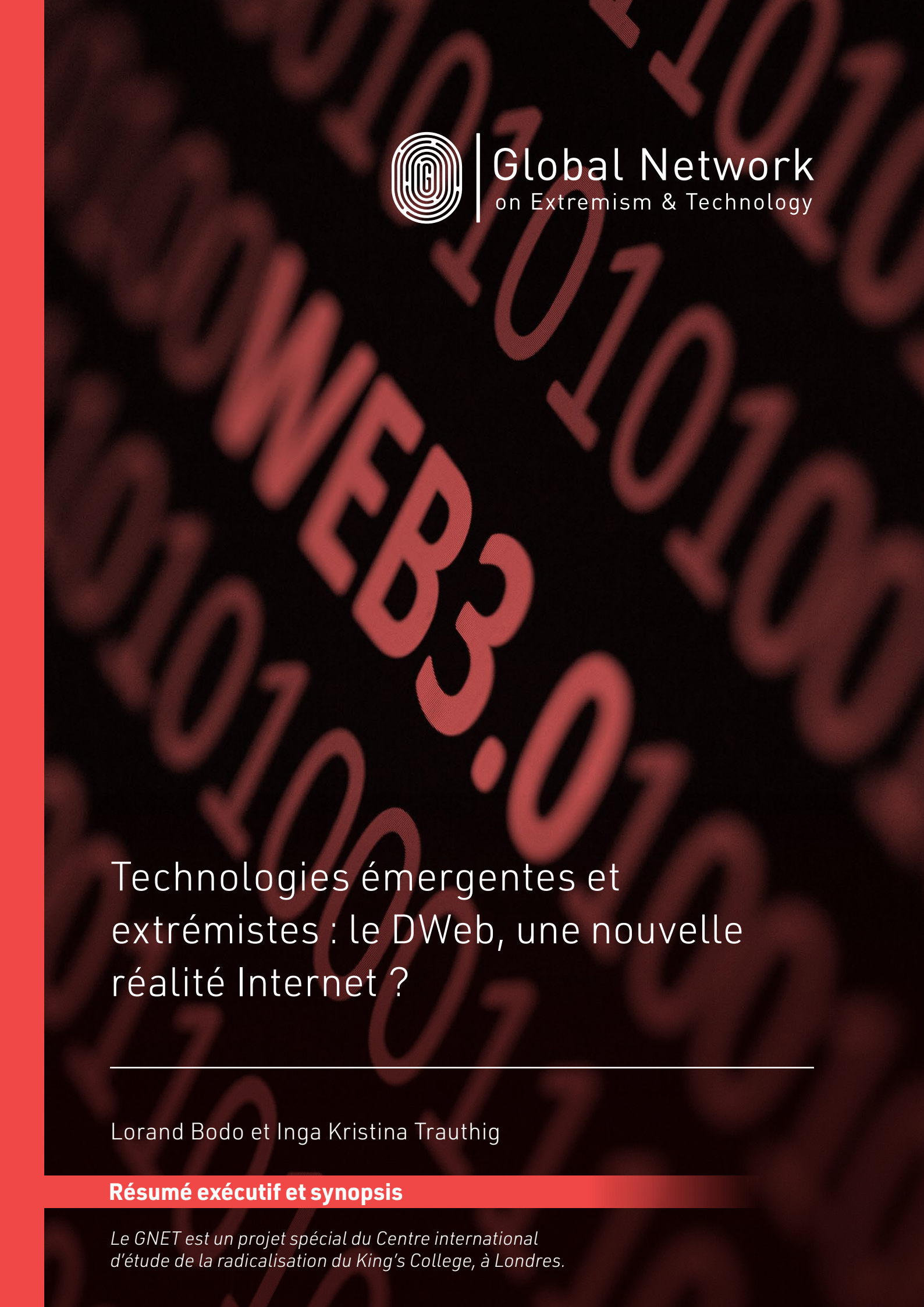

Technologies émergentes et extrémistes : le DWeb, une nouvelle réalité Internet ?

Lorand Bodo et Inga Kristina Trauthig

Résumé exécutif et synopsis

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

Ce rapport a été coécrit par Lorand Bodo et Inga Kristina Trauthig.

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

Depuis sa création par Sir Tim Berners-Lee en 1989, le World Wide Web s'est transformé en un écosystème dont les milliards d'utilisateurs dépendent d'un nombre relativement faible d'entreprises gigantesques. Ces sociétés proposent des services bénéfiques à ces milliards d'Internautes, prenant la forme par exemple de moteurs de recherche, de réseaux sociaux ou encore d'outils de communication ou de stockage de données sur le nuage. Mais le pouvoir des utilisateurs s'est aussi intensifié à mesure que leur nombre grandissait. Le transfert du pouvoir de cette poignée de très grandes entreprises vers les cybernautes est fondamental pour les défenseurs du web décentralisé (DWeb). Mais cette « redécentralisation » doit aussi donner aux utilisateurs plus de contrôle sur leurs données. Il va de soi que les groupes extrémistes s'intéressent de près au DWeb, puisqu'ils tentent d'innover et de trouver des solutions inventives pour diffuser leur propagande et mieux résister aux suppressions de comptes et de contenu. Nous proposons dans ce rapport un aperçu de la situation actuelle du DWeb et traitons de son exploitation effective et potentielle par les extrémistes. Nous nous intéressons particulièrement aux groupes d'extrême droite et à l'autoproclamé État islamique, puisqu'il a été prouvé que ces deux ensembles d'extrémistes présentent le potentiel de menace le plus élevé dans de nombreuses régions. Nous analysons un échantillon de trente canaux Telegram qui répondent aux caractéristiques que nous avons définies comme relevant du spectre des groupes d'extrêmes droite. Le deuxième jeu de données, fourni par le partenariat public-privé Tech Against Terrorism, appuyé par les Nations Unies, soumet l'exploitation du DWeb par l'autoproclamé État islamique à un examen critique.

L'examen de la littérature, les entretiens menés et les données analysées nous amènent aux conclusions suivantes :

- Puisque les extrémistes cherchent à exploiter n'importe quelle technologie, il n'est pas surprenant que le DWeb n'échappe pas à leurs investigations. Le DWeb est une technologie attrayante notamment parce que les contenus hébergés « sur le DWeb » ne peuvent être supprimés, puisqu'il n'est contrôlé par aucune autorité centrale.

- Toutefois, notre analyse révèle que ces acteurs se tournent encore de préférence vers d'autres technologies.

- Globalement, le risque d'exploitation des services du DWeb par les groupes d'extrême droite et l'État islamique est modéré.

- Par ailleurs, le DWeb n'est pas forcément nécessaire pour faciliter l'hébergement, la diffusion et le contrôle de contenus par les groupes extrémistes, puisque les services nécessaires pour y parvenir existent déjà.

- Enfin, les services du DWeb peuvent atténuer le risque d'être exploités et ne constituent donc pas nécessairement un refuge sûr pour les extrémistes.

Synopsis

Les termes relatifs au web décentralisé (DWeb) qui circulent à l'heure actuelle, comme Web3 ou bitcoin, sont devenus des fourre-tout pour tout ce qui a à voir avec les blockchains et la cryptomonnaie. Globalement, les grandes questions portant sur le web décentralisé s'articulent autour de deux thématiques principales : (1) Le web décentralisé est-il suffisamment viable et attrayant pour un nombre suffisant de personnes ? et (2) Quelle est la nature de ce « nouvel Internet » ? En d'autres termes, le web décentralisé évitera-t-il les écueils du web actuel ? Ce dernier est souvent tenu responsable de la radicalisation en ligne ou du renforcement de l'autoritarisme. Le DWeb pourrait au contraire favoriser les aspects positifs du web, en permettant par exemple aux activistes de s'organiser à l'abri de la censure des régimes.

Le présent rapport tente de répondre à ces deux questions en s'interrogeant sur l'usage que réservent les extrémistes au DWeb, et sur l'usage qu'ils pourraient en faire à l'avenir. Pourquoi le web décentralisé est-il une force du « bien » ou du « mal » ? Pourquoi y a-t-on recours ? La petite proportion de gens qui en abusent met-elle déjà en péril cette version d'Internet ? Que pourraient prendre en compte dans leur réflexion les développeurs au vu des données probantes dont nous disposons à l'heure actuelle ? Que doivent garder en tête les décideurs politiques lorsqu'ils légifèrent sur les technologies ? Les angles possibles envisagés par les chercheurs et les journalistes concernant le DWeb sont nombreux et vont des questions portant sur l'économie politique aux ramifications normatives d'un principe éthique partagé par les développeurs du Web3 selon lequel on ne peut pas faire confiance au « Big Tech ». Ce rapport s'intéresse aux implications pour les extrémistes et aux conséquences en matière de sécurité pour les sociétés dans leur ensemble.

Une stratégie en trois temps a guidé notre méthode de recherche. Dans un premier temps, nous avons procédé à un examen systématique de la littérature relative au DWeb, en nous concentrant en particulier sur la modération de contenu et l'extrémisme. Nous avons ensuite collecté et collationné les données prouvant l'utilisation du DWeb par les groupes d'extrême droite et l'État islamique. Enfin, nous avons mené des entretiens semi-structurés avec des défenseurs, détracteurs et développeurs du DWeb pour mieux comprendre ce sujet en pleine évolution. La nature exploratoire de ce rapport est directement liée au fait que le DWeb constitue plus une idée qu'une réalité pour une grande majorité de la population mondiale.

Dans le contexte de l'extrémisme violent et du terrorisme en ligne, l'un des risques majeurs est que les technologies du DWeb soient exploitées pour stocker ou extraire des données. Dans ce cas, « […] les méthodes décentralisées de stockage de données pourraient rendre la censure très difficile, voire pratiquement impossible »[1]. Il serait alors difficile de supprimer les contenus extrémistes, qui seraient alors accessibles à toute personne sachant où les trouver.

Nous avons conclu, à l'issue de notre examen de la littérature, que les groupes extrémistes avaient repéré les technologies du DWeb depuis un bon moment, mais que leurs caractéristiques limitatives et leur portée limitée en avaient limité l'exploitation par ces entités. La principale préoccupation porte toutefois sur le fait que le développement global du DWeb pourrait aller de pair avec une exploitation accrue de cette technologie par les extrémistes.

Concernant les groupes d'extrême droite, les données nous ont amenés à quatre conclusions :

1) Les services de DWeb ne sont pas représentés de façon significative.
2) La plupart des liens sortants mènent à deux grands réseaux sociaux.
3) L'échantillon de sympathisants d'extrême droite a partagé plus de liens vers des blogs et informations non fiables que vers des sources d'information fiables.
4) Les services d'archivage sont tout autant utilisés que les services de DWeb.

Concernant l'État islamique, les données nous ont amenés à trois conclusions :

1) Les services décentralisés sont exploités, mais pas autant que les services centralisés.
2) Les services d'hébergement et de partage de fichiers sont des cibles de choix.
3) Il y a plus de contenu terroriste vérifié sur les services d'hébergement et de partage, d'archivage et de collage de fichiers que sur les réseaux sociaux.

1 Barabas, Chelsea, Neha Narula et Ethan Zuckerman. « Defending Internet Freedom through Decentralization: Back to the Future? » The Center for Civic Media et The Digital Currency Initiative MIT Media Lab, août 2017. https://static1.squarespace.com/static/59aae5e9a803bb10bedeb03e/t/59ae908a46c3c480db42326f/1504612494894/decentralized_web.pdf.

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.