HARCÈLEMENT | CENSURE D'ETAT | FAKE NEWS DÉSINFORMATION | ESPIONNAGE-SURVEILLANCE

LES YODDHAS DE MODI

Inde **140/180***

Moyen(s) utilisé(s) : Insultes, appels au viol et menaces de mort sur les réseaux sociaux.

Cible(s) identifiée(s) : Auteure des *Gujarat Files*, un livre-enquête sur l'ascension au pouvoir de l'actuel Premier ministre indien Narendra Modi, la journaliste Rana Ayyub est l'une des cibles privilégiées des millions de "Yoddhas" - des trolls volontaires ou des employés rémunérés, au service du parti nationaliste hindou au pouvoir, le Bharatiya Janata Party (BJP). Swati Chaturvedi, journaliste et auteure de *I Am a Troll: Inside the Secret World of the BJP's Digital Army*, une enquête sur l'armée digitale au service de la droite nationaliste hindoue, est également fréquemment ciblée.

LES ARMÉES DE TROLLS DU KREMLIN

Russie **149**/180*

Moyen(s) utilisé(s) : Propagation de fausses informations et vidéos, publication d'informations personnelles ("doxxing"), diffamation.

Cible(s) identifiée(s) : Depuis qu'elle enquête sur les trolls du Kremlin, la journaliste d'investigation finlandaise Jessikka Aro est devenue l'une de leurs cibles. Dans un récent livre-enquête, *Putin's Troll Army*, elle révèle les activités de propagande de ces trolls à l'encontre de ceux qui dénoncent leurs agissements. Les professionnels de l'information font partie de leurs cibles privilégiées. Par exemple, le journaliste russe Igor Yakovenko et les journalistes étrangers basés à Moscou, Isabelle Mandraud, ancienne correspondante du Monde, et Shaun Walker, correspondant du Guardian ont révélés être fréquemment la cible de cette armée de trolls.

LE "CABINET DE LA HAINE" DE BOLSONARO

Brésil **105**/180*

Moyen(s) utilisé(s) : Campagne d'insultes et de menaces sur les réseaux sociaux.

Cible(s) identifiée(s) : La députée Joice Hasselmann, ancienne alliée du président Bolsonaro, a révélé l'existence d'un *"cabinet de la haine"*, qui publie à grande échelle des attaques contre des journalistes. Ce groupe, composé de conseillers très proches du président et coordonné par son fils Carlos, ont notamment dans leur ligne de mire les journalistes Patricia Campos Mello, Constança Rezende et Glenn Greenwald. Leurs révélations sur le gouvernement brésilien leur valent d'être fréquemment victimes de campagnes de haine sur les réseaux sociaux.

LES MOUCHES ÉLECTRONIQUES DU POUVOIR ALGÉRIEN

Algérie **141**/180*

Moyen(s) utilisé(s) : Signalements abusifs de pages et de profils contestataires sur les réseaux sociaux, pour inciter la plateforme à les fermer. Publication d'informations personnelles, dilution d'informations, commentaires virulents, attaques personnelles, chantage, stigmatisation.

Cible(s) identifiée(s) : L'objectif de cette armée de trolls payée par le gouvernement est de discréditer tous les journalistes critiques du pouvoir en place. Depuis qu'ils couvrent le mouvement de contestation populaire en Algérie, le journaliste indépendant et correspondant de RSF, Khaled Drareni, et deux journalistes qui eux aussi ont couvert le mouvement de protestation du Hirak, Lamine Maghnine et Redouane Boussag, sont ciblés quotidiennement. Ces deux derniers n'ont aujourd'hui plus accès à leur compte Facebook.

GANGS DE TROLLS MEXICAINS

Mexique **144/180***

Moyen(s) utilisé(s) : Dénigrement, menaces et insultes sur les réseaux sociaux

Cible(s) identifiée(s) : Pour avoir questionné le président Andrés Manuel López Obrador sur sa décision de relâcher le fils du baron de la drogue El Chapo, plusieurs journalistes, ont été attaqués pendant plusieurs jours par des trolls. Parmi ces journalistes, Irving Pineda, reporter pour Tv Azteca, et Silvia Chocarro, qui représentait ce jour-là une coalition d'ONG de défense de la liberté d'expression incluant RSF. Les trolls se ralliaient en utilisant notamment les hashtags *#PrensaCorupta*, *#PrensaSicaria* et *#PrensaProstituida* signifiant respectivement "presse corrompue", "presse tueur à gage" et "presse prostituée".

* Classement mondial de la liberté de la presse 2019

HARCÈLEMENT | **CENSURE D'ÉTAT** | FAKE NEWS DÉSINFORMATION | ESPIONNAGE-SURVEILLANCE

ROSKOMNADZOR, AUTORITÉ FÉDÉRALE DE CONTRÔLE DES COMMUNICATIONS ET DES MÉDIAS RUSSES

Russie **149/180***

Moyen(s) utilisé(s) : Blocage de sites internet et d'applications.

Cible(s) identifiée(s) : Le Roskomnadzor, autorité officielle de contrôle des médias de Russie, a bloqué plus de 490.000 sites internet, sans respecter la procédure légale ni envoyer d'avertissement préalable. Il tient une liste noire, secrète, de sites à proscrire. Ses cibles sont des agences de presse comme Ferghana, des sites d'investigation comme Listok ou Grani.ru et des magazines politiques tels ej.ru ou mbk.news. Il bloque également les sites et applications qui refusent de stocker leurs données sur des serveurs en Russie ou de livrer aux autorités leurs clés de déchiffrement des messages. C'est le cas de la messagerie cryptée ProtonMail qui a été partiellement bloquée en janvier 2020.

CONSEIL SUPRÊME DU CYBERESPACE IRANIEN

Iran **170/180***

Moyen(s) utilisé(s) : Accès sélectif et contrôle d'Internet, blocage de sites d'information et d'applications comme Telegram, Signal, Whatsapp, Facebook et Twitter.

Cible(s) identifiée(s) : Créé en mars 2012, cet organisme, composé de hautes personnalités militaires et politiques, est l'architecte de "l'Internet halal", réseau national iranien séparé du reste du monde. Il construit un mur numérique en utilisant des techniques de filtrage de l'Internet. Ils ont de plus en plus recours aux coupures internet pour contenir et réprimer les mouvements de contestation dans le pays, et limiter la transmission et la diffusion d'informations indépendantes, considérées comme des tentatives *«contre-révolutionnaires subversives».*

MINISTÈRE INDIEN DES AFFAIRES INTÉRIEURES

Inde **140/180***

Moyen(s) utilisé(s) : Coupure des télécommunications.

Cible(s) identifiée(s) : Le 5 août 2019, le ministère de l'Intérieur indien a coupé totalement les communications téléphone et Internet dans la province de Jammu-et-Cachemire. Cette mesure extrême empêche les journalistes cachemiris de travailler librement et prive l'ensemble des citoyens de la région d'un accès à une information indépendante. Six mois plus tard, le gouvernement a partiellement rétabli les connexions haut débit, mais l'accès à de nombreux sites reste largement aléatoire. L'Inde est le pays ayant le plus recours aux coupures internet, 121 en 2019.

COMMISSION NATIONALE DES TÉLÉCOMMUNICATIONS (CONATEL)

Venezuela **148/180***

Moyen(s) utilisé(s) : Blocages de sites internet et d'applications.

Cible(s) identifiée(s) : Contrôlée en sous-main par le gouvernement, la Conatel peut ordonner le blocage de sites Internet dérangeants pour le pouvoir en place. De nombreux sites d'information dont infobae.com, elpitazo.com, dolartoday.com et armando.info ont ainsi été fermés définitivement, sans aucun recours. La Conatel organise aussi le blocage temporaire des réseaux sociaux, notamment Facebook, en particulier lorsque le dirigeant de l'opposition Juan Guaido y transmet des discours en direct.

L'ADMINISTRATION DU CYBERESPACE CHINOIS (CAC)

Chine **177/180***

Moyen(s) utilisé(s) : Censure de l'internet et supervision des plateformes privées comme Baidu, WeChat, Weibo et TikTok; blocage et suppression des contenus et d'applications.

Cible(s) identifiée(s) : Depuis le déclenchement de l'épidémie de coronavirus, l'organisme de contrôle de l'internet chinois a encore renforcé sa lutte contre la propagation de rumeurs. Des comptes de médias et de blogueurs ont été supprimés des réseaux sociaux et plusieurs médias ont été censurés dont Caijing, magazine basé à Pékin, qui avait publié un rapport sur des cas d'infection non répertoriés.

CONSEIL SUPRÊME DE RÉGULATION DES MÉDIAS ÉGYPTIENS

Egypte **163/180***

Moyen(s) utilisé(s) : Blocage de sites d'informations et des applications de messagerie instantanée.

Cible(s) identifiée(s) : Afin de museler la presse, cet organisme étatique bloque des sites de médias pour publication de fausses informations. A ce jour, plus de 500 sites internet sont inaccessibles, dont ceux de RSF, de la BBC et de la chaîne américaine en arabe Al-Hurra. Fin septembre 2019, le Conseil bloquait 11 messageries instantanées, notamment Wicker et Signal. Il a aussi tenté de bloquer l'accès aux messageries de Wire et de Facebook.

* Classement mondial de la liberté de la presse 2019

HARCÈLEMENT | CENSURE D'ETAT | FAKE NEWS **DÉSINFORMATION** | ESPIONNAGE-SURVEILLANCE

FORCE 47 VIETNAMIENNE

Vietnam **176/180***

Moyen(s) utilisé(s) : Campagnes de *"réinformation"* sur les réseaux sociaux.

Cible(s) identifiée(s) : Cette armée de 10 000 cyber militaires, dirigée par le ministère de la Sécurité publique, traque *"les abus"* et les *"forces réactionnaires"* c'est-à-dire opposées au gouvernement vietnamien. Le 9 janvier dernier, suite à un incident meurtrier à Dong Tam dont la gestion par les autorités a été vivement critiquée, la Force 47 a diffusé sur les réseaux sociaux des confessions forcées de citoyens avouant avoir fabriqué des bombes à essence et d'autres armes pour attaquer la police.

LES "CALL CENTER HUBS" DES PHILIPPINES

Philippines **134/180***

Moyen(s) utilisé(s) : Diffusion de fausses informations et de mèmes fallacieux, campagnes de harcèlement ciblées, informations fausses ou tronquées.

Cible(s) identifiée(s) : Aux Philippines, les partisans du président Duterte ont lancé une campagne de dénigrement et de boycott de la chaîne de télévision ABS-CBN visant la révocation de sa licence d'exploitation. Ils sont allés jusqu'à dénoncer un complot imaginaire, censé réunir en secret divers médias indépendants, dont l'objectif serait de renverser le président. Depuis sa campagne en 2016, les armées de cyber-trolls sont devenues une industrie prospère. Elles soutiennent et amplifient les messages des membres du gouvernement dans l'objectif de dénigrer les médias et manipuler l'opinion publique.

BRIGADE ÉLECTRONIQUE SAOUDIENNE

Arabie Saoudite **172/180***

Moyen(s) utilisé(s) : Propagation de fausses informations et de discours de haine.

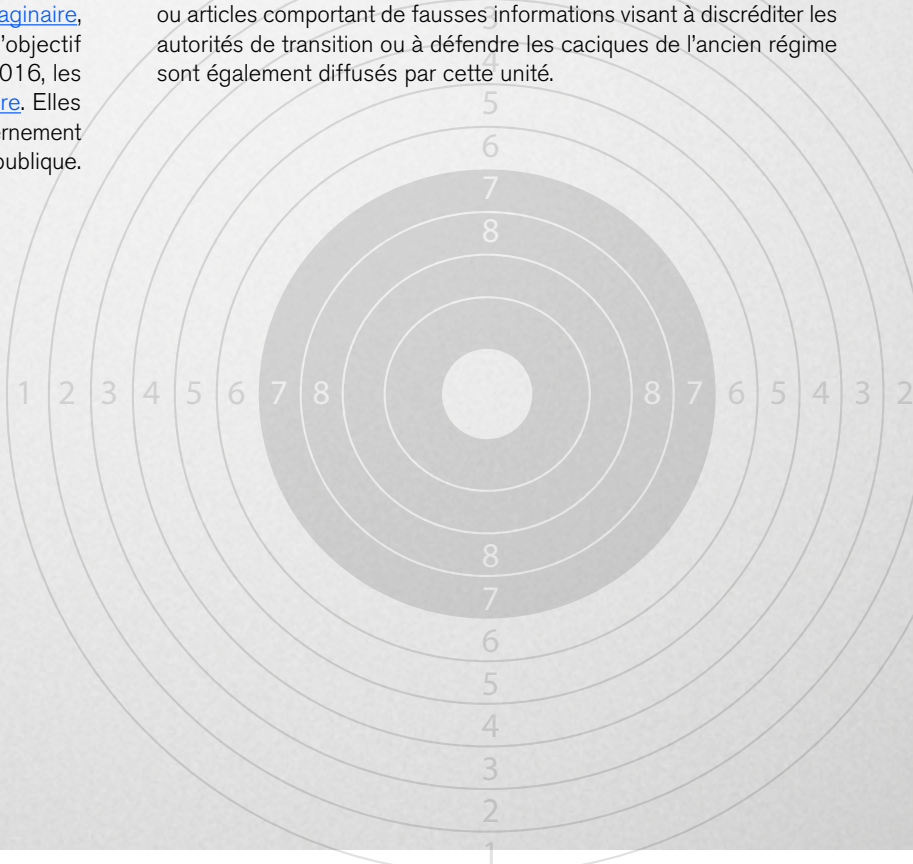
Cible(s) identifiée(s) : Ce réseau de trolls pro-régime et de robots créé par Saud Al-Qahtani, alors qu'il était conseiller du prince héritier d'Arabie Saoudite, produit actuellement plus de 2 500 tweets par jour. Il fait surtout la promotion des contenus de la chaîne d'information par satellite conservatrice Saudi 24. Il est notamment responsable de la propagation de discours de haine sectaire, d'antisémitisme et de théories du complot visant le journaliste assassiné Jamal Khashoggi, dont Saud Al-Qahtani a manifestement été l'un des instigateurs.

CYBER JIHADIST UNIT SOUDANAISE

Soudan **175/180***

Moyen(s) utilisé(s) : Espionnage sur les réseaux sociaux, fabrication et propagation de fausses informations.

Cible(s) identifiée(s) : Créée peu après le déclenchement des printemps arabes, cette armée de trolls sous les ordres des services de renseignement soudanais a espionné des activistes, des leaders politiques et des journalistes sur les réseaux sociaux. Des messages ou articles comportant de fausses informations visant à discréditer les autorités de transition ou à défendre les caciques de l'ancien régime sont également diffusés par cette unité.



* Classement mondial de la liberté de la presse 2019

HARCÈLEMENT | CENSURE D'ETAT | FAKE NEWS DÉSINFORMATION | **ESPIONNAGE-SURVEILLANCE**

NSO GROUP (Q CYBER TECHNOLOGIES)

Israël — **88/180*** 

Moyen(s) utilisé(s) : Logiciels de surveillance utilisant une faille de la messagerie Whatsapp pour installer un virus sur les appareils visés, en leur envoyant des fichier infectés qui s'ouvrent automatiquement.

Cible(s) identifiée(s) : D'après des experts des Nations Unies, un logiciel de NSO a probablement été utilisé par le royaume d'Arabie Saoudite pour surveiller le journaliste Jamal Khashoggi quelques mois avant son assassinat, en infiltrant les téléphones de trois de ses associés. De nombreux journalistes ont été ciblés par ce logiciel espion, notamment Ben Hubbard du *New York Times*, ou encore Griselda Triana, épouse du journaliste mexicain assassiné Javier Valdez Cárdenas, ainsi que plusieurs de ses collègues. Récemment, 1400 appareils ont été infectés via Whatsapp dont ceux de journalistes indiens, parmi lesquels le correspondant de RSF en Inde.

MEMENTO LABS (EX HACKING TEAM)

Suisse — **6/180*** 

Italie — **43/180*** 

Arabie Saoudite — **172/180*** 

Moyen(s) utilisé(s) : Outils de surveillance capables d'extraire des fichiers d'un appareil ciblé, d'intercepter des courriels et messages instantanés, ou d'activer à distance la webcam ou le microphone d'un appareil.

Cible(s) identifiée(s) : Parmi les deux logiciels probablement utilisés pour infecter le téléphone du propriétaire du Washington Post, Jeff Bezos, celui développé par cette entreprise. Plutôt discrète ces dernières années, elle avait déjà été pointée du doigt il y a quelques années lorsqu'un de ses produits, vendu exclusivement aux gouvernements, avait permis de cibler des journalistes marocains de Mamfakinch et des journalistes éthiopiens de la Ethiopian Satellite Television Service (ESAT).

ZERODIUM (EX-VUPEN)

Etats-Unis — **48/180*** 

Moyen(s) utilisé(s) : Recherche des failles de sécurité dans les logiciels et services internet, puis revente à des tiers intéressés.

Cible(s) identifiée(s) : Pour repérer des failles inédites dans des logiciels grand public, Zerodium rémunère des hackers du monde entier pour leurs découvertes. Une fois les vulnérabilités identifiées et exploitées, les informations sont revendues, selon l'entreprise, à *"des organismes gouvernementaux principalement européens et nord-américains"*. L'une de ces failles a permis la mise sous surveillance d'un blogueur émirati critique du gouvernement, Ahmed Mansoor, qui travaillait sur les violations des droits humains dans son pays. Il est aujourd'hui emprisonné aux Emirats Arabes Unis, accusé notamment d'avoir publié de fausses informations dans le but de nuire à la réputation du pays.

MOLLITIAM INDUSTRIES

Espagne — **29/180*** 

Moyen(s) utilisé(s) : Outils d'interception des conversations téléphoniques et des e-mails.

Cible(s) identifiée(s) : Ces logiciels de surveillance ont notamment été achetés par l'armée colombienne, qui s'en est servie pour surveiller illégalement des magistrats de la Cour suprême, des élus de différents partis, ainsi que des journalistes et leurs sources. Parmi eux, des journalistes du magazine Semana, notamment leur directeur Alejandro Santos, après la publication d'enquêtes sur des crimes et délits commis par des militaires.

GAMMA INTERNATIONAL

Allemagne — **13/180*** 

Royaume-Uni — **33/180*** 

Moyen(s) utilisé(s) : Outils de surveillance et d'intrusion permettant d'accéder aux applications et aux données personnelles stockées dans les téléphones - conversations, photos, données GPS...

Cible(s) identifiée(s) : L'entreprise est soupçonnée d'avoir vendu illégalement le logiciel espion Finspy à la Turquie, qui l'a utilisé pour espionner des activistes et des journalistes. Il a été retrouvé sur une fausse version du site d'opposition turc *Adalet*, créé pour aider les activistes à se coordonner pendant les protestations contre le président turc Recep Erdogan durant l'été 2017. RSF Allemagne, et plusieurs organisations de la société civile, ont déposé plainte contre l'entreprise. L'enquête est en cours.

* Classement mondial de la liberté de la presse 2019