MODI'S YODDHAS

India **140**/180*

Methods used: Social media insults, calls for rape and death threats.

Known targets: Rana Ayyub, a journalist who wrote the *Gujarat Files*, a book about Prime Minister Narendra Modi's rise to power, is one of the favourite targets of the "Yoddhas" – the trolls who either volunteer their services or are paid employees of the ruling Hindu nationalist Bharatiya Janata Party (BJP). Swati Chaturvedi, a journalist, author of the investigation *I Am a Troll: Inside the Secret World of the BJP's Digital Army*, is also often targeted.

THE KREMLIN'S TROLL ARMY

Russia **149**/180*

Methods used: Spreading false reports and videos, publishing personal information ("doxxing"), defamation.

Known targets: Finnish investigative journalist Jessikka Aro has been one of their targets ever since she began writing about the Kremlin's trolls. In a recent book, *Putin's Troll Army*, she shed light on the propaganda they spread about those who denounce their activities. For example, the Russian journalist Igor Yakovenko and the Moscow-based foreign journalists Isabelle Mandraud (a former Le Monde correspondent) and Shaun Walker of the Guardian, are often targeted by this troll army.

JAIR BOLSONARO'S "HATE OFFICE"

Brazil **105**/180*

Methods used: Social media campaigns of insults and threats.

Known targets: Joice Hasselmann, a parliamentarian and former ally of President Bolsonaro, revealed the existence of a "hate office." Consisting of close presidential advisers and coordinated by the president's son Carlos, it publishes attacks against journalists on a large scale. Patricia Campos Mello, Constança Rezende and Glenn Greenwald are among the journalists who are often targeted because of their revelations about the Brazilian government.

THE ALGERIAN REGIME'S ELECTRONIC FLIES

Algeria **141**/180*

Methods used: Reporting alleged abuses to international online platforms to get them to remove posts or shut down accounts, posting personal information about journalists, discrediting what they report, virulent comments, personal attacks and shaming.

Known targets: The aim of this army of trolls in the government's pay is to discredit all journalists critical of the government. Journalists covering the current "Hirak" anti-government protests, including Lamine Maghnine, Redouane Boussag and RSF correspondent Khaled Drareni, are constantly targeted. The first two are currently unable to access their Facebook accounts.

MEXICAN TROLL GANGS

Mexico **144/180***

Methods used: Social media smears, threats and insults.

Known targets: Several journalists, including TV Azteca reporter Irving Pineda, were attacked by trolls for days for questioning President Andrés Manuel López Obrador's decision to release drug baron El Chapo's son. These attacks are becoming more and more frequent and are often directed at women. In November 2019, Silvia Chocarro, then representing a free speech NGO coalition that includes RSF, was among those targeted. The trolls use the hashtags *#PrensaCorupta*, *#PrensaSicaria* and *#PrensaProstituida*, which mean "corrupt press," "hired killer press" and "prostituted press."

* 2019 World Press Freedom Index

ROSKOMNADZOR, RUSSIAN FEDERAL AGENCY FOR COMMUNICATIONS AND MEDIA SUPERVISION

Russia 149/180*

Methods used: Blocking websites and messaging apps.

Known targets: It has blocked more than 490,000 websites without warning and without respecting legal procedure and has a secret blacklist of banned sites. Its targets have included news agencies such as Ferghana, investigative sites such as Listok and Grani.ru, and political magazines such as ej.ru and mbk.news. It also blocks platforms and apps that refuse to store their data on servers in Russia or provide the Russian authorities with keys to decrypt messages. This has been the case with the encrypted messaging service ProtonMail, which was partially blocked in January 2020.

IRANIAN CYBERSPACE SUPREME COUNCIL

Iran 170/180*

Methods used: Online selective access and control, blocking news websites, platforms and apps such as Telegram, Signal, WhatsApp, Facebook and Twitter.

Known targets: Created in March 2012 and consisting of senior military and political figures, this entity is the architect of the "Halal Internet", an Iranian national Internet cut off from the rest of the world. It is constructing a firewall using Internet filtering techniques. Internet shutdowns are increasingly used to contain and suppress waves of street protests, and to restrict the transmission and circulation of independent information regarded as "*counter-revolutionary*" or "*subversive*" in nature.

INDIAN MINISTRY OF HOME AFFAIRS

India 140/180*

Methods used: Disconnecting the Internet.

Known targets: It completely disconnected fixed-line and mobile Internet communication in the northern state of Jammu and Kashmir on 5 August 2019 – an extreme measure preventing Kashmiri journalists from working freely and depriving all of the state's citizens of access to independently reported news and information. After six months, the government partially restored broadband connections but access to many sites remains largely uncertain. India is the country that most uses Internet shutdowns – a total of 121 in 2019.

NATIONAL TELECOMMUNICATIONS COMMISSION (CONATEL)

Venezuela 148/180*

Methods used: Blocking websites, platforms and apps.

Known targets: Indirectly controlled by the government, CONATEL orders the blocking of websites that annoy the authorities. Many news sites such as infobae.com, elpitazo.com, dolartoday.com and armando.info have been closed for good without any possibility of appeal. CONATEL also temporarily blocks social media such as Facebook, especially when opposition leader Juan Guaidó's speeches are being broadcast live on Facebook.

CYBERSPACE ADMINISTRATION OF CHINA (CAC)

China 177/180*

Methods used: Internet censorship and supervision of private-sector platforms such as Baidu, WeChat, Weibo and TikTok; blocking and deleting content and apps.

Known targets: The CAC has stepped up its fight against the spread of rumours ever since the start of the coronavirus epidemic. The social media accounts of media outlets and bloggers have been suppressed and several media outlets have been censored, including Caijing, a Beijing-based magazine that ran a story about unreported cases of coronavirus infection.

EGYPTIAN SUPREME COUNCIL FOR MEDIA REGULATION

Egypt 163/180*

Methods used: Blocking news sites and messaging apps.

Known targets: In order to gag the media, this state entity blocks media websites on the grounds that they publish false information. More than 500 websites are currently inaccessible, including those of RSF, the BBC and the US Arabic-language TV channel Al-Hurra. In September 2019, the Council blocked 11 messaging apps including Wicker and Signal. It has also tried to block access to the Wire messaging app and Facebook Messenger.

* 2019 World Press Freedom Index

FORCE 47

Vietnam 176/180*

Methods used: "Reinformation" campaigns on social media.

Known targets: Run by the Ministry of Public Security, this army of 10,000 cyber-soldiers combats online "*abuses*" and "*reactionary forces*", meaning those opposed to the government. After a deadly incident in Dong Tam on 9 January, in which the actions of the police were widely criticized, Force 47 flooded social media with forced confessions in which individuals said they had made petrol bombs and other weapons in order to attack the police.

"CALL CENTRE HUBS"

Philippines 134/180*

Methods used: Disseminating fake or maliciously edited content, and fake memes, conducting targeted harassment campaigns.

Known targets: President Duterte's supporters have launched a campaign to smear and boycott the ABS-CBN radio and TV network with the aim of blocking the renewal of its licence. They have even gone so far as to denounce an imaginary conspiracy by various media outlets to overthrow the president. Cyber-troll armies, which have become big business ever since Duterte's 2016 election campaign, support and amplify the messages of members of the government with the aim of smearing the media and manipulating public opinion.

THE SAUDI ELECTRONIC BRIGADE

Saudi Arabia 172/180*

Methods used: Spreading false information and hate messages.

Known targets: Created by Saud Al-Qahtani when he was an adviser to the Crown Prince, this network of pro-regime trolls and bots currently produces more than 2,500 tweets a day, above all promoting the content of the conservative satellite TV news channel Saudi 24. It has also been responsible for spreading sectarian and antisemitic messages and conspiracy theories about Jamal Khashoggi, the Saudi journalist whose murder Al-Qahtani was clearly one of the instigators.

CYBER JIHADIST UNIT

Sudan 175/180*

Methods used: Spying on social media, producing and spreading false information.

Known targets: Created shortly after the start of the Arab Spring, this Sudanese intelligence agency-run troll army spies on activists, politicians and journalists on social media. It also disseminates messages and articles with false information designed to discredit members of the current transitional government and defend leading members of the old regime.

* 2019 World Press Freedom Index

HARASSMENT | STATE CENSORSHIP | FAKE NEWS | DISINFORMATION | **SPYING SURVEILLANCE**

NSO GROUP (Q CYBER TECHNOLOGIES)

Israel	**88/180***

Methods used: Spyware that uses a WhatsApp flaw to install on targeted smartphones and send them infected files that open automatically.

Known targets: According to UN experts, one of NSO's software was probably used by Saudi Arabia to spy on the journalist Jamal Khashoggi a few months before his murder by infiltrating the phones of three of his associates. Many journalists have been the targets of this spyware, including Ben Hubbard of the New York Times, Griselda Triana, the wife of the murdered Mexican journalist Javier Valdez Cárdenas, and several of his colleagues. 1,400 devices are believed to have recently been infected via WhatsApp. They include RSF's correspondent in India and other Indian journalists.

MEMENTO LABS (FORMERLY HACKING TEAM)

Switzerland	**6/180***
Italy	**43/180***
Saudi Arabia	**172/180***

Methods used: Spyware capable of extracting files from a targeted device, intercepting emails and instant messages, and activating a device's webcam or microphone.

Known targets: This company developed one of the two spyware programmes probably used to infect Washington Post owner Jeff Bezos' phone. It has kept a low profile of late but a few years ago one of its products, which are sold only to governments, was used to target Moroccan journalists with the citizen media project Mamfakinch and Ethiopian journalists with the Ethiopian Satellite Television Service (ESAT).

ZERODIUM (FORMERLY VUPEN)

United States	**48/180***

Methods used: Searches for "zero-day exploits" (previously unknown or unaddressed vulnerabilities) in widely-used software and sells the information to third parties.

Known targets: In order to learn about "zero-day exploits," Zerodium pays bounties to hackers and security researchers to be exclusively informed about their discoveries. The company says it then resells this information to "mainly European and North American governments". One of these exploits was used to spy on Ahmed Mansoor, a blogger in the United Arab Emirates who covers human rights violations and is critical of the government. He is currently serving a ten-year jail term including on a charge of publishing false information to damage the country's reputation.

MOLLITIAM INDUSTRIES

Spain	**29/180***

Methods used: Tools for intercepting phone calls and emails.

Known targets: Those who have bought its surveillance tools include the Colombian armed forces, which have used them to illegally spy on supreme court judges, politicians, journalists and journalists' sources. The Colombian targets have included Alejandro Santos the editor of the news magazine Semana, and some of his reporters after they published articles about crimes committed by the members of the military.

FINFISHER

Germany	**13/180***

Methods used: Surveillance and intrusion software used to get access to apps and personal data on smartphones, including chats, photos and GPS data.

Known targets: FinFisher is suspected of selling its FinSpy software to Turkey, which used it to spy on activists and journalists. It was found on a spoof version of Adalet, a Turkish opposition website created to help activists coordinate protests against President Erdogan in the summer of 2017. RSF Germany and several other civil society organizations have filed a complaint against the company that is still on-going.

* 2019 World Press Freedom Index