Global Network
on Extremism & Technology

Manipulation de l'accès aux technologies de la communication : lutte contre le terrorisme ou répression d'État ?

Fatima Mustafa

Résumé exécutif et synopsis

Le GNET est un projet spécial du Centre international d'étude de la radicalisation du King's College, à Londres.

L'autrice de ce rapport est Fatima Mustafa.

Le Global Network on Extremism and Technology (Réseau mondial sur l'extrémisme et la technologie – GNET) est une initiative de recherche universitaire bénéficiant du soutien du Forum mondial de l'Internet contre le terrorisme (GIFCT), une initiative indépendante mais financée par le secteur qui vise à mieux comprendre et lutter contre l'utilisation des technologies par les groupes terroristes. Le GNET est formé et dirigé par le Centre international d'étude de la radicalisation (ICSR), un centre de recherche universitaire basé dans les locaux du Département d'étude des guerres du King's College, à Londres. Les opinions et conclusions exprimées dans ce document sont celles des auteurs et ne doivent en aucun cas être interprétées comme représentant les opinions et conclusions, expresses ou implicites, du GIFCT, du GNET ou de l'ICSR.

COORDONNÉES

Pour toute question, demande d'information et demande de copies supplémentaires du présent rapport, contacter :

ICSR
King's College London
Strand
Londres WC2R 2LS
Royaume-Uni

T. **+44 20 7848 2098**
E. **mail@gnet-research.org**

Twitter : **@GNET_research**

Les présents résumé exécutif et synopsis ont été traduits en allemand, anglais, arabe, français, indonésien et japonais. Ces traductions, de même que le rapport complet en anglais, peuvent, comme toutes les autres publications du GNET, être téléchargées gratuitement à partir du site Internet du GNET : www.gnet-research.org.

Résumé exécutif

Qu'ils soient démocratiques ou autoritaires, les États du monde entier misent de plus en plus sur l'interruption des services Internet et cellulaires pour limiter la violence, contrer les manifestations, faire obstacle aux mouvements d'opposition et contrôler la diffusion des informations. Des données collectées par Access Now témoignent de la hausse régulière, entre 2016 et 2019, du nombre d'interruptions du réseau et de limitations de l'accès aux technologies de la communication (213 interruptions en 2019 contre 75 en 2016) dans un large éventail de pays, par exemple le Vénézuela, l'Inde, l'Égypte ou le Soudan.[1] Si les États invoquent généralement la lutte contre la violence pour justifier ces perturbations, les défenseurs et défenseuses des droits humains estiment que ces mesures drastiques limitant l'accès aux technologies de la communication violent les droits humains, y compris le droit à la liberté d'expression, et portent gravement atteinte à l'accès aux soins de santé, à l'éducation et au travail. Ces coupures sont par ailleurs très coûteuses sur le plan économique. Elles auraient ainsi fait perdre 8 milliards de dollars à l'économie mondiale pour la seule année 2019.[2] Malgré ces coûts astronomiques, peu de travaux empiriques ont visé à déterminer si elles permettaient réellement d'atteindre les objectifs prétendument recherchés par les États. En l'absence de preuves, ces derniers font souvent valoir l'argument de la lutte contre la violence ou les fausses informations, ou encore la défense de la sécurité nationale, pour justifier leurs mesures.

Le présent rapport examine de plus près l'un des arguments fréquemment invoqués pour justifier les interruptions de réseau à l'échelle nationale : la lutte contre le terrorisme. Il évalue par ailleurs l'efficacité de ces mesures à cet égard. À partir de données journalières (recueillies et publiées par Access Now et la Coalition #KeepItOn) sur les coupures de réseau Internet et mobile, ainsi que sur les mesures visant à ralentir Internet et les interdictions d'accès aux réseaux sociaux mises en œuvre à l'échelle nationale dans plusieurs pays entre 2016 et 2019[3], le présent rapport propose une analyse préliminaire des liens entre ces différentes mesures et la violence terroriste. Les données sur les personnes tuées ou blessées au quotidien par des attentats terroristes perpétrés à travers le monde sont tirées de la base de données Global Terrorism Database,[4] et servent de fondement à l'analyse de régression à effets fixes effectuée dans ce rapport. Cette dernière conclut que les interruptions du réseau (coupures et ralentissements), de même que l'interdiction de l'accès aux réseaux sociaux tels que Facebook, Twitter ou WhatsApp, ne sont pas corrélées au nombre de victimes d'attentats terroristes. Cette analyse présente des limites liées au fait que les

1 Access Now et Coalition #KeepItOn, « Shutdown Tracker Optimization Project (STOP) », https://www.accessnow.org/keepiton/ (consulté le 8 novembre 2021).
2 Chloe Taylor (2020) « Government-led internet shutdowns cost the global economy $8 billion in 2019, research says » CNBC, 8 janvier 2020, https://www.cnbc.com/2020/01/08/government-led-internet-shutdowns-cost-8-billion-in-2019-study-says.html (consulté le 6 novembre 2021).
3 Access Now et #KeepItOn Coalition, « Shutdown Tracker Optimization Project (STOP) ».
4 National Consortium for the Study of Terrorism and Responses to Terrorism, Global Terrorism Database, https://www.start.umd.edu/gtd/ (consulté le 6 août 2021).

interruptions du réseau ne sont pas aléatoires. Elle ne permet pas, par conséquent, d'établir un lien de cause à effet entre ces mesures et la violence terroriste. Elle donne toutefois un premier aperçu de leur effet sur le terrorisme, et ouvre ainsi la voie à des recherches ultérieures. Dans la dernière partie du rapport, nous passerons outre les justifications officielles des États pour analyser brièvement les autres raisons pouvant expliquer le recours à ces mesures, telles que la volonté de dissimuler des répressions ou d'empêcher la publication de certains contenus. Nous examinerons également les autres usages réservés par les États aux technologies de la communication et aux réseaux sociaux au nom de la lutte contre le terrorisme, tels que les demandes de suppression des contenus de nature extrémiste ou de communication des données personnelles aux fins de contrôle approfondi addressées aux plateformes.

Synopsis

Avec la diffusion rapide des technologies de la communication telles qu'Internet et les téléphones portables, qui occupent aujourd'hui une place centrale dans nos vies (notre dépendance vis-à-vis de ces technologies a récemment été mise en lumière par la pandémie mondiale de coronavirus), les États se retrouvent face à un dilemme. S'ils autorisent l'utilisation illimitée des technologies de la communication, ils risquent de se heurter à une opposition organisée au travers de ces mêmes technologies. Mais s'ils en limitent l'accès, ils risquent aussi d'en subir le contrecoup. Kedzie appelle ce phénomène le « dilemme du dictateur »[5]. Les États autoritaires ne sont cependant pas les seuls à y être confrontés : les célèbres travaux d'Agarwal, de Howard et de Hussain montrent en effet que 39 % des coupures de réseau survenues entre 1995 et 2011 ont eu lieu dans des démocraties.[6] Face au « dilemme du dictateur », pourquoi certains États, démocratiques ou non, choisissent-ils de plus en plus fréquemment de limiter l'accès aux réseaux de communication à certaines périodes décisives ?

Les États nient souvent avoir délibérément recours aux interruptions de réseau. Lorsqu'ils l'admettent, ils présentent ces mesures comme un instrument permettant de lutter contre la violence, d'endiguer les manifestations, d'assurer la sécurité du public, d'empêcher la propagation de fausses informations et d'éviter la triche aux examens.[7] Des données publiées par Access Now et la Coalition #KeepItOn sur les interruptions de réseau survenues entre 2016 et 2019 dans diverses régions du monde révèlent que la lutte contre le terrorisme était le premier motif invoqué par les États pour justifier les coupures nationales. Dans certains cas, ils prétextent que ces mesures empêchent l'opposition ou les groupes terroristes de s'organiser pour planifier ou perpétrer des attentats ou, plus généralement, qu'elles aident à surmonter les problèmes liés aux actions collectives.[8] Selon leurs détracteurs, ces coupures portent atteinte aux droits humains fondamentaux, comme le droit à la liberté d'expression ou l'accès aux soins de santé, à l'éducation et au travail. Elles nuisent par ailleurs aux entreprises et à l'économie. En Inde, leur coût s'élevait par exemple à 2,8 milliards de dollars l'an dernier.[9] Malgré ces coûts humains et financiers, nous n'avons encore que peu d'éléments permettant d'affirmer que les interruptions de réseau fonctionnent réellement de la façon dont les États le prétendent.

Ce rapport propose une analyse préliminaire de l'efficacité des interruptions de réseau en matière de lutte contre la violence terroriste.

5 Christopher Kedzie (1997) « Communication and Democracy: Coincident Revolutions and the Emergent Dictators », Santa Monica, CA : RAND Corporation, https://www.rand.org/pubs/rgs_dissertations/RGSD127.html (consulté le 6 novembre 2021).

6 P. N. Howard, S. Agarwal et M. Hussain (2011) The Dictator's Digital Dilemma: When Do States Disconnect Their Digital Networks? *Issues in Technology Innovation* vol. 13, p. 1–11. Washington, D.C. : Center for Technology Innovation at Brookings.

7 Access Now et #KeepItOn Coalition, « Shutdown Tracker Optimization Project (STOP) ».

8 Fahad Desmukh (2012) « Ban on Cellphone Use in Pakistan », PRI, 31 décembre 2012, https://www.pri.org/stories/2012-12-31/ban-cell-phone-use-pakistan (consulté le 13 septembre 2020).

9 Archana Chaudhary (2021) « World's Worst Internet Shutdowns Cost India $2.8 Billion in 2020 », Bloomberg, 5 janvier 2021, https://www.bloomberg.com/news/articles/2021-01-05/world-s-worst-internet-shutdowns-cost-india-2-8-billion-in-2020 (consulté le 6 novembre 2021).

Nous y étudions les liens entre les interruptions de réseau et le nombre de personnes tuées ou blessées lors d'attentats terroristes pour déterminer la validité de l'argument fréquemment invoqué selon lequel ces mesures seraient un instrument central de la lutte contre le terrorisme. Un modèle de régression à effets fixes fondé sur un jeu de données de panel consacrées aux interruptions de réseau et aux attentats terroristes survenus respectivement à l'échelle nationale et mondiale entre 2016 et 2019 révèle l'absence de corrélation entre le nombre de victimes d'attentats terroristes et les coupures de réseau nationales d'une part, et les interdictions d'accès aux réseaux sociaux (Facebook, Twitter et WhatsApp) d'autre part. Compte tenu des limites de cette analyse, telles que l'attribution non aléatoire du traitement (à savoir, les interruptions de réseau) et l'absence de variable de contrôle pour mesurer le renforcement de la sécurité lors des coupures, il est difficile d'établir un lien de causalité. Dans l'ensemble, ces conclusions offrent une autre perspective sur le débat, qui se concentre souvent sur les conséquences des coupures de réseau en matière de droits humains et de participation démocratique et élude les données empiriques quant à leur véritable potentiel.

Les rares publications scientifiques consacrées aux liens entre les technologies de la communication et l'organisation et l'exécution d'actes violents donnent des résultats contradictoires. Certaines d'entre elles concluent que l'accès aux technologies de la communication (téléphones portables ou Internet) permet aux membres d'organisations terroristes de se coordonner et de planifier leurs attaques[10]. D'autres estiment que ces technologies sont utilisées par les civils pour signaler des activités terroristes aux organes gouvernementaux et faire ainsi obstacle aux actes de violence.[11] Quelques spécialistes ont examiné les données empiriques sur les niveaux de mobilisation et de violence pendant les coupures de réseau, et en concluent que ces dernières entraînent en réalité une hausse de la violence et de la mobilisation politique, notamment en Égypte (Hassanpour)[12] et en Inde (Rydzak)[13] : dans les deux cas, les coupures de réseau étaient liées à une intensification, et non à un recul, de certaines formes de mobilisation politique. Au Pakistan, Mustafa a démontré que le nombre d'attentats terroristes baissait lors des coupures de réseau imposées par l'État, mais augmentait le lendemain.[14] Bon nombre des travaux consacrés aux liens entre les réseaux de communication et la violence sont fondés sur des analyses nationales. Le présent rapport s'appuie sur un jeu de données de panel international pour analyser l'effet des interruptions de réseau sur la violence terroriste dans différents pays, proposant ainsi des conclusions généralisables qui enrichissent le corpus de connaissances existant sur la question.

10 Jan H. Pierskalla et Florian M. Hollenbach (2013) « Technology and Collective Action: The Effect of Cell Phone Coverage on Political Violence in Africa », *American Political Science Review* vol. 107, n° 2, p. 207–24. https://doi.org/10.1017/S0003055413000075.

11 Jacob N. Shapiro et Nils B. Weidmann (2015) « Is the Phone Mightier Than the Sword? Cellphones and Insurgent Violence in Iraq », *International Organization* vol. 69, n° 2, p. 247–74. https://doi.org/10.1017/S0020818314000423.

12 Navid Hassanpour (2014) « Media Disruption and Revolutionary Unrest: Evidence from Mubarak's Quasi-Experiment », *Political Communication* vol. 31, n° 1, p. 1–24. https://doi.org/10.1080/10584609.2012.737439.

13 Jan Rydzak (2019) « Of Blackouts and Bandhs: The Strategy and Structure of Disconnected Protest in India », https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3330413 (consulté le 21 septembre 2021).

14 Fatima Mustafa (2021) « Can Cellphone Shutdowns Stop Terrorist Violence? Evidence from Pakistan », *Terrorism and Political Violence*, https://doi.org/10.1080/09546553.2021.1908270.

Global Network
on Extremism & Technology

COORDONNÉES

Pour toute question, demande d'information et demande de copies supplémentaires du présent rapport, contacter :

ICSR
King's College London
Strand
Londres WC2R 2LS
Royaume-Uni

T. **+44 20 7848 2098**
E. **mail@gnet-research.org**

Twitter : **@GNET_research**

Ce rapport peut, comme toutes les autres publications du GNET, être téléchargé gratuitement à partir du site Internet du GNET : www.gnet-research.org.