former Fox News journalist Megyn Kelly and Trump's attacks via television and Twitter.

Donald Trump, media-bashing champion on social networks



Since succeeding Barack Obama, the American president has.been.haranguing.journalists.nonstop, heaping abuse on them as purveyors of "fake news" every time that a news story doesn't reflect his views. In a series of tweets posted in April, Trump targeted New York Times correspondent Maggie Haberman, accusing her of being a "third-rate reporter" working for "dishonest media".

This type of behaviour clearly encourages online harassment. In July 2017, CNN journalist Andrew Kaczynski published an article about a user of the discussion site Reddit who had created a video of the American president engaged in a wrestling match with an opponent who bore the CNN logo. Trump supporters with large numbers of followers on the networks then posted negative comments about Kaczynski. Shortly thereafter, personal data about him was posted online: his address, his personal phone number and information about those close to him. His parents and his wife received some 50 threats over the phone in the days that followed.

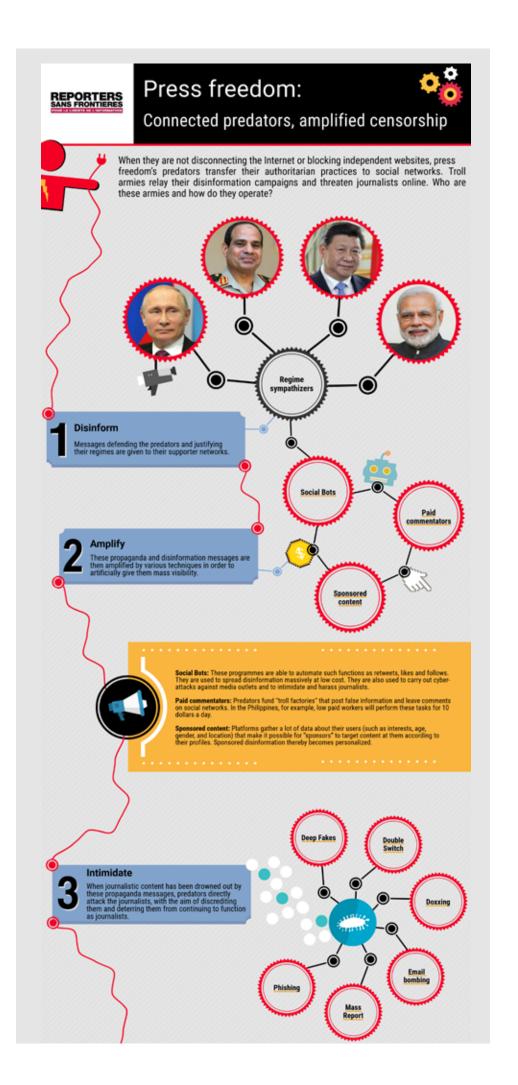
Threats to press freedom in the country of the First Amendment have become so frequent that in August 2017 RSF joined a coalition of more than 20 organizations in launching a monitoring tool on US press freedom called the the <u>U.S.</u>

Press Freedom Tracker.

"Bravo Donald!" –
Press freedom
predators hail Donald
Trump's efforts to
denigrate journalists.
© RSF







HARASSMENT IN FULL FORCE

On the web, a troll generates polemics. Trolling consists of posting messages with the aim of sparking a conflictive debate. Who are these cyberharassers? Their identity is hard to establish. Decoding these harassment campaigns requires studying dozens of accounts as well as interactions between them, thereby strengthening research efforts on these new digital threats. Still, a line can be drawn between communities of individuals and political trolls, who may or may not be paid by governments.

CROWD PSYCHOLOGY 3.0: "ANYONE CAN BE A TROLL"

In the fall of 2017, French journalist Nadia Daam of the "28 minutes" program – broadcast on the French-German Arte channel – and of the French *Europe1* radio channel, <u>was harassed</u> by members of the forum for 18-to-25-year-olds on JeuxVideo.com. The gamer site is <u>known for misogyny and weak moderation</u>. After Daam reported on the trolls who ganged up against an "anti-jerk" app, her personal email was subscribed to porn and pedophile sites. She received calls for her murder, photos of firearms, and threats that mentioned her daughter. On the night of November 1, she heard loud knocking on her door. It was hard not to connect this attempted break-in with the attacks underway against her on social networks. Daam filed a complaint for criminal threats and two of her alleged cyberharassers are being prosecuted and were given a six-month suspended sentence and a 2,000 euro fine. Daam later received online death threats from a third person, who was given a six-month suspended prison sentence.

An individual's behaviour changes when he becomes part of a crowd, the sociologist Gustave Le Bon wrote in 1895 in *The Crowd: A Study of the Popular Mind.* The anonymity of the screen, at times indispensable to journalists' reporting efforts, is used by trolls to silence them.

"These results combine to suggest that ordinary people can, under the right circumstances, behave like trolls," researchers Justin Cheng, Michael Bernstein, Cristian Danescu-Niculescu-Mizil and Jure Leskovec of Stanford and Cornell universities write in a paper. For example, they may use the hashtag #RIP – Rest in Peace – followed by a journalist's name in commenting on an article viewed unfavourably by some, as RSF has documented.



Europe 1 and Arte journalist Nadia Daam.
© PxHere / DR

COMPANIES ALSO BEHIND THE ATTACKS?

"I would really like to shoot this son of a bitch right in the forehead." Leonard Sakamoto, founder of the Repórter Brasil NGO, is often insulted on social networks. The Brazilian journalist reports on human rights in his country, specializing in investigating modern forms of slavery.

In April 2016 he became aware of a sponsored link that topped the list of every search result that included his name. The link sends a user to a fake article from the site FolhaPolitica.org, which has more than one million Facebook fans. The article alleges that Sakamoto received 250,000 euros from the Brazilian government for attacking opposition members. Upon taking legal action, the journalist discovered that the sponsored link was tied to the JBS and 4Buzz companies. The former is the major Brazilian agribusiness multinational, a world market leader in meat production, criticized many times by Sakamoto for environmental and labour-rights violations.

TERRORIST GROUPS CONDUCTING ONLINE HARASSMENT

"In many countries, journalists are threatened by the Islamic State", recalls Saudi TV presenter Nadine Al Budair, known for her feminist views. These threats are often made online. In 2014, the Islamic State disseminated a video on the web that showed the beheading of American journalist James Foley. He had been kidnapped in Syria in 2012 while covering the uprising against Bashar al-Assad. The propaganda video was then used to intimidate journalists working in the region. Rukmini Callimachi, a New York Times correspondent and NBC contributor, has been targeted by this intimidation tactic. The terrorists mentioned her on Twitter in disseminating the Foley execution video. She has also been targeted by cyberattacks and doxxing — with her personal information pirated in order to threaten her. An Islamic State member used a fake account to become a Facebook friend of Callimachi. He then downloaded all photos accessible from her profile in order to disseminate them online and intimidate her.

THE <u>WORLD PRESS FREEDOM INDEX</u>'S BEST-RANKED COUNTRIES ALSO HIT BY ONLINE HARASSMENT

In **Sweden** (2e), the Swedish Editors' Association released a <u>study showing that one-third of journalists have been threatened and harassed</u>. Seventy-two percent of women journalists working in 163 of the country's media organizations have suffered harassment.

In **Finland** (4e) one in four journalists has been targeted by harassment. Journalist Linda Pelkonen, for example, received an avalanche of messages threatening her with rape after she wrote about the rape of an adolescent girl. She had noted that the police report included the suspect's ethnicity. One reader cited her phone number in commenting on the article.

Online harassment of journalists has also claimed victims in the **Netherlands** (3e). After she called on advertisers to boycott the misogynistic and anti-Semitic GeenStij site, journalist Loes Reijmer Schreef saw her photo pinned on the site, which called on users to respond to this question: "Here is Loes Reijmer. What would you do to her?".

JOURNALISTS: VICTIMS OF SOCIAL NETWORK POLARIZATION

Social networks provide those trying to incite virulent debate with a brand-new kind

of echo chamber that favours polarization. In **Spain**, disputes over independence for Catalonia have been especially heated. As <u>RSF reported in December 2017</u>, many journalists have been hit by harassment during the debates. Henry de Laguérie, correspondent for *Europe1* in Spain, cited attacks by "senior officials who are followed by thousands of people, who then assail you. Comments by those in high-level official positions provide a blank cheque to thousands of 'trolls' who feel themselves authorized to denigrate you. I don't see 'troll' attacks as important at all, but comments coming from people in public office worry me and have given me a bad time."



The Nordic nations head the 2018 World Press Freedom Index but many journalists are subjected to online harassment in these countries, especially Sweden.

© holidays ads

For his part, the editor-in-chief of *El Periódico* in Catalonia, a national newspaper based in Barcelona, has received a never-ending series of threats in the course of the Catalonian independence debates. He has been targeted by campaigns disseminated on change.org that focused on his "Spanish-fied" name in order to declare him *persona non grata*.

In **Italy**, sensitive issues also inflame online tormentors. In 2014, Silvia Fabbia, a journalist with *Corriere dell'Alto Adige*, was insulted and criticized on Facebook for having written an article on a group of individuals who had converted to Islam. The article displeased a municipal council member, Maria Teresa Tomada, who accused the journalist of *"obtuse and naive optimism."* Her remarks were commented on by

many, among them Sergio Armanini, the Northern League candidate for mayor of Merano, who fed the trolls by writing of the journalist: "Why don't we put a burka on her head and send her to Nigeria! She'll get the picture after the hundredth rape."

In **France** as well, journalists become collateral victims of polarized debates. Local journalists, more isolated and in closer proximity to their critics, have become targets. Among them are journalists from la *Voix du Nord* reporting from Hénin-Beaumont. The newspaper had taken a stand against the far right during the 2015 regional elections. In their

wake, a strong current of hate was directed at the journalists. "After the parliamentary elections in France, and before the presidential race, the FN felt strong. I've been a journalist for 40 years, and this is the first time that we felt threatened to this extent," says the editor-in-chief. "We were treated as bastards, liars. All day long. All you can do when you can't take it any more is to disconnect from the networks."

"Virtually every day, we're getting insults and violent attacks, which sometimes become threats", says Samuel Laurent, who heads the Décodeurs [Decoders] team at French newspaper Le Monde, journalists devoted to fact-checking, especially of online rumours. They are also collateral victims of a political debate deliberately polarized by partisans on various sides. "In order to call us out, a number of movements, from the Insoumis [Unbowed] to Printemps républicain [Republican Spring], including the FN, mobilized their online communities. On certain issues, you know ahead of time that you're going to have a bad quarter-hour. It is systematic."

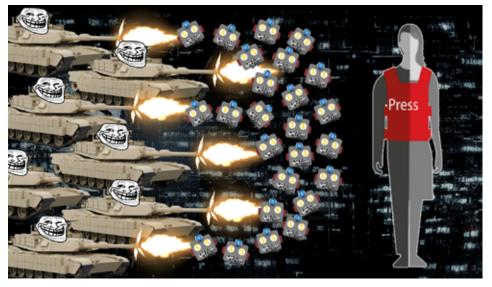


Catalonia's independence referendum fuelled tension not only on the streets but also online, especially against journalists.

TROLL ARMIES: THREATS AND PROPAGANDA

Some attacks are organized by communities of individuals and non-state groups, but they may also be set off at the highest levels by regimes that want to use the web to spread their repressive model. To this end, some 30 countries have deployed troll armies, or commenters paid by the authorities to silence online dissidence, according to a 2017 report by Freedom House as well as a University of Oxford report by Samantha Bradshaw and Philip N. Howard.

Behind the scenes is an army of activists or low-paid subcontractors who are compensated for launching campaigns aimed at discrediting or attacking journalists and disseminating propaganda. Among these new information mercenaries are the Vietnamese cyber-soldiers, the Russian troll factories; the Chinese "little pinks"; Narendra Modi's "yoddhas" in India; Erdogan's "white trolls" in Turkey; Iran's cyberguardians of the revolution for a halal Internet. And in the Philippines, impoverished workers make 10 dollars a day posting fake news favouring the president on social networks.



Troll armies target independent voices and especially journalists.
© RSF

RUSSIA: TROLL FACTORY WEB BRIGADES

Paid trolls echo messages posted by regime backers. That is the pattern in Russia, where Vladimir Putin remains quite popular. These paid commenters tend to focus on discussion topics rather than on writers themselves. Journalist Igor Yakovenko receives "routine insults on the web." He adds, "half of them are from 'enthusiasts,' the rest from professional trolls. You can easily spot the latter by their style." Yet it is difficult to differentiate paid from unpaid commenters. Dmitry Gubin, a Russian journalist and radio host, tells RSF, "I have 'personal' trolls who target discussion threads in which I participate. But there are others, 'part-time' trolls who show up every time I write something at the top of threads."

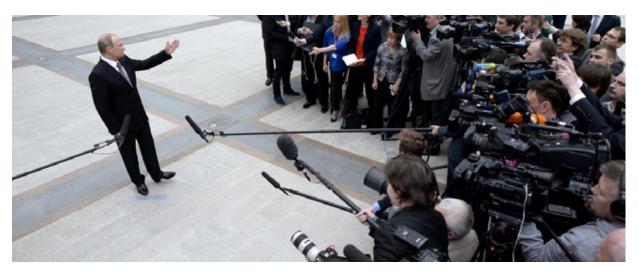
When Kremlin trolls produce fake videos to discredit an investigative journalist

In 2014, a journalist from Finnish public television who was investigating Kremlin trolls was targeted on social networks. Jessikka Aro was depicted variously as a drug addict and NATO agent by her tormentors. On one occasion, the journalist received a text message whose sender had stolen the identity of her father, who had died 20 years earlier, saying he was spying on her. "Troll accounts were sharing a studio-quality song about me, alleging I'm a 'stupid blonde' who was only imagining this whole troll phenomenon and I'm some sort of American or NATO spy. They hired an actress to play me in some of these videos, and they shared these videos on Twitter and Facebook." The harassment didn't stop in 2014. Two of her cyberharassers are being prosecuted.



Jessikka Aro, an investigative journalist who has been harassed since 2014.

In 2013, an investigation by *Novaya Gazeta* revealed the existence of the "Olgino" troll factory", located in a Saint Petersburg suburb that is home to the offices of the Internet Research Agency. The company belongs to Yevgeny Prigozhin, a close associate of Vladimir Putin. According to numerous accounts, IRA has hundreds, perhaps thousands, of people on its payroll. It is the biggest and most wellknown firm in Russia, but perhaps not the only one. It is apparently run by Maria Kuprashevich, known for her involvement in provocations against independent media organizations. Kuprashevich denies heading this "troll factory," so called because of its reported production norms which require each worker to post at least 135 commentaries a day on blogs and social networks. The main targets of the "Olgino trolls" are not journalists themselves, but the comments generated in discussions sparked by their articles. Journalist Anna Polyanskaya has a coined a term for the these pro-Kremlin trolls: "web brigades". These are the same brigades who rose to media notoriety after spreading messages to American voters during the election that brought Donald Trump to power in the United States. In September 2017, Facebook announced the shut-down of 470 fake accounts linked to the Russian troll factory. In April, 2018, hundreds more were shut down.



The difficult process of identifying the source of a disinformation campaign.

Nicholas Vanderbiest, assistant professor at the Catholic University of Louvain and a specialist in the reputation crisis of organizations on social networks, investigated the so-called "macronleaks," revealing a pro-Russian influence. In his work, he has cross-checked content disseminated on two groups of accounts – those that relay rumors in general and those that relay pro-material. Troll-spotting can only be carried out on a large scale, he tells RSF. "I have observed three months worth of activity by Russia Today and Sputnik. Twelve-hundred accounts had spread three rumors about Emmanuel Macron when he was a candidate. I chose the 6,000 most active in terms of Russian propaganda. Then I concentrated on those that shared the major rumors concerning the presidential election. When I took those that had relayed at least three rumors, I found a 92 percent consistency between the two databases." For researchers, proving a direct link between fake accounts, fake content aimed at harassing journalists, and authoritarian regimes remains an arduous task.

Vladimir Putin.
Pro-Kremlin trolls target journalists online.

CHINA: "LITTLE PINK THUMBS," THE NEW RED GUARD

In China, those who denigrate the Communist Party or the policies of President Xi Jinping are targeted by "data warriors" mobilized for the online defence of the president's "red and positive" new order.

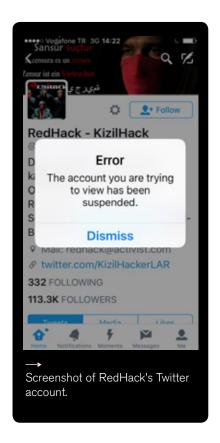
Not content merely attacking their compatriots, they hunt critics outside the country, effectively working to export the Chinese new order. In 2015, French journalist Ursula Gauthier, a China specialist who was then the Beijing correspondent of the weekly L'*Obs*, became the target of a veritable media lynching launched by incendiary editorials in the semi-official *Global Times* and *China Daily* newspapers. They took aim at an article which examined Chinese reaction to the November, 2015 attacks in Paris. Chinese authorities, normally quick to censor commentary on Chinese news sites, authorized the unleashing of a wave of hate directed at the journalist – more than 8,000 negative comments, although no one could read her article in China, where it was censored.

These new censors are mostly women – 83 percent of them, according to figures from the Weibo analysis tool developed at Beijing University. They are nicknamed the "xiao fen hong" – "little pink thumbs," after the colour of the opening page of the Jinjiang Girl Group, which attracts a largely female readership. Initially centering on literary issues, discussions soon took a turn toward more political debates, focused on criticizing those who posted negative news about China. Research published by the Chinese Academy of Social Science shows that these women are for the most part aged 18-24, living in China and abroad.

"AK TROLLS" CONTINUE THE PURGE ONLINE

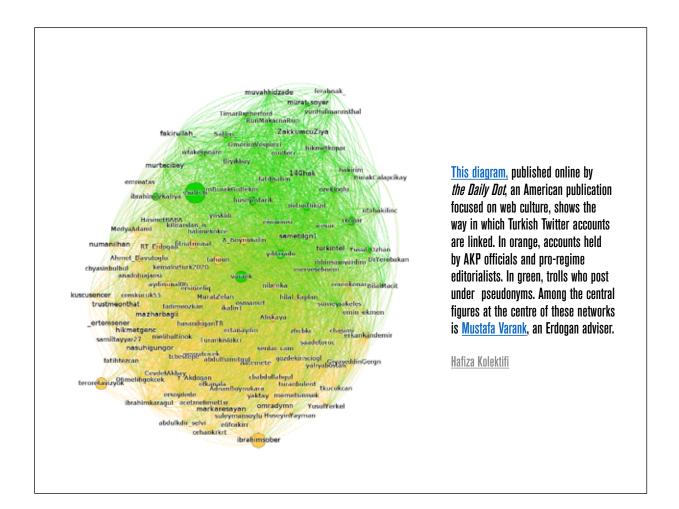
In 2013, 2.5 million Turks took to the streets to protest against President Recep Tayyip Erdogan. The response by AKP, the ruling party, included the formation of a 6,000-strong troll army dubbed the "AK Trolls" or "White Trolls," from the party's acronym which also means "white" or "clean." Now that the regime is continuing its massive media purge, the troll army is used to carry out this repression online using fake news as well as harassment. The aim? To identify online influencers, especially opposition media, in order to inflict greater damage on the credibility of journalists who report critically on the authorities. The trolls' favourite tactic is the "double switch", which occurs when trolls take control of journalists' or activists' accounts in order to publish fake posts expressing regret for having criticized the government. The Twitter account of Klaus Brinkbäumer, editorin-chief of Germany's Der Spiegel magazine, was hacked on January 14, 2018. A photo of President Erdogan and the Turkish flag were then published on the account, together with the following message in Turkish: "We would like to apologize for the bad news that we have reported and published up till now about Turkey and President Recep Tayyip Erdogan."

In 2016, the Turkish Marxist "hacktivist" organization RedHack published leaked emails between government officials. One of the emails sent by Energy Minister Berat Albayrak, who is also an Erdogan son-in-law, discusses the possibility of bringing together graphic designers, developers, and ex-military to form an online army. Following these revelations, the authoritarian Turkish regime has forbidden coverage of the subject and thrown into prison the main journalists who had been examining these connections.





Erdogan has endorsed cyberharassment as a weapon for silencing journalists online. © BULENT KILIC / AFP



ALGERIA: ONLINE MERCENARIES DOMINATE POPULAR FACEBOOK PAGES

In Algeria, a veritable online army was organized during the election campaign of Abdelaziz Bouteflika. After the arrival of 3G technology in 2013, and of 4G in 2016, the number of social network users skyrocketed. Disinformation is carried out by the orchestrated takeover of Facebook groups that have the largest numbers of followers. Administrators of these groups are approached and amounts are proposed – as much as 1 million dinars, more than 7,000 euros –for controlling the pages. Hackers are recruited to attack Facebook pages of dissidents who opposed Bouteflika's re-election. Targeted by insults, threats, and calls for their murder, journalists become the collateral victims of this war carried out in the media.

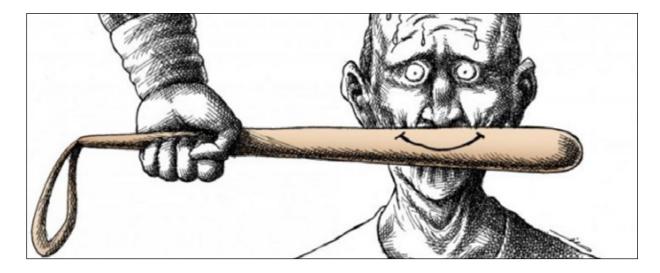
IRAN: THE ISLAMIC REPUBLIC'S VIRTUAL MILITIA

Ayatollah Khamenei has said, "Social networks should not be left in enemy hands." Since President Hassan Rouhani was inaugurated in 2013, Iran's policy of international openness has led the regime to lessen its reliance on direct harassment of journalists. Instead, the government focuses on the web, providing selective, controlled access to the internet and social media. The strategy is known as "Intelligent Filtering." The establishment of a "Halal Internet," subject to censorship and favourable to the regime, has not been abandoned; it has simply changed its name.

According to information gathered by RSF, a department devoted to monitoring journalists was established in the Intelligence Ministry and the Guardians of the Revolution. In March 2017, Abdolsamad Khoramabadi, head of the committee in charge of identifying unauthorized sites, announced that "more than 18,000 volunteers monitor the network and report offences and crimes committed on social networks to prosecutors."

The favourite target: independent journalists and citizen-journalists – including foreigners – who publish news about the regime. A BBC journalist was targeted at the end of 2017. Her sister was arrested in Iran and suspicious messages were sent from her Facebook account to the journalist in order to gain access to content. "Most of my colleagues are regularly hit by 'phishing," says Mohammad Reza Nikfar, editorin-chief of Radio Zamaneh. Journalists' email inboxes are hacked via fake links in order to discover their sources.

"Social networks played a major role in the Arab world's revolutions. Today, they are destroying it," says Zeinobia, Egyptian blogger



A cartoon by Iranian cartoonist Mana Neyestani. The regime has created a "Halal internet" that is censored and serves the regime's interests.

EGYPT: "SISIFIED" MEDIA ATTACK ONLINE JOURNALISTS



Egyptian blogger and human right activist Waël Abbas was arrested on 23 May 2018.

Not satisfied with blocking the sites of dozens of independent media organizations and human rights defence groups, Egyptian authorities also attack journalists, including foreigners, which instigate the trolls. Many journalists' accounts are also shut down on social networks, undoubtedly having been reported as abusive by the regime's online armies. And journalists are regularly insulted online. While the Twitter account of BBC Cairo correspondent Waël Hussein was blocked, fake content was disseminated by a fake account under his name. Reuters journalist Amina Ismail, whose Twitter account was suspended and then reinstated, was hit by the same tactic. Egyptian activist Waël Abbas, named by the BBC as one of the most influential people in the Middle East, was hit by the same tactic. "Only the Egyptian government benefits from the closing of my account!" the journalist told RSF before he was arrested in May 2018. At that time, he had not been able to open another account on the site. In effect, he had been deprived for life of his digital identity. Online harassment of journalists is taking place against the backdrop of a persecution campaign against the media.

VIETNAM: 10,000 "CYBER-INSPECTORS" TO HUNT DOWN DISSIDENTS

In Vietnam, where 25 bloggers were imprisoned in 2017, an announcement in late December 2017 of the <u>deployment of 10,000 cyber-inspectors</u> marked a strengthening of official control of the web. The brigade, nicknamed "Force 47," was formed to repress online dissidence and thereby the voices of independent journalists on social networks, according to accounts gathered by RSF. A country where more than half the population has Internet access, and whose population is among the world's top ten Facebook users per capita, is ranked 175th of 180 in RSF's 2018 World Press Freedom Index.



Ý O

THAILAND: STUDENT JOBS AS GOVERNMENT "CYBER-SCOUTS"

Fifteen dollars is the going rate for those who name opponents of the military regime. After the military coup d'état of 2014, Thai authorities invited citizens to become the government's eyes and ears. More than 100,000 students have been trained as "cyber-scouts" to monitor and report online behaviour capable of threatening national security. Meanwhile, regime supporters are conducting a Facebook campaign to identify and denounce users — human rights defenders, dissidents, independent journalists — who voice the slightest criticism of the monarchy.

SUB-SAHARAN AFRICA: PERSECUTION MOVES ONLINE

In many African countries, press freedom predators have begun fueling the online harassment of journalists on social networks. In Uganda, a monitoring team focused on social networks was established by the media regulation agency in order to silence criticism. In Ethiopia, leaked documents revealed that officials had hired commenters to support the regime on social networks. Sonia Rolley, the former RFI correspondent in Kigali who expelled in June 2006, was harassed for months on Twitter while she was in Rwanda in 2014. It was eventually revealed that the account from which she was being harassed was held by a person who had access to the account of Rwandan President Paul Kagame. In the wake of the controversy, numerous journalists were blocked from Kagame's official Twitter account.



"Kill these journalists once and for all"

In the summer of 2017, a fearful message was spread on social networks in Togo: "Kill all these journalists once and for all." It was accompanied by photos of four journalists, pasted onto images of pigs. The journalists' personal data was disseminated and they were accused by their critics of supporting the Lomé regime.

Online harassment has become a new way of censoring journalists. The impact on press freedom is all the more dangerous because the widespread nature of this new threat is rarely acknowledged.

RSF'S 25 RECOMMENDATIONS

TO GOVERNMENTS:

- Strengthen laws authorizing prosecution for online harassment of journalists. Enforce these laws strictly. Governments must systematically investigate online harassment cases and prosecute and convict their perpetrators. Law enforcement agencies must be granted the human and financial resources necessary to accomplish these goals.
- Strengthen the responsibility of online platforms in regard to content shared on their networks. Online platforms must not be given the power to control or censor this content. The system of platform responsibility must be linked to the effects of their activities on the quality of public debate. Governments must likewise strengthen requirements on platforms, especially concerning the transparency of their curation algorithms, as well as the extent to which their moderation policies are consistent with freedom of expression and freedom of information.
- Implement systems for alert and rapid intervention in harassment cases. These mechanisms must be coordinated with prosecutorial authorities.
- Guarantee that the rules for fighting hateful content are applied fairly and consistently. The rules must not lead to abusive limits on freedom of online freedom of expression and information. Specifically, governments must implement procedures to shield against misuse of these rules and alert mechanisms to censor and silence journalists.
- Implement recovery procedures for cyberharassment victims.

 These could include financial restitution, medical and psychological aid, and relocation assistance.
- Prohibit resorting to online influence and destabilization agents

 trolls in order to manipulate public opinion and harass
 journalists.

International level

- At the United Nations, governments must urge creation of a Special Representative for the Safety of Journalists. This office would enforce governments' respect for their obligations.
- European governments must sign and ratify the Additional Protocol to the Council of Europe's Convention on Cybercriminality. State members of the African Union must likewise ratify the Convention on Cybersecurity and Personal Data Protection. State members of other regional multilateral organizations (Organization of American States, Association of Southeast Asian Nations, African Unions) must work to create similar conventions.
- Governments must encourage multidisciplinary international research on censorship techniques. These practices change constantly. Research must focus on operating methods and on responses to cyber-harassment in general and on cyberharassment of journalists in particular.

Education

- **Governments must strengthen digital education.** The aim is to increase internet users' awareness of the impact of online harassment, and the legal consequences for perpetrators.
- All public policies concerning online violence must take into account its gender-specific nature. Women journalists are the major targets.

TO INTERNATIONAL ORGANIZATIONS

- Continue to urge governments to uphold the principle that "the same rights that people have offline must also be protected online, in particular freedom of expression."
- Contribute to research on methods of online harassment.

 Organizations must help finance this research and make recommendations to governments on fighting cyberharassment.
- International and regional human rights protective systems must include online harassment in their monitoring of abuses against journalists.

TO ONLINE PLATFORMS

- Online platforms must be transparent concerning their rules for moderating online content. They must strengthen the public nature and the transparency of their actions against online harassment. And they must establish alert systems focused on hate content.
- They must ensure that these rules are not turned into methods to silence journalists. All alerts concerning potentially illicit content must be subject to careful analysis. The platforms must be able to distinguish abusive alerts, designed solely to muffle upsetting opinions, from alerts over genuinely abusive content.
- Establish a victim-centred emergency alert system for journalists who are targeted by online threats and attacks.
- Cooperative actively with law enforcement authorities in investigations of cyberviolence against journalists, with measures including public release of the perpetrators' names.
- Combat online harassment campaigns that are orchestrated by troll factories or bots.
- **Develop communication and awareness campaigns concerning online violence,** with special attention to the targeting of journalists, especially women.

TO MEDIA ORGANIZATIONS

- Acknowledge the threat and learn to anticipate attacks. The media must strengthen the awareness of owners, executives and journalists, and implement emergency internal mechanisms such as cyberharassment hotlines to assure support and protection of journalists hit by harassment.
- Encourage the creation of networks to exchange best practices by developing a holistic approach. Those involved should include editors, community managers, digital security and legal executives as well as journalists within a media organization, but also from other media organizations, including those from abroad and even from other industries.
- **Make online harassment of journalists a major issue.** Devote more reporting and investigating to a topic that is not well known, thereby informing and building awareness in the public at large, and among government officials and journalists themselves.

TO ADVERTISERS

- Refuse to advertise on sites that participate in dissemination of hate content. And shun sites that do not do enough to fight cyberviolence.
- Develop ethics codes and best practices for online advertising.

 This work should be done in cooperation with civil society organizations, in order to ensure that online advertising does not help finance online harassment.

TUTORIAL JOURNALISTS

HOW TO DEAL WITH TROLL ARMIES

In the face of cyberviolence, RSF recommends that journalists and media organizations in general strengthen their basic training in digital security.

In advance:

- Understand that journalists are especially vulnerable to online attacks stemming from pirated personal information. The violence of these attacks can be personally destabilizing, with serious consequences for even the most experienced journalists.
- Take account of the fact that these attacks mainly target female journalists.
- Journalists must follow these indispensable rules of digital security:
 - Withdraw all personal information that is online (managing the confidentiality standards on social networks -- for example making one's Instagram account private).
 - Always evaluate the hazards and especially the trade-off between personal risks (pirating of photos of your children, for example) versus the advantages (the pleasure of sharing personal photos).
 - Note that automatic geo-localization immediately pins down your whereabouts.
 - Protect your domain names on Whois.
 - Run a Google alert for your name.
 - Use software such as Securedrop and Privacy Badger.
 - Do not make your personal phone number available online (or on an automatic absence-response message, for example)
 - Use two-factor authentification for your email accounts, and disconnect after each session.
 - Use a pass-phrase rather than a password.
 - Watch out for phishing attacks by never clicking on a suspect link.
 - Place several administrators on pages that you create, not all of them connected to your media organization.
 - As a general practice, follow <u>digital security rules</u> such as those specified in the <u>RSF Safety Guide for Journalists</u>.

During an attack:

- Continuously report and block abusive content on the online platforms that attackers use.
- Inform your colleagues and superiors.
- Retain the evidence, assembling a file with all of the harassment data.
 Ask friends or associates to do it for you if you cannot bear to read the insults and threats against you.
- Count on journalistic solidarity. Some victims of online harassment launch counter-offensives, linking supporters via a hashtag from TrollBusters, which defends women journalists hit by cyberviolence.
- Don't feed the trolls. Attacks generally display an extraordinary level of violence, but do not last long. Disconnect from social networks for several hours if necessary.
- Make sure to take screenshots.

Post-attack:

- Your account has been hacked, so take care to warn your sources because they may also be targeted. Report harassers immediately.
- If you are able, file a formal report with solid evidence to the courts.
- File a complaint with the police making sure to use the procedure for opening a case against the perpetrator as opposed to simply reporting an event.

TrollBusters has published a guide on how to respond to various forms of harassment.

PEN America published a manual for writers, journalists and journalists' employers on fighting back against online harassment. The Tactical Technology collective has also put up a site for women victims of cyberharassment.

GLOSSARY

OF CENSORSHIP WITH MANY FORMS OF ATTACK

Astroturfing. This propaganda technique, named after the artificial lawn material used in sports stadiums, creates the illusion of a spontaneous, popular movement on the internet started by a fake grassroots organization.

DDoS Attack. A Denial of Service attack aims to incapacitate a server, a service or an organization by overloading bandwidth or monopolizing all resources to exhaustion. DDoS attackers send a vast number of requests simultaneously from multiple sites on the Net. The intensity of this crossfire makes the target unstable or, at worst, non-operational. DDoS attacks are regularly launched on Russian sites. These attacks are sometimes accompanied by real-world threats as well as cyberharassment.

Dol Attack. A Denial of Information attack consists of amplifying messages through autonomous software – bots – thereby drowning an information channel in false or distracting information. Access to genuine information becomes more difficult. This massive disinformation tactic is used to discredit journalistic information. In July 2017, the French newspaper *Le Monde* investigated 100 Facebook pages which had accumulated 70 million likes, identifying 233 postings that disseminated fake information. In many that RSF investigated, spreading of fake news is used to feed predators' hateful rhetoric. The idea is to discredit a reporter's articles about a government by attacking him personally. These fake news items sometimes aim to silence independent media or those investigating ruling powers.

Deep Fakes. Producing a video, then using software to substitute one person's face for another. The technique can be used to create fake news or damage a journalist's credibility.

DoubleSwitch. The DoubleSwitch method, revealed by Access Now, consists of hacking an accounting, stealing a journalist's identity and then disseminating fake news in order to discredit him or her. This method is especially favoured in Venezuela, Burma, and Bahrain.

Doxxing. Personal data is unearthed from the web. This can include pseudonyms, photos, videos, and credit card numbers. The information is then disseminated in order to cause harm. The term comes from the verb "to document."

Email bombing. The victim is signed up to a vast number of sites, often pornographic, in order to prevent her from accessing her own email. Software available online facilitates this tactic, and allows a sender to automatically sign up for thousands of subscriptions.

Hashtag poisoning. A rallying cry for troll gangs. Once an attack is launched, a hashtag unites the attackers. Sometimes, the message is an insult aimed at a journalist. But it may be a call for her murder.

Mass report. This involves reporting a journalist's account as abusive. Once the call is made on social networks the reporting becomes massive, leading to the account being closed. This is a censorship technique that is becoming ever more widely used by perverting a function that was designed as a protection from hate speech and other illegal content. The tactic may also take advantage of platforms' moderation rules, putting them at the service of predatory moves by authoritarian regimes.

Memes. Doxxing can take the form of "memes," or reformulated photos and videos that circulate on the internet. "Even though I control my confidentiality parameters as much as possible on Facebook, memes based on photos of me have circulated on the Internet, using personal data gleaned from Facebook," says Amber Shamsi, a journalist for the BBC Urdu service. Originally, memes were a form of well-intentioned schoolyard humour, as is the norm in digital culture. These highly visual forms, which can easily go viral on the web, are now used as weapons in a war against journalists.

Non-consensual pornography. A bigger phenomenon than "revenge porn," this tactic uses sexual imagery to damage the target. Photos of journalists, often taken from their Facebook accounts, are altered by the addition of bodies taken from porn sites. Kelsey McKinney, a reporter for Vox, was harassed this way after reporting on stars whose nude photos were pirated. "I get emails that have my head photoshopped onto porn stars' bodies, or dead animals, or brutally hurt women."

Phishing. A fake link that takes the sender to a trap site is sent to a journalist. He clicks and his email inbox is hacked and his identity stolen. Phishing traditionally was used for commercial ends, but is also used to find a journalist's sources. The tactic is used for example in Iran, where the Islamic Republic's online militia attacks independent journalists.

Social Bots. These software programs are capable of automating tasks such as retweets, likes, and followers. They are used to disseminate disinformation on a massive scale, but also to launch cyber-attacks against media organizations and to intimidate and harass journalists.

Advertising sponsorship. Platforms harvest a considerable quantity of data, including interests, age, gender, and location, which then allows content to be targeted according to users' profiles. Sponsored disinformation is personalized in the same way.

Swatting. This tactic involves calling 911 – the US emergency response number – pretending the call is coming from the target's house. The attacker reports a horrible crime in progress, which results in the dispatch of a SWAT team. This tactic was used in 2013 on journalist Brian Krebs.

REPORTERS SANS FRONTIÈRES assure la promotion et la défense de la liberté d'informer et d'être informé partout dans le monde. L'organisation, basée à Paris, compte 6 bureaux à l'international (Rio, Londres, Tunis, Washington DC, Bruxelles et Taipei) et plus de 150 correspondants répartis sur les cinq continents.

Secrétaire général : CHRISTOPHE DELOIRE

SECRÉTARIAT INTERNATIONAL CS 90247 75083 Paris Cedex 02 Web: Www.rsf.org

