AYETA!

BOÎTE À OUTILS SUR LES DROITS NUMÉRIQUES

Kingdom of the Netherlands

PARADIGM INITIATIVE

Stanford PACS

AYETA

BOÎTE À OUTILS SUR LES DROITS NUMÉRIQUES

Publié par Paradigm Initiative

Publié en avril 2024

Chercheurs: Khadijah El-Usman, Ihueze Nwobilor, Angela Onyegbuna, Bridgette Ndlovu, Miriam Wanjiru et Sani Suleiman
Assistants de recherche: Dinchi Ikpa, Ifiokobong Uko et Joshua Oke
Édité par: Khadijah El-Usman 'Gbenga Sesan
Rédacteur en chef: Izak Minnaar
La traduction de la langue:
Conception et mise en page: Kenneth Oyeniyi

AVANT-PROPOS

Alors que les défenseurs des droits numériques s'inquiètent de plus en plus de leur sécurité numérique, il est essentiel qu'ils prennent des mesures pour se protéger dans l'exercice de leurs fonctions. Les conseils de sécurité numérique mis à jour et les mesures de prévention contre les menaces potentielles sont inclus dans cette nouvelle version de la boîte à outils Ayeta. Il comprend également des listes d'acteurs de la sécurité numérique, des événements pertinents sur les droits numériques sur le continent, des liens vers des études de cas sur la sécurité numérique de certains pays africains, des modèles de notes d'orientation et des modèles de déclarations de coalition. Une section de la boîte à outils est consacrée aux perturbations du réseau, à ce que vous pouvez faire pour contourner les perturbations, à la manière de conserver des enregistrements et aux ressources de plaidoyer pour de tels incidents.

La première boîte à outils a été développée dans le cadre d'un projet de bourse de recherche de la société civile numérique de Stanford 20201, avec le soutien supplémentaire du Fonds néerlandais pour les droits de l'homme. « Gbenga Sesan, assisté de Bonface Witaba, a dirigé la coordination du projet, l'élaboration du programme, la rédaction et l'édition, avec le soutien de l'équipe de Paradigm Initiative.

Nous sommes reconnaissants envers les partenaires du PIN qui nous ont fait part de leurs commentaires sur la manière d'améliorer l'édition précédente, et leurs idées utiles nous ont

1 https://pacscenter.stanford.edu/person/gbenga-sesan/

aidé à améliorer la boîte à outils pour le monde d'aujourd'hui. Beaucoup de travail a été consacré à la recherche et à la mise à jour de la boîte à outils, et c'était pris en charge par les membres de l'équipe PIN Angela Onyegbuna, Sani Suleiman, Khadijah El-Usman, Bridgette Ndlovu, Ihueze Nwobilor, Joshua Oke et Miriam Wanjiru. Nous apprécions le travail de révision effectué par Izak Minnaar. Judith Ogutu, Giyo Ndzi et Samuel Ojezele du PIN ont dirigé les travaux sur l'enquête, tandis que Kenneth Oyeniyi et David Chima se sont occupés de la conception.

Les liens ont été révisés par Dinchi Ikpa, Ifiokobong Uko et Angela Onyegbuna et cette version de la boîte à outils a été éditée par Khadijah El-Usman, Angela Onyegbuna et 'Gbenga Sesan.

Cette boîte à outils est conçue dans le but primordial de répondre au besoin croissant de protéger les défenseurs des droits numériques, les journalistes, les lanceurs d'alerte et autres personnes travaillant avec des informations sensibles dans les pays du Sud. PIN s'engage à garantir qu'il reste une ressource vivante en publiant des versions mises à jour. Nous comptons sur vos commentaires pour y parvenir – veuillez envoyer vos commentaires, vos idées, critiques et histoires à hello@ayeta.africa.

« Les conseils de sécurité numérique mis à jour et les mesures de prévention contre les menaces potentielles sont inclus dans cette nouvelle version de la boîte à outils Ayeta »

TABLE DES MATIÈRES

CHAPITRE I DROITS NUMÉRIQUES

L'avènement d'Internet et son ouverture au monde en 1989 ont vu les défenseurs des droits humains innover dans leur utilisation des espaces en ligne pour faire progresser la liberté d'expression, la liberté d'association en ligne, ainsi que pour renforcer la capacité d'une société numérique. Internet est aujourd'hui considéré comme un bien social, connectant plus de la moitié du monde. Cependant, la situation est devenue de plus en plus instable et les défis posés aux militants, aux défenseurs des droits humains, aux dissidents et aux journalistes sont en augmentation. Les régimes autoritaires ont eu recours à des outils et tactiques numériques tels que les coupures d'Internet, la censure en ligne et la surveillance numérique pour réprimer la liberté d'expression.

Comme le documente le rapport 2019 sur les droits numériques en Afrique de Paradigm Initiative,[2] « au cours de la dernière décennie, l›impact des organisations africaines défendant les droits numériques a augmenté — connectivité Internet abordable et de qualité, de

2 https://paradigmhq.org/report/digital-rights-in-africa-2019
3 https://paradigmhq.org/wp-content/uploads/2023/04/Londa-2022.pdf

confidentialité, liberté d›opinion, d›expression et d›association, entre autres. Contrairement à cette renaissance des droits numériques parmi les citoyens du continent, la vision des gouvernements africains concernant le rôle de la connectivité Internet et de l'accès numérique sur le continent a consisté en grande partie à conserver le pouvoir et le contrôle politiques par tous les moyens. L'instinct dominant a été en grande partie de subordonner les droits et l'accès afin de conserver le contrôle politique sur les citoyens. Le rapport Londa 2022 sur les droits numériques et l›inclusion en Afrique[3] met en lumière de nouveaux problèmes qui se posent: « les technologies émergentes comme l'intelligence artificielle (IA) gagnent du terrain, sont connues et adoptées de plus en plus sur le continent » ainsi que « la confidentialité et la gouvernance des données et le manque de responsabilité et de surveillance.

Un rapport de 2022 d'Access Now a révélé le nombre le plus élevé jamais enregistré de coupures d'Internet en une seule année : 35 pays dans le monde ont connu des coupures d'Internet. Parmi eux, sept se trouvaient en Afrique (Burkina Faso, Éthiopie, Sierra Leone, Nigéria, Somaliland, Ouganda et Zimbabwe). L'année précédente a notamment été marquée par des coupures d'Internet dans 12 pays africains.[4]

Les actions de ces pays contreviennent directement au principe 38.2 (« Les *États ne s'engageront ni ne toléreront aucune perturbation de l'accès à Internet et aux autres technologies numériques pour des segments du public ou une population entière. »)* de la Déclaration de principes de 2019 sur la liberté d'expression. Expression et accès à l'information en Afrique publiée par la Commission africaine[5] des droits de l'homme et des peuples (la Déclaration CADHP de 2019), ainsi que la Déclaration universelle des droits de l'homme.[6]

1.1

Que sont les droits numériques ?

Les droits numériques sont fondamentalement des droits humains à l'ère d'Internet. Les droits à la vie privée en ligne et à la liberté d'expression, par exemple, sont en réalité des extensions des droits égaux et inaliénables énoncés dans la Déclaration universelle des droits de l'homme des Nations Unies.[7] Les droits numériques concernent les droits des individus à accéder à l'ordinateur et à la capacité d'utiliser et de publier des contenus numériques. Il fait référence aux autorisations accordées pour une utilisation équitable du matériel numérique et au droit à la vie privée. Selon l'ONU, déconnecter les gens d'Internet viole ces droits et va à l'encontre du droit international.[8]

En outre, le préambule de la Déclaration CADHP de 2019 affirme que les mêmes

4 https://www.accessnow.org/wp-content/uploads/2023/03/2022-KIO-Report-Africa.pdf
5 https://achpr.au.int/en/node/902
6 https://www.un.org/en/about-us/universal-declaration-of-human-rights
7 https://www.un.org/en/about-us/universal-declaration-of-human-rights
8 https://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf

droits dont jouissent les personnes hors ligne doivent être protégés en ligne, et reconnaît que l'exercice des droits de liberté d'expression et d'accès à l'information via Internet est essentiel à la jouissance d'autres droits et essentiel pour réduire la fracture numérique[9] — appliquer efficacement les droits d'accès à l'information et de liberté d'expression de l'article 9 de la Charte africaine des droits de l'homme et des peuples pour être efficace à l'ère numérique.

1.2.

Chartes, déclarations, protocoles et traités numériques/des droits de l'homme

Les droits de l'homme s'appliquent à toutes les interactions humaines, que ce soit en ligne ou hors ligne, comme indiqué ci-dessus. Les principes consacrés dans les droits numériques et les droits de l'homme en général doivent être synchronisés pour s'appliquer à l'ensemble de l'environnement Internet et à l'éventail des domaines d'élaboration des politiques Internet.

Déclaration des droits de l'homme des Nations Unies[10]

La Déclaration universelle des droits de l'homme (DUDH) est un document marquant dans l'histoire des droits de l'homme. Rédigée par des représentants issus de milieux juridiques et culturels différents de toutes les régions du monde, la Déclaration a été proclamée par l'Assemblée générale des Nations Unies à Paris le 10 décembre 1948 (résolution 217 A de l'Assemblée générale) comme une norme commune à atteindre pour tous les peuples et tous les pays. Il énonce les droits humains fondamentaux qui doivent être universellement protégés et a été traduit dans plus de 500 langues.

Charte africaine des droits de l'homme et des peuples[11]

La Charte africaine des droits de l'homme et des peuples (également connue sous le nom de Charte de Banjul) est un instrument multilatéral des droits de l'homme destiné à promouvoir et à protéger les droits de l'homme et les libertés fondamentales sur le continent africain. La Charte a été adoptée le 1er juin 1981, est entrée en vigueur le 21 octobre 1986 et reste l'instrument essentiel des droits de l'homme de l'Union africaine (UA). La Charte a créé la Commission africaine des droits de l'homme et des peuples pour superviser la mise en œuvre des droits individuels et des droits socio-économiques, civils et politiques couverts par la Charte.[12]

La Convention de Malabo[13]

La Convention de l'UA sur la cybersécurité et la protection des données personnelles, aussi connue sous le nom de Convention de Malabo, est le seul traité régional contraignant sur la protection des données en dehors de l'Europe. Il est entré en vigueur le 8 juin 2023 après avoir été ratifié par 15 États, neuf ans

9 https://achpr.au.int/en/node/902
10 https://www.un.org/en/about-us/universal-declaration-of-human-rights
11 https://au.int/en/treaties/african-charter-human-and-peoples-rights
12 https://achpr.au.int/en
13 https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection

après son adoption le 27 juin 2014. Le pacte offre un cadre holistique à l'échelle du continent pour harmoniser les politiques en matière de protection des données, de droits numériques, de confidentialité et de liberté sur Internet. La convention de Malabo vise, entre autres, à atteindre deux objectifs majeurs. Premièrement, il exige que les États membres établissent un cadre juridique adéquat qui protège les droits fondamentaux et les données personnelles. Deuxièmement, elle cherche à équilibrer les droits nécessaires des personnes concernées avec ceux des prérogatives de l'État et des droits des communautés locales.[14]

Déclaration de principes de la CADHP sur la liberté d'expression et l'accès à l'information en Afrique[15]

La Déclaration CADHP de 2019 remplace la Déclaration de 2002 sur la liberté d'expression en Afrique et comprend de nouvelles sections sur l'accès à l'information et les droits en ligne, guidées par des normes de droit dur et de droit doux tiré des instruments et normes africains et internationaux des droits de l'homme, y compris la jurisprudence des instances judiciaires africaines. La Déclaration comprend des principes sur les obligations des États en matière de protection des droits en ligne, de fourniture d'un accès universel, équitable, abordable et significatif à Internet, de protection des informations personnelles en ligne et de surveillance des communications.

Cadre politique de l'Union africaine en matière de données[16]

Le cadre politique des données de l'UA (DPF) publié en juillet 2022 est l'un des instruments les plus importants en matière de gouvernance des données sur le continent. Développé par la Commission de l'UA en consultation avec des partenaires à l'intérieur et à l'extérieur de l'écosystème de l'UA, le DPF a été approuvé par le Conseil exécutif de l'UA en février 2022. Le DPF est un plan détaillé visant à guider les efforts des pays africains pour établir des régimes efficaces de gouvernance des données afin de tirer parti de l'évolution des données et révolution numérique. Comme la plupart des instruments politiques régionaux et internationaux, le DPF n'est pas juridiquement contraignant pour les États membres de l'UA. Il s'agit néanmoins d'une source de référence faisant autorité pour les gouvernements et les défenseurs de la révolution des données en Afrique.[17]

Déclaration africaine sur les droits et libertés de l'Internet[18]

La Déclaration africaine sur les droits et libertés de l'Internet (AfDec) est une initiative dirigée par une coalition panafricaine de la société civile visant à promouvoir les normes des droits de l'homme et les principes d'ouverture dans la formulation et la mise en œuvre des politiques Internet sur le continent. La Déclaration vise

14 https://www.ejiltalk.org/the-african-unions-malabo-convention-on-cyber-security-and-personal-data-protection-enters-into-force-nearly-after-a-decade-what-does-it-mean-for-data-privacy-in-africa-or-beyond/
15 https://achpr.au.int/en/node/902
16 https://au.int/sites/default/files/documents/42078-doc-AU-DATA-POLICY-FRAMEWORK-ENG1.pdf
17 https://cipesa.org/wp-content/files/briefs/Five_Takeaways_From_the_2022_African_Union_Data_Policy_Framework_Brief.pdf
18 https://africaninternetrights.org/about/

à développer les principes nécessaires au respect des droits de l'homme et des peuples sur Internet, et à cultiver un environnement Internet qui puisse répondre au mieux aux besoins et objectifs de développement social et économique de l'Afrique. L'AfDec s'appuie sur des documents africains bien établis relatifs aux droits de l'homme, notamment la Charte africaine des droits de l'homme et des peuples, la Déclaration de Windhoek sur la promotion des médias indépendants et pluralistes[19] de 1991, la Charte africaine de l'audiovisuel[20] de 2001, la Déclaration de principes initiale sur la liberté d'expression en Afrique de 2002 et la Déclaration de la Plateforme africaine sur l'accès à l'information[21] de 2011.

Déclaration de l'Union africaine sur la gouvernance de l'Internet[22]

La Déclaration de l'UA de 2017 sur la gouvernance de l'Internet a été élaborée dans le cadre d'un processus consultatif dans le but d'utiliser les avantages de l'économie numérique pour créer un environnement propice permettant aux parties prenantes africaines de délibérer sur les questions émergentes critiques et de contribuer au développement de politiques publiques de l'Internet qui prennent en compte des besoins de l'Afrique. La Déclaration sert de principes directeurs pour les parties prenantes et constitue les valeurs partagées pour les délibérations sur l'avenir de l'Internet d'un point de vue africain.

1.3.

Traités sous-régionaux

L'Afrique compte diverses organisations sous-régionales, généralement appelées CER (communautés économiques régionales), il s'agit de

- La Communauté de Développement de l'Afrique Australe (SADC)
- De l'Autorité Intergouvernementale pour le Développement (IGAD),
- De la Communauté Economique des États de l'Afrique Centrale (ECCAS),
- L'Union du Maghreb Arabe (UMA), la Communauté des États Sahélo-Sahariens (CEN-SAD),
- Le Marché Commun de l'Afrique Orientale et Australe (COMESA),
- La Communauté de l'Afrique de l'Est (EAC) et
- La Communauté Economique des États de l'Afrique de l'Ouest (CEDEAO).

Certaines de ces communautés ont leurs propres traités tels que la Politique régionale de protection des infrastructures critiques de la CEDEAO[23] et la Directive de la CEDEAO sur la cybercriminalité (adoptée en 2011), le

19 https://www.veritaszim.net/sites/veritas_d/files/Windhoek-Declaration%281%29.pdf
20 http://www.mediaombudsmannamibia.org/pdf/African_Charter_on_Broadcasting.pdf
21 https://www.africanplatform.org/fileadmin/Content/PDF/APAI-Declaration-English.pdf
22 https://au.int/sites/default/files/newsevents/workingdocuments/33025-wd-african_declaration_on_internet_governance_en_0.pdf
23 https://www.ocwarc.eu/wp-content/uploads/2021/02/ECOWAS-Regional-Critical-Infrastructure-Protection-Policy-EN.pdf

cadre politique modèle des TIC de la CAE[24], et la SADC a une loi type sur la criminalité informatique et la cybercriminalité (2012).[25]

1.4.

Lois du pays

Au niveau des États, certains aspects de ces chartes, déclarations et protocoles sont appliqués par les lois sur les droits de l'homme, les lois nationales sur la protection des données et parfois les lois sur la cybercriminalité. Selon les informations publiées par Data Protection Africa, en janvier 2024, 35 pays africains avaient adopté une législation nationale sur la protection des données et trois pays avaient rédigé des projets de loi sur la protection des données.[26]

24 https://eaco.int/admin/docs/publications/EAC_MODEL_ICT_POLICY.pdf
25 https://www.itu.int/en/ITU-D/Cybersecurity/Documents/SADC%20Model%20Law%20Cybercrime.pdf
26 https://dataprotection.africa/

1.5.

Acteurs de la sécurité numérique

De nombreux acteurs de la sécurité numérique ont pris des initiatives pour atténuer les vulnérabilités et les risques des journalistes et des défenseurs des droits humains. Ces organisations peuvent être contactées pour obtenir des conseils et/ou une assistance sur des questions liées aux violations de données, aux rapports d'incidence, aux questions de politique, etc.

Accédez Maintenant[27]

AccessNow fournit une ligne d'assistance téléphonique 24 heures sur 24 en matière de sécurité numérique, une analyse politique fondée sur des preuves, plaidoyer et des subventions aux organisations de base et aux groupes d'activistes qui travaillent avec les utilisateurs et les communautés les plus exposées aux violations des droits numériques.

Défenseurs africains[28]

Un réseau panafricain de défenseurs des droits humains regroupant cinq organisations sous-régionales africaines,[29] dédié à la promotion et à la protection des défenseurs des droits humains (DDH) à travers le continent africain.

Centre africain des droits numériques (African Digital Rights Hub - ADRH)[30]

Le Hub est un « groupe de réflexion et d'action » à but non lucratif qui promeut la recherche panafricaine et le renforcement des capacités en matière de droits numériques. Axé sur l'impact de la technologie numérique sur les personnes, le Hub rassemble des chercheurs universitaires, des parties prenantes, des décideurs politiques, des organismes régionaux et internationaux pour aborder les questions de droits numériques en Afrique.

Réseau Africain des Droits Numériques (African Digital Rights Network - ADRN)[31]

27 https://www.accessnow.org/
28 https://africandefenders.org/
29 https://africandefenders.org/members/
30 https://africadigitalrightshub.org/
31 https://www.africandigitalrightsnetwork.org/

Il s'agit d'un réseau d'activistes, d'universitaires et d'analystes qui mènent des recherches sur les droits numériques en Afrique. Ils réalisent des études inédites, produisent des rapports uniques et publient une série révolutionnaire de livres sur les droits numériques.

Africtivistes[32]

Un réseau panafricain d'activistes et de blogueurs en ligne pour la démocratie, comprenant une communauté de 200 cyberactivistes de 35 pays différents.

Association pour le progrès de la communication (APC)[33]

L'APC s'efforce de construire un monde dans lequel tous les individus ont un accès facile, égal et abordable au potentiel créatif des TIC pour améliorer leur vie et créer des sociétés plus démocratiques et égalitaires.

Association des femmes des médias au Kenya (Association of Media Women in Kenya - AMWIK)[34]

L'AMWIK est une association nationale de médias dont l'objectif est d'améliorer la visibilité des femmes dans la société et de promouvoir leur participation au leadership et à la prise de décision.

Association des avocats de la protection de la vie privée en Afrique (Association of Privacy Lawyers in Africa - APLA)[35]

L'APLA est une organisation fondée en 2022 avec pour mission de centraliser les efforts visant à définir, promouvoir et améliorer la profession juridique en matière de confidentialité des données dans tous les pays africains.

32 https://www.africtivistes.org/
33 https://www.apc.org/
34 http://amwik.org/
35 https://aplafrica.com/

Article 19[36]

L'article 19 – travaillant sur deux libertés imbriquées: la liberté de parler et la liberté de savoir – vise à permettre aux individus du monde entier de s'exprimer librement et de s'engager activement dans la vie publique sans crainte de discrimination.

CoCréation Hub Nigéria[37]

Communément appelé CC-HUB ou HUB, il s'agit d'une plate-forme avec laquelle des personnes orientées vers la technologie partagent des idées sur la résolution des problèmes sociaux au Nigeria et au-delà.

Collaboration sur la politique internationale des TIC pour l'Afrique orientale et australe (Collaboration on International ICT Policy for Eat and Southern Africa - CIPESA)[38]

Basée à Kampala, en Ouganda, CIPESA est une organisation politique sur Internet qui promeut des politiques et des pratiques efficaces et inclusives en matière de TIC pour améliorer la gouvernance, les moyens de subsistance et les droits de l'homme en Afrique.

Comité pour la protection des journalistes (CPJ)[39]

Une organisation non gouvernementale indépendante à but non lucratif, basée à New York, avec des correspondants dans le monde entier. Le CPJ promeut la liberté de la presse et défend les droits des journalistes du monde entier.

Cybersécurité Afrique[40]

Une société de conseil en sécurité de l'information proposant une gamme complète de services et de produits pour aider les organisations à protéger leurs précieux actifs.

36 https://www.article19.org/
37 https://cchub.africa
38 https://cipesa.org/
39 https://cpj.org/
40 https://www.cybersecurityafrica.com/

Coalition des défenseurs, Kenya[41]

Une coalition nationale au Kenya pour renforcer la capacité des défenseurs des droits humains à travailler efficacement et à réduire leur vulnérabilité au risque de persécution, notamment en plaidant pour un environnement juridique et politique favorable.

Société Numérique d'Afrique (Digital Society of Africa - DSA)[42]

La DSA s'efforce de renforcer la résilience et la capacité des militants de première ligne, des défenseurs des droits humains et d'autres groupes à risque dans la région à reconnaître et à répondre de manière indépendante aux menaces et attaques numériques.

Alliance de sécurité numérique (Digital Security Alliance - DSA)[43]

Une coalition d'organisations et d'experts individuels en sécurité numérique en Ouganda œuvrant à sécuriser les actifs numériques de la société civile, des défenseurs des droits humains, des journalistes et d'autres militants face aux menaces posées par de puissantes entreprises, des criminels sans scrupules, l'État et d'autres acteurs non étatiques.

Maison de la liberté[44]

Une organisation non gouvernementale à but non lucratif basée aux États-Unis qui mène des recherches et plaide en faveur de la démocratie, de la liberté politique et des droits de l'homme.

Défenseurs de première ligne[45]

Une organisation de défense des droits de l'homme fondée à Dublin, en Irlande, en 2001, pour protéger ceux qui travaillent de manière non violente pour faire respecter les droits humains d'autrui, tels qu'énoncés dans la Déclaration universelle des droits de l'homme.

41 https://defenderscoalition.org/
42 https://digitalsociety.africa/
43 https://www.defendersprotection.org/dsa/
44 https://freedomhouse.org/
45 https://www.frontlinedefenders.org/

Alliance gambienne pour la cybersécurité[46]

L'organisation vise à sensibiliser et à accroître la compréhension des Gambiens sur la cybersécurité, les cybermenaces, l'espionnage et à leur donner les moyens d'être plus en sécurité en ligne.

Union de la presse gambienne[47]

Le Syndicat de la Presse de Gambie est un syndicat de journalistes en Gambie, créé en 1978 par un groupe de journalistes, avec pour mission de promouvoir des médias libres et dynamiques.

Réseau des défenseurs des droits humains - Sierra Leone (Human Rights Defenders Network, Sierra Leone - HRDN-SL)[48]

HRDN-SL est une coalition d'organisations de la société civile de défense des droits de l'homme et d'individus travaillant pour la protection et la promotion des droits de l'homme en Sierra Leone.

Réseau d'action TIC du Kenya (Kenya ICT Action Network - KICTANET)[49]

Un groupe de réflexion multipartite pour les parties prenantes intéressées et impliquées dans la politique et la réglementation des TIC. Son travail est aidé par quatre piliers: le plaidoyer politique, le renforcement des capacités, la recherche et l'engagement des parties prenantes.

Fondation des Médias pour l'Afrique de l'Ouest (Media Foundation for West Africa - MFWA)[50]

Créée en 1997 et basée à Accra, au Ghana, la MFWA est une organisation non gouvernementale régionale qui promeut et défend le droit à la liberté d'expression de toutes les personnes, et particulièrement des médias et des défenseurs des droits de l'homme en Afrique de l'Ouest.

46 https://twitter.com/CyberGambia
47 https://gpu.gm/
48 https://grassrootsjusticenetwork.org/connect/organization/pan-african-human-rights-defenders-network/
49 https://www.kictanet.or.ke
50 https://www.mfwa.org/

Défense des médias[51]

Une organisation non gouvernementale créée en 2008 pour fournir une assistance juridique aux journalistes et aux médias indépendants. Il soutient également la formation en droit des médias et promeut l'échange d'informations, d'outils contentieux et de stratégies pour les avocats travaillant sur des affaires de liberté des médias.

Initiative Paradigme (PIN)[52]

PIN est une entreprise sociale qui construit un système de soutien basé sur les TIC et défend les droits numériques afin d'améliorer les moyens de subsistance des jeunes mal desservis. Le programme de défense des droits numériques de PIN se concentre sur le développement de politiques publiques en faveur de la liberté sur Internet en Afrique.

PaixFemmes[53]

Le programme Femmes, paix et sécurité de la Ligue internationale des femmes pour la paix et la liberté (Women's International League for Peace and Freedom - WILPF)[54], une organisation féministe mondiale de consolidation de la paix.

Politique[55]

Un collectif féministe de technologues, de data scientists, de créatifs et d'universitaires travaillant à l'intersection des données, du design et de la technologie pour créer de meilleures expériences de vie en influençant une culture d'utilisation responsable des données, promouvoir des pratiques appropriées de gouvernance des données et plaider en faveur de politiques qui soutiennent un écosystème de données favorable.

Sœurs en sécurité [56]

Safe Sisters (Sœurs en sécurité) est un programme de bourses destiné aux

51 https://www.mediadefence.org/
52 https://paradigmhq.org/
53 https://www.peacewomen.org/
54 http://wilpf.org/
55 https://pollicy.org/
56 https://safesisters.net/

femmes, défenseures des droits humains, journalistes, travailleuses des médias et militantes. Les boursiers sont formés pour comprendre et répondre aux défis de sécurité numérique auxquels ils sont confrontés dans leur travail et leur vie quotidienne.

Réseau des femmes ougandaises (Women of Uganda Network - WOUGNET) [57]

WOUGNET promeut l'utilisation des technologies de l'information et de la communication parmi les femmes et les filles comme outils pour partager des informations et aborder des questions telles que l'égalité des sexes et le développement durable.

Fondation zambienne de l'Initiative de Cybersécurité (Zambian Cyber Security Initiative Foundation) [58]

Le ZCSI est une organisation qui fournit des connaissances et des outils pour rester en sécurité dans le monde numérique d'aujourd'hui et protéger les individus et les organisations contre les dommages causés par les cybermenaces.

57 https://wougnet.org
58 https://zcsi-foundation.org/

1.6.

Événements sur les droits numériques

Chaque année, dans toute l'Afrique, un certain nombre d'événements sur les droits et la sécurité numériques sont organisés, réunissant des parties prenantes d'horizons différents pour discuter de questions politiques, de tendances émergentes et proposer des formations pratiques.

École africaine sur la gouvernance de l›Internet (African School on Internet Governance - AfriSIG)[59]

Une initiative de formation multipartite qui vise à donner aux Africains l'opportunité d'acquérir les connaissances et la confiance nécessaires pour participer efficacement aux processus et aux débats sur la gouvernance de l'Internet aux niveaux national, régional et mondial.

D'autres écoles de gouvernance de l'Internet aux niveaux régional et national comprennent :

- École de gouvernance de l›Internet en Afrique de l›Ouest (WASIG)[60]
- École de gouvernance de l›Internet du Kenya (KeSIG)[61]
- École nigériane sur la gouvernance de l›Internet (NSIG)[62]
- École de gouvernance de l›Internet du Soudan du Sud (SSSIG)[63]
- École des femmes d›Arusha pour la gouvernance de l›Internet (AruWSIG)[64]

Forum sur les droits numériques et l'inclusion (Digital Rights and Inclusion Forum - DRIF)[65]

DRIF est un forum bilingue organisé chaque avril par Paradigm Initiative où des questions mondiales d'actualité difficiles concernant les droits de l'Internet, en particulier en Afrique, sont discutées entre la société civile, les entreprises technologiques, le gouvernement, le monde universitaire et d'autres parties prenantes.

Forum sur la liberté d'Internet en Afrique (Forum on Internet Freedom in Africa - FIFAfrica)[66]

Organisé chaque année en septembre par le CIPESA,[67] le FIFAfrica se concentre sur la promotion d'un Internet libre et ouvert en

59 https://afrisig.org/
60 https://waigf.org/about-wasig/
61 https://kigf.or.ke/kesig/
62 https://sig.ng/
63 https://ssigf.org.ss/about-ss-sig/
64 https://www.ksgen.or.tz/aruwsig/
65 https://drif.paradigmhq.org/
66 https://internetfreedom.africa/
67 https://cipesa.org/service/forum-on-internet-freedom-in-africa/

Afrique.

7. Études de cas sur les droits numériques

Les tentatives des États visant à violer les droits des journalistes et des défenseurs des droits numériques par le biais de lois, de coupures d'Internet et de poursuites judiciaires, entre autres moyens, sont illustrées par les exemples suivants à travers l'Afrique:

Cameroun: Dans ce pays, il est impossible pour un média d'adopter une politique éditoriale critique et indépendante sans s'exposer à des menaces et à un harcèlement importants si ses reportages mettent en danger les intérêts du gouvernement et de ses représentants. Cet environnement répressif alimente l'autocensure et conduit la plupart des médias à se rallier aux opinions des autorités ou de leurs proches. Les journalistes camerounais, en particulier ceux qui critiquent ou s'expriment ouvertement, sont constamment exposés au risque d'agressions verbales ou physiques.

Par exemple, le corps gravement mutilé du journaliste Martinez Zogo a été retrouvé cinq jours après son enlèvement en janvier 2023.[68] En tant qu'animateur d'une émission de radio quotidienne populaire , Embouteillage (ou Gridlock en anglais), il s'attaque régulièrement à des affaires de corruption et de malversations présumées, n'hésitant pas à citer nommément des personnalités importantes. Le meurtre de Martinez Zogo a choqué de nombreuses personnes alors que les ONG ont continué de dénoncer les violations de la liberté de la presse et de la liberté d'expression.[69]

Égypte: Le 22 août 2023, des forces de sécurité de l'État en civil ont arrêté Gamal Abdelhamid Ziada, le père du journaliste égyptien indépendant basé en Belgique Ahmed Gamal Ziada, dans une rue de Gizeh, selon des informations et un tweet du journaliste.[70] Le lendemain, les procureurs ont accusé le père Gamal Ziada d'utilisation abusive des médias sociaux, de diffusion de fausses nouvelles et d'appartenance à un groupe interdit, et ont ordonné sa détention en attendant son procès. Ahmed Gamal Ziada couvre les questions relatives aux droits de l'homme et à la politique étrangère égyptienne pour des sites d'information régionaux indépendants, notamment Raseef, Daraj et Middle East Eye.[71] Le gouvernement égyptien a continué de faire taire les critiques en procédant à des arrestations et en poursuivant injustement des journalistes et des blogueurs, et le Parlement a adopté des lois très restrictives qui restreignent encore davantage la liberté d'expression et l'accès à l'information. En plus de recourir aux tribunaux de sûreté de l'État, dont les jugements ne peuvent faire l'objet d'un appel, les autorités continuent de poursuivre des milliers de civils devant les tribunaux militaires. Les deux systèmes judiciaires sont intrinsèquement abusifs et ne respectent pas les normes minimales d'une procédure régulière, selon

68 https://rsf.org/en/country/cameroon
69 Cameroonian prosecutors wind up probe into the murder of Martinez Zogo I Africanews
70 اعتقال والد الناشط المصري أحمد جمال زيادة
71 https://cpj.org/2023/08/egyptian-authorities-arrest-father-of-freelance-journalist-ahmed-gamal-ziada/

le rapport mondial 2019 de Human Rights Watch.[72]

Nigeria: La technologie de surveillance a été utilisée pour espionner des militants pacifiques, des hommes politiques de l'opposition et des journalistes, les accusant de harcèlement, d'arrestation et de torture, en violation du droit international des droits humains et des mesures d'auto-surveillance des fournisseurs. Le Nigeria est l'un des principaux clients de toutes les principales technologies de surveillance, y compris l'interception Internet et mobile, la surveillance des médias sociaux, les données d'identification biométriques et la surveillance dite « ville sûre » des citoyens dans les espaces publics.

Par exemple, Omoyele Sowore, militant des droits humains et ancien candidat à la présidentielle, a découvert que le gouvernement nigérian avait désactivé son identification biométrique en janvier 2022. Cela signifiait que sa carte d'identité nationale, sa carte d'électeur permanente, son passeport étranger et son permis de conduire figuraient parmi les documents désactivés, l'empêchant de voyager, de conduire ou de voter.[73]

Tanzanie: Selon un rapport du Département d'État américain de 2022 sur les pratiques en matière de droits de l'homme,[74] le 27 juin 2022, le gouvernement a envoyé une lettre à DarMpya Media accusant le média d'avoir dénaturé une manifestation du 17 juin devant l'ambassade du Kenya à Dar es Salaam, liée aux tensions entre les résidents Massaï et les autorités de Loliondo. Le gouvernement a accusé DarMpya d'opérer sans licence et a interdit au média de publier du contenu en ligne. DarMpya a demandé le renouvellement de sa licence de publication en août de la même année, ce qui a ensuite été refusé par l'Autorité tanzanienne de régulation des communications (Tanzania Communications Regulatort Authority - TCRA)

.

Ouganda: Le gouvernement ougandais a fermé l'accès à Internet et aux plateformes de réseaux sociaux lors des élections présidentielles et parlementaires de janvier 2021, entravant ainsi la communication et l'accès à l'information.[75]

Les données réseau de l'Observatoire Internet NetBlocks confirment les restrictions généralisées imposées aux réseaux sociaux et aux plateformes de communication en ligne par les principaux fournisseurs d'accès Internet en Ouganda à partir du mardi 12 janvier, deux jours avant les élections. Les conclusions de NetBlocks révèlent l'étendue des restrictions exigées par ordre [76] de la Commission ougandaise des communications avant les élections du 14.[77] Le black-out a été levé le lundi après les élections, plus de 100 heures après son imposition. Les autorités se sont excusées pour la gêne occasionnée et ont

72 https://www.hrw.org/world-report/2019/country-chapters/egypt
73 https://www.ids.ac.uk/press-releases/nigeria-spending-billions-of-dollars-on-harmful-surveillance-of-citizens/
74 https://www.state.gov/reports/2022-country-reports-on-human-rights-practices/tanzania/
75 https://www.hrw.org/world-report/2022/country-chapters/uganda
76 https://www.reuters.com/article/us-uganda-election/uganda-bans-social-media-ahead-of-presidential-election-idUSKBN29H0KH
77 https://www.business-humanrights.org/en/latest-news/uganda-shuts-down-internet-ahead-of-general-election/

déclaré que la fermeture avait pour but d'éviter toute ingérence extérieure dans les élections, que le leader de longue date, Yoweri Museveni, aurait remporté contre le chanteur populaire devenu homme politique Bobi Wine.[78]

1.8.

Modèles de notes d'orientation

Le rôle des défenseurs des droits numériques, des journalistes et autres militants sociaux est mieux apprécié lorsqu'ils sont perçus comme contribuant à apporter des solutions à la myriade de défis auxquels la société est confrontée.

Voici une boîte à outils[79] pour élaborer des notes de politique efficaces, et des exemples de telles notes de politique incluent:

- L'absence de l'Afrique dans les technologies émergentes[80]
- Évaluation du processus du cybertraité des Nations Unies[81]
- L'intelligence artificielle au Kenya[82]
- Censure et modération des contenus en Angola, en République centrafricaine et en République démocratique du Congo[83]
- Vers un plan d'action national inclusif sur les entreprises et les droits de l'homme au Nigeria[84]

1.9.

Modèles de déclarations de coalition

La volonté croissante des gouvernements africains de réglementer l'utilisation des médias sociaux par le biais de lois aux termes vagues ou larges sert à diminuer l'ouverture d'Internet, à masquer les violations des droits de l'homme et à créer des obstacles à la stabilité à long terme et au dialogue pacifique. La capacité de s'opposer à cette tendance est renforcée lorsque les parties prenantes s'unissent d'une seule voix. Voici des exemples de déclarations de coalition faites pour aborder de telles questions :

- Une lettre ouverte de 2023 signée par diverses organisations sur le blocage de Telegram au Kenya.[85]

- Une déclaration commune de 2023 au nom de 59 pays présentée au Conseil des droits de l'homme de l'ONU sur les risques accrus associés aux technologies de surveillance et l'importance des garanties dans l'utilisation de ces outils.[86]

- Un groupe international d'organisations et d'experts appelant le gouvernement indien à

78 https://www.reuters.com/article/us-uganda-internet-rights-trfn-idUSKBN29P1V8/
79 https://socialwork.utoronto.ca/wp-content/uploads/2021/06/Policy-Toolkit-Final-v2-Apr27.pdf
80 https://paradigmhq.org/report/policy-brief-africas-absence-in-emerging-technologies/
81 https://paradigmhq.org/report/policy-brief-assesing-the-united-nations-cybertreaty-process/
82 https://paradigmhq.org/report/policy-brief-artificial-inteligence-in-kenya/
83 https://paradigmhq.org/report/policy-brief-censorship-and-content-moderation-in-angola-central-african-republic-and-democratic-republic-of-congo/
84 https://paradigmhq.org/report/policy-brief-towards-an-inclusive-national-action-plan-on-business-and-human-rights-in-nigeria/
85 https://www.accessnow.org/press-release/open-letter-clarification-on-telegram-blocking-in-kenya/
86 https://freedomonlinecoalition.com/joint-statement-heightened-risks-associated-with-surveillance-technologies-and-the-importance-of-safeguards-in-the-use-of-these-tools/

retirer le projet de loi sur les télécommunications de 2023 et à protéger les droits fondamentaux.[87]

- Une déclaration de la NetRights Coalition condamnant les raids sur les technologies numériques des acteurs de la société civile au Zimbabwe lors des élections de 2023.[88]

Une déclaration de la NetRights Coalition de 2023 contre une réglementation générale des médias sociaux au Nigeria.[89]

87 https://www.accessnow.org/press-release/india-must-withdraw-the-telecommunications-bill-2023/
88 https://paradigmhq.org/press-release-the-netrights-coalition-condemns-raids-of-digital-technologies-of-civil-society-actors-in-zimbabwe-during-the-2023-elections/
89 https://paradigmhq.org/the-netrights-coalition-strongly-condemns-the-call-for-blanket-social-media-regulation-in-nigeria/

CHAPITRE II

SÛRETÉ ET SÉCURITÉ NUMÉRIQUES

La sécurité numérique, appelée indifféremment sécurité Internet, sécurité en ligne ou cybersécurité, fait référence à un ensemble de pratiques et de précautions suivies par un individu lorsqu'il utilise Internet dans le but de garantir que les informations personnelles sensibles et celles de son(ses) appareil(s) rester en sécurité.

Selon une infographie de 2023 « Que se passe-t-il en une minute Internet »[90], 241,2 millions de mails, 347 222 tweets et 18,8 millions de SMS sont envoyés toutes les 60 secondes. Alors que les statistiques[91] de l'UIT pour 2023 indiquent que plus de 5,4 milliards de personnes, soit 67 pour cent de la population mondiale, sont connectées en ligne, cela ne peut que signifier qu'il y a plus d'acteurs malveillants, de pirates informatiques, de menaces et d'escroqueries en ligne que jamais auparavant.

90 https://ediscoverytoday.com/2023/04/20/2023-internet-minute-infographic-by-ediscovery-today-and-ltmg-ediscovery-trends/
91 https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

Internet en 2023 chaque minute

2.1.

Menaces pour la sécurité numérique

Voici quelques menaces courantes en matière de sécurité numérique dont tout le monde doit être conscient.

Logiciel malveillant

Malware est l'abréviation de « logiciel malveillant ». Il s'agit d'un programme ou d'un fichier conçu pour être perturbateur, invasif et nuisible à un système informatique et à des appareils mobiles. Il est le plus souvent transmis via des pièces jointes à des e-mails, des messages instantanés (MI), des téléchargements, du phishing et des sites Web trompeurs. Les épidémies de logiciels malveillants causent des dommages en détruisant les données sur les appareils infectés et/ou en augmentant le trafic réseau, ce qui peut provoquer des pannes complètes du réseau. De plus, les logiciels malveillants peuvent permettre aux attaquants d'obtenir toutes les informations qu'ils souhaitent à partir d'un ordinateur compromis, y compris les informations personnelles, les données et les sources d'un journaliste.

Les types de logiciels malveillants incluent:

Adware - Il s'agit d'un type de logiciel qui s'installe de manière malveillante sur votre appareil et est conçu pour afficher des publicités et des pop-ups non sollicités.

Cryptojacking - Ce type de malware détourne un appareil dans le but de l'utiliser pour l'extraction de bitcoins, augmentant considérablement le traitement sur l'appareil, ce qui le ralentit et vide la batterie.

Ransomware - Type de malware conçu pour bloquer l'accès à tout ou partie d'un système informatique jusqu'à ce qu'une somme soit payée, bien que le paiement ne garantisse pas que l'accès sera restauré. Étant donné que les attaquants cherchent à maximiser leur salaire, les cibles sont généralement des entités plus grandes (organisations, départements, collèges, entreprises) qui non seulement sont susceptibles de disposer des fonds, mais qui subissent également une perte importante lorsqu'elles ne peuvent pas accéder à leurs systèmes. Cependant, les individus restent la cible des ransomwares, car ils peuvent constituer une porte d'entrée vers les systèmes d'une organisation.

Logiciel espion – Il s'agit d'un logiciel malveillant installé secrètement sur l'ordinateur ou l'appareil mobile d'une personne afin d'obtenir des informations privées sur son propriétaire, telles que des listes de sites Web visités, des mots de passe et des numéros de carte de crédit.[92]

Chevaux de Troie - Il s'agit de programmes trompeurs téléchargés de manière malveillante sur un appareil qui permettent à un cybercriminel d'accéder à distance à l'appareil hôte, soumettant l'appareil à diverses activités malveillantes ou destructrices, ou même simplement surveillant (espionnage) les activités ou les interactions sur l'appareil.

92 https://www.britannica.com/technology/spyware

Virus - Un type de malware qui s'attache à un autre programme et à la capacité de se propager entre les appareils et d'endommager les données et les logiciels. Si les virus ne sont pas stoppés rapidement, le flot d'e-mails peut submerger les serveurs, perturbant ainsi les services de messagerie pour tous.

Vers - Un ver informatique est un type de logiciel malveillant qui se réplique automatiquement lorsqu'il se propage à d'autres ordinateurs sur un réseau.

Indices d'une éventuelle infection par un logiciel malveillant sur votre appareil

- Fonctionnalité du système inhabituellement lente ou gelée.
- Spam et publicités pop-up.
- Pannes fréquentes du système.
- Icônes inconnues sur le bureau.
- Redirection d'un site Web populaire vers un site inconnu.
- Nouveaux fichiers ou dossiers créés sans votre autorisation.
- La batterie s'épuise rapidement.

Menaces liées à la surveillance numérique

Cela comprend la localisation, la reconnaissance faciale, la surveillance de masse et l'interception des communications. La surveillance a un effet néfaste sur la capacité des écrivains et des journalistes à rechercher et à publier des articles, et rend plus difficile la protection de leurs sources.

Attaques d'ingénierie sociale

L'ingénierie sociale est une technique utilisée pour inciter les utilisateurs à divulguer certaines informations, à effectuer une action spécifique pour des raisons illégitimes ou à fournir un point d'entrée à des logiciels malveillants. Il peut s'agir d'une tentative par un inconnu d'extraire de vous des informations que vous ne partageriez normalement pas en ligne, par exemple les détails de votre carte de crédit, votre date de naissance, votre lieu de vacances préféré, le nom de votre animal. Ont-ils vraiment besoin de ces informations ? Les réponses à ces questions peuvent entraîner la compromission des comptes.

Certaines formes d'ingénierie sociale comprennent:

- **Attaques de phishing** – Les campagnes de « phishing » ou de « spear phishing » utilisent souvent des liens ou des pièces jointes dans des e-mails ou sur les réseaux sociaux contenant des logiciels malveillants. Une fois ces liens cliques, ils peuvent causer des dégâts importants.[93]
- **Smishing** – Également connu sous le nom de phishing par SMS, il s'agit d'un type d'attaque d'ingénierie sociale menée via des messages SMS. Dans le cadre de cette attaque, les fraudeurs tentent d'inciter l'utilisateur à cliquer sur un lien qui

93 https://www.exabeam.com/information-security/cyber-security-threat/

le mène vers un site Web malveillant.[94]

- **Vishing** – Une forme de phishing dans laquelle des individus sont amenés à divulguer des informations sensibles par téléphone ou par messagerie vocale.[95]
- **Appâtage** – Une forme d'attaque d'ingénierie sociale dans laquelle les fraudeurs offrent quelque chose de valeur à la victime en échange de la fourniture par celle-ci d'informations personnelles sensibles. Par exemple, la victime peut recevoir un e-mail lui promettant une carte-cadeau gratuite en échange d'un clic sur un lien.[96]
- **Pretexting** — type d'ingénierie sociale dans lequel les cybercriminels se font passer pour une source fiable pour convaincre les victimes de partager des informations précieuses ou sensibles.[97]

Fausses attaques de domaine

Il s'agit de sites Web créés pour usurper l'identité de sites Web légitimes à des fins malveillantes. Les médias indépendants et les sites Internet de la société civile en étaient souvent victimes. Les faux sites diffusent des logiciels malveillants ou publient de fausses informations dans le but de discréditer le véritable site médiatique ou un journaliste en particulier.

Attaques de l'homme du milieu (Man-in-the-Middle - MitM)

Une attaque de l'homme du milieu est une cyberattaque dans laquelle l'attaquant peut secrètement intercepter des messages entre deux ou plusieurs parties croyant communiquer entre elles.[98] Par exemple, un routeur sans fil est configuré pour agir comme un point d'accès Wi-Fi dans un lieu public, afin de faire croire aux gens qu'il est légitime. Lorsque des individus s'y connectent, l'attaquant a un accès instantané aux données transitant par le routeur.

Attaques par déni de service distribué (Distributed Denial of Service - DDoS)

Ces attaques sont assez courantes et impliquent qu'un ou plusieurs ordinateurs et connexions Internet inondent un serveur de trafic, le rendant inaccessible aux autres. Pour les sites Web d'information, ces attaques empêchent l'information d'atteindre le public et peuvent devenir coûteuses, à mesure que le nombre de visiteurs diminue et qu'une aide technique est nécessaire.

Cyberharcèlement

L'utilisation d'Internet ou d'autres moyens électroniques pour traquer et/ou harceler un individu, un groupe ou une organisation. Cela peut inclure de fausses accusations, de la diffamation, des calomnies et des calomnies. Cela peut également inclure la surveillance, le vol d'identité, les menaces, le vandalisme ou la collecte d'informations pouvant être utilisées pour menacer, embarrasser ou harceler.

94 https://www.aura.com/learn/types-of-social-engineering-attacks
95 https://www.exabeam.com/information-security/cyber-security-threat/
96 https://www.aura.com/learn/types-of-social-engineering-attacks
97 https://www.aura.com/learn/types-of-social-engineering-attackshttps://www.aura.com/learn/types-of-social-engineering-attacks

Harcèlement sur internet

L'utilisation de moyens électroniques tels que le courrier électronique, les réseaux sociaux, la messagerie instantanée et d'autres formes de communication en ligne dans l'intention d'abuser, d'intimider ou de maîtriser un individu ou un groupe.

Mesures préventives contre les menaces numériques

Avec un peu d'effort, vous pouvez protéger votre ordinateur et contribuer à éviter des problèmes plus importants. Les étapes suivantes empêcheront une attaque ou traiteront les virus si un ordinateur est infecté:[99]

- **Installer un logiciel antivirus :** les outils anti-malware aident à détecter et à supprimer les logiciels malveillants de votre ordinateur ou appareil mobile.
- **Maintenir les applications à jour:** assurez-vous que toutes les applications sont à jour. Les applications obsolètes qui ne disposent pas des correctifs de sécurité les plus récents les rendent vulnérables aux logiciels malveillants.
- **Limiter l'accès aux partages de fichiers réseau:** autorisez uniquement le niveau d'accès requis par la fonction métier de l'utilisateur. Limiter l'accès aux partages de fichiers réseau empêchera un appareil infecté par un ransomware de le propager à d'autres appareils du réseau.
- **N'ouvrez pas et n'exécutez pas de pièces jointes inattendues.**
- **Désactivez la fonction d'aperçu** dans vos programmes pour une protection supplémentaire.
- **Désactivez toutes les fonctionnalités du programme susceptibles** d'ouvrir automatiquement un e-mail, un message instantané, une pièce jointe ou un téléchargement.

2.2.

Hygiène numérique

Pour garantir la sécurité numérique des journalistes, des défenseurs des droits numériques et des autres internautes, un ensemble de mesures d'hygiène numérique sont disponibles pour contribuer à lutter contre les menaces et les incidents de sécurité numérique.

L'hygiène numérique (ou cyberhygiène ou hygiène Internet) est le terme fourre-tout désignant les pratiques et les comportements liés au nettoyage et à la maintenance de notre monde numérique. Cela inclut tout, de l'organisation des fichiers sur votre appareil numérique à la protection de votre identité numérique et des données associées, en passant par l'installation de nouvelles applications ou technologies pour rendre votre vie numérique plus facile et plus sécurisée.

En protégeant les informations que vous partagez en ligne ou bien en sécurisant les appareils que vous utilisez, vous réduisez à la

98 https://www.eccouncil.org/cybersecurity-exchange/penetration-testing/man-in-the-middle-attack-mitm/
99 https://it.osu.edu/security

fois le risque d'être attaqué et la gravité d'une attaque réussie. Tout ce que vous publiez en ligne peut devenir une source ou une information utilisée par un mauvais acteur pour lancer une escroquerie ou une cyberattaque contre vous. En tant qu'acteur des droits numériques, le maintien de bonnes pratiques d'hygiène numérique est essentiel pour assurer votre sécurité sur Internet.

Le reste du chapitre répertorie quelques mesures simples que vous pouvez prendre, sans acheter de technologie coûteuse ni investir beaucoup de temps dans la reconfiguration de votre réseau domestique, pour rendre votre informatique en ligne plus sûre.

2.3.

Mots de passe

Si vous cherchez un moyen d'améliorer votre cybersécurité, la sécurité des mots de passe est le point de départ. Un mot de passe est un mécanisme de sécurité de base qui consiste idéalement en une phrase secrète créée à l'aide de caractères alphabétiques, numériques, alphanumériques et symboliques, ou d'une combinaison. Ce mécanisme de sécurité est utilisé pour restreindre l'accès à un système, une application ou un service aux seuls utilisateurs qui l'ont mémorisé ou stocké ou bien sont autorisés à l'utiliser.

La pratique standard de sécurité numérique consiste à créer des mots de passe forts, à ne pas réutiliser les mots de passe, à utiliser des phrases secrètes et une authentification multifacteur, à examiner attentivement les questions de réinitialisation des mots de passe, à ne pas écrire les mots de passe et, enfin et surtout, à utiliser un gestionnaire de mots de passe.

Générateurs de mots de passe

Un générateur de mots de passe est un outil logiciel qui crée des mots de passe aléatoires ou personnalisés pour les utilisateurs. Il aide les utilisateurs à créer des mots de passe plus forts qui offrent une plus grande sécurité pour un type d'accès donné.

Les générateurs de mots de passe aident ceux qui doivent constamment trouver de nouveaux mots de passe à garantir un accès autorisé aux programmes et à gérer de nombreux mots de passe pour la gestion des identités et des accès.

Gestionnaires de mots de passe

Un gestionnaire de mots de passe est un outil qui crée et stocke des mots de passe afin que de nombreux mots de passe différents puissent être utilisés sur différents sites et services sans avoir à les mémoriser.

Gestionnaires de mots de passe

- Générer des mots de passe forts qu'il est peu probable qu'un être humain puisse deviner
- Stocker plusieurs mots de passe (et réponses aux questions de sécurité) en toute sécurité
- Protégez tous les mots de passe avec un seul mot de passe principal (ou phrase

secrète).[100]

Si votre ordinateur ou appareil est compromis et qu'un logiciel espion est installé, celui-ci peut vous surveiller en train de saisir votre mot de passe principal et voler le contenu du gestionnaire de mots de passe. Il est donc toujours très important de garder votre ordinateur et vos autres appareils exempts de logiciels malveillants lorsque vous utilisez un gestionnaire de mots de passe.

Note!

Utiliser des gestionnaires de mots de passe, c'est comme mettre tous vos œufs dans le même panier et les protéger au prix de votre vie. Le risque avec les gestionnaires de mots de passe piratés est que l'accès au « panier » signifie l'accès à tous vos « œufs ».

Synchronisation des mots de passe sur plusieurs appareils [101]

De nombreux gestionnaires de mots de passe permettent d'accéder aux mots de passe sur tous les appareils via une fonction de synchronisation des mots de passe. Cela signifie que lorsqu'un fichier de mots de passe est synchronisé sur un appareil, il est automatiquement disponible sur tous les autres appareils.

Les gestionnaires de mots de passe peuvent stocker les mots de passe « dans le cloud », c'est-à-dire cryptés sur un serveur distant. Lorsque les mots de passe sont nécessaires, ces gestionnaires récupèrent et déchiffrent automatiquement[102] les mots de passe. Les gestionnaires de mots de passe qui utilisent leurs propres serveurs pour stocker ou aider à synchroniser les mots de passe sont plus pratiques, mais sont légèrement plus vulnérables aux attaques. Si les mots de passe sont stockés à la fois sur l'ordinateur et dans le cloud, un attaquant n'a pas besoin de s'emparer de l'ordinateur pour découvrir les mots de passe. (Ils devront cependant casser la phrase secrète du gestionnaire de mots de passe.) Si cela vous inquiète, ne synchronisez pas les mots de passe avec le cloud, choisissez plutôt de les stocker uniquement sur les appareils.

Note!

Conservez une sauvegarde de la base de données de mots de passe au cas où. Avoir une sauvegarde est utile si la base de données de mots de passe est perdue lors d'une panne du système ou si l'appareil est retiré. Les gestionnaires de mots de passe ont généralement un moyen de créer un fichier de sauvegarde, ou on peut utiliser le programme de sauvegarde habituel.

Attaques de mot de passe courantes

L'un des moyens les plus simples et les plus

100 https://ssd.eff.org/glossary/passphrase
101 https://ssd.eff.org/en/module/creating-strong-passwords#3
102 https://ssd.eff.org/glossary/decrypt

courants de pirater[103] un compte consiste à essayer des mots de passe courants ou à faire une petite recherche sur la victime ciblée et à essayer des mots de passe liés à cette personne.

Un rapport de Cybernews de 2024 a révélé que les 10 mots de passe les plus couramment utilisés et piratés étaient:

1. 123456
2. 123456789
3. qwerty
4. password
5. 12345
6. qwerty123
7. 1q2w3e
8. 12345678
9. 111111
10. 1234567890

Ce sont des mots de passe TRÈS peu sécurisés. Ils sont faciles à deviner et les cybercriminels commenceront à essayer d'accéder à des comptes avec des mots de passe perçus comme faibles comme ceux-ci.

N'utilisez JAMAIS de mots de passe contenant les informations suivantes:

- Votre nom ou les noms de votre famille et de vos amis,
- Votre anniversaire ou ceux de votre famille et de vos amis,
- Noms des animaux de compagnie, et
- Les lieux où vous vivez ou avez vécu, y compris les noms de villes ou de rues.

Il est étonnant de constater combien d'informations sur une personne sont disponibles sur Internet. Ainsi, si votre mot de passe contient des informations vous concernant d'une manière qui peut être discernée sur Internet ou en discutant avec vos amis, il peut être facilement deviné.

Attaque de force brute

Une attaque par force brute essaie simplement toutes les combinaisons possibles de caractères autorisés jusqu'à ce qu'elle trouve une correspondance. Ce type d'attaque est très efficace sur les mots de passe plus courts et pourra même pirater des mots de passe composés de caractères aléatoires. Mais la longueur compte.

Une attaque par force brute n'est pas très efficace et si votre mot de passe est suffisamment long, il peut être difficile à pirater. Jetez un œil au tableau qui montre le temps qu'il faudrait pour détecter un mot de passe sur un fichier avec une attaque par force brute, en fonction de la longueur et de la complexité du mot de passe. Gardez à l'esprit que ce tableau suppose que l'ordinateur peut essayer beaucoup plus de 1 000 mots de passe par seconde.

Longueur du mot de passe	Tous les personnages	Seulement les minuscules
3 personnages	0.86 seconde	0.02 seconde
4 personnages	1.36 minute	0.46 seconde

103 https://edition.cnn.com/2019/04/22/uk/most-common-passwords-scli-gbr-intl/index.html

5 personnages	2.15 heures	11.9 secondes
6 personnages	8.51 jours	5.15 minutes
7 personnages	2.21 années	2.23 heures
8 personnages	2.10 des siècles	2.42 jours
9 personnages	20 des millénaires	2.07 mois
10 personnages	1,899 des millénaires	4.48 années
11 personnages	180,365 des millénaires	1.16 des siècles
12 personnages	17,184,705 des millénaires	3.03 des millénaires
13 personnages	1,627,797,068 des millénaires	78.7 des millénaires
14 personnages	154,640,721,434 des millénaires	2,046 des millénaires

Notez que le temps nécessaire pour pirater un mot de passe augmente de façon exponentielle avec chaque caractère ajouté. Pour un mot de passe composé de caractères aléatoires de tous types, la différence entre 6, 7, 8 et 9 caractères est de jours, années, siècles et millénaires ! Notez également combien de temps, il faut pour pirater un mot de passe contenant tous les types de caractères par rapport à un mot de passe de même longueur qui utilise uniquement des caractères minuscules.

Création et maintenance de mots de passe forts et sécurisés

La réutilisation des mots de passe est une pratique de sécurité exceptionnellement mauvaise. Si un acteur malveillant met la main sur un mot de passe que vous avez réutilisé sur plusieurs services, il peut accéder à plusieurs de vos comptes. C'est pourquoi il est si important d'avoir plusieurs mots de passe forts et uniques. Heureusement, un gestionnaire de mots de passe peut vous aider.[104]

Conseils pour créer des mots de passe forts :

- Utilisez une combinaison de lettres juscules et minuscules, de chiffres et de symboles.
- Un mot de passe fort doit comporter entre huit et douze caractères.
- Évitez l'utilisation de données personnelles.
- Changez-le régulièrement.
- Ne l'utilisez jamais pour plusieurs comptes.
- Utilisez l'authentification multifacteur.
- Il existe quelques mots de passe que vous devez mémoriser et qui doivent être particulièrement forts. Ceux-ci inclus:
- Mots de passe pour votre appareil
- Mots de passe pour le chiffrement (comme le chiffrement complet du disque)[105]
- Le mot de passe principal,[106] ou « phrase

104 https://ssd.eff.org/en/glossary/password-manager
105 https://ssd.eff.org/en/glossary/encryption
106 https://ssd.eff.org/glossary/master-password

secrète »,[107] de votre gestionnaire de mots de passe

- Votre mot de passe de messagerie[108]

Créer des mots de passe forts à l'aide de dés

L'une des nombreuses difficultés rencontrées lorsque les gens choisissent eux-mêmes leurs mots de passe est qu'ils ne sont pas très doués pour faire des choix aléatoires et imprévisibles.[109] Un moyen efficace de créer un mot de passe[110] fort et mémorable consiste[111] à utiliser des dés et une liste de mots[112] pour choisir des mots au hasard. Ensemble, ces mots forment votre « phrase secrète ». Une « phrase secrète » est un type de mot de passe plus long pour plus de sécurité. Pour le chiffrement du disque et votre gestionnaire de mots de passe, nous vous recommandons de sélectionner un minimum de six mots.

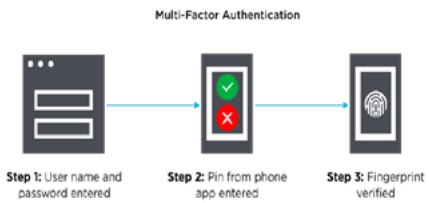
Pourquoi utiliser un minimum de six mots ? Pourquoi utiliser des dés pour choisir au hasard des mots dans une phrase ?

Plus le mot de passe est long et aléatoire, plus il est difficile à deviner, tant pour les ordinateurs que pour les humains. Pour découvrir pourquoi vous avez besoin d'un mot de passe aussi long et difficile à deviner, voici une vidéo explicative.[113]

2.4. Authentification multifacteur (Multi-Factor Authentification - MFA)

Des mots de passe forts et uniques rendent beaucoup plus difficile l'accès des acteurs malveillants aux comptes numériques. Pour protéger davantage vos comptes numériques, activez l'authentification à deux facteurs.[114]

MFA est une fonctionnalité de sécurité proposée par de nombreux sites Web, applications et appareils qui améliorent considérablement la sécurité des comptes. Techniquement, MFA fait référence à un système dans lequel il existe plus de deux formes d'authentification.



Comment fonctionne l'authentification multifacteur

(Authentification multifacteur)

Étape 1: Nom d'utilisateur et mot de passe saisis

Étape 2: Code PIN saisi depuis l'application téléphonique

107 https://ssd.eff.org/en/glossary/passphrase
108 https://ssd.eff.org/en/glossary/password
109 http://people.ischool.berkeley.edu/~nick/aaronson-oracle/
110 https://www.eff.org/deeplinks/2016/07/new-wordlists-random-passphrases
111 https://www.eff.org/dice
112 https://www.eff.org/deeplinks/2018/08/dragon-con-diceware
113 https://ssd.eff.org/en/module/animated-overview-how-make-super-secure-password-using-dice
114 https://ssd.eff.org/en/glossary/two-factor-authentication

Étape 3: *Empreinte digitale vérifiée*

Si vous disposez d'une configuration MFA pour un compte donné (site Web, application ou appareil), lorsque vous vous connectez avec votre nom d'utilisateur et votre mot de passe, ce serveur de compte demandera une deuxième forme d'authentification indépendante avant de vous laisser accéder au système. C'est comme lorsqu'un compte bancaire est ouvert et qu'ils demandent à voir une pièce d'identité avec photo et une autre forme d'identification, comme la carte de Sécurité sociale ou le passeport international. Il est beaucoup plus difficile de prétendre que vous êtes quelqu'un que vous n'êtes pas quand vous devez prouver qui vous êtes de deux manières différentes.

Méthodes d'authentification multifacteur

Nous vous recommandons d'enregistrer au moins deux appareils pour l'authentification multifacteur. Ainsi, si vous perdez un appareil, vous pouvez vous protéger en effaçant les données à distance, puis utiliser l'autre appareil pour vous authentifier. Avec MFA, la deuxième authentification peut être effectuée à l'aide de plusieurs méthodes différentes.

Les méthodes les plus courantes incluent:

Méthode de « notification push » de l'application pour appareil mobile

Le moyen le plus populaire d'obtenir la deuxième forme d'authentification consiste à envoyer un « push » vers une application sur votre appareil mobile. Avec cette méthode, le serveur de compte auquel vous essayez de vous connecter enverra une notification à votre appareil mobile. La notification apparaîtra sur l'appareil mobile et dira quelque chose du genre: « Hé, quelqu'un essaie de se connecter à ce site Web, n'est-ce pas ? Devons-nous les laisser entrer ? Il y a généralement un gros bouton vert et un gros rouge pour que vous puissiez facilement répondre « Oui » ou « Non ». Si vous cliquez sur « Oui », vous êtes connecté. Mais si vous n'avez pas fait la demande de connexion initiale, vous savez que quelqu'un connaît votre mot de passe et essaie de se connecter à votre compte. Vous pouvez appuyer sur le bouton « Non » et leur accès sera refusé. Vous pouvez ensuite vous connecter vous-même et modifier votre mot de passe pour que l'attaquant revienne à la case départ.

C'est une mesure de sécurité simple, mais extrêmement efficace. Le principal avantage de cette méthode est qu'un attaquant doit non seulement compromettre votre mot de passe, mais doit également avoir un accès physique à votre appareil mobile et doit pouvoir se connecter à cet appareil. Les chances que tout cela se produit sont extrêmement faibles si vous utilisez des mots de passe corrects et si vous gardez une trace de votre téléphone. Un autre avantage de cette méthode est que vous recevez une notification en temps réel lorsque quelqu'un tente de se connecter illégalement à votre compte, vous permettant ainsi de réagir rapidement en modifiant votre mot de passe.

Applications d'authentification d'appareil mobile

Parfois, le serveur de compte ne vous enverra pas de notification push, mais il peut vous demander de saisir un code unique généré

par l'application d'authentification sur votre appareil mobile. Ces codes sont courts (peut-être six chiffres ou plus), ils peuvent donc sembler peu sécurisés. Ce qui est cool, c'est que les codes sont régénérés toutes les minutes environ et qu'ils sont basés sur un algorithme connu uniquement de votre application d'authentification et du serveur de compte auquel vous essayez de vous connecter. Il serait extrêmement difficile pour un cybercriminel de deviner correctement le code à 6 chiffres dans de telles circonstances, car le délai est très court. Encore une fois, le principal avantage ici est que l'attaquant doit avoir un accès physique à votre appareil mobile et la possibilité de s'y connecter. Un inconvénient est que vous ne recevez aucune notification en temps réel si quelqu'un tente de se connecter à votre compte. Habituellement, cette méthode est également une option de sauvegarde de la méthode push. La plupart des applications d'authentification prennent en charge les deux méthodes.

Méthode de code SMS

Cette méthode utilise aussi votre appareil mobile, mais elle n'utilise pas d'application. Par conséquent, cela fonctionne avec des téléphones non-smartphones. Si vous configurez cette méthode de MFA, lorsque vous vous connectez avec votre nom d'utilisateur et votre mot de passe, le serveur de compte enverra à votre téléphone mobile un message texte avec un code à usage unique. Vous saisirez ensuite ce code sur le site Web ou le portail de l'appareil sur lequel vous avez saisi votre mot de passe. Cela présente fondamentalement tous les avantages de la méthode « push », mais elle n'est tout simplement pas aussi pratique, car vous devez saisir le code. Vous recevrez cette notification en temps réel d'une tentative de connexion et vous recevrez un message texte par tentative. L'inconvénient est qu'un attaquant ne doit pas nécessairement pouvoir se connecter à votre téléphone. Ils doivent avoir physiquement le téléphone, parce que des messages texte apparaissent souvent sur l'écran du téléphone, même lorsque le téléphone est verrouillé.

Méthode de code de courrier électronique

Cette méthode fonctionne de manière très similaire à la méthode du code SMS, sauf que le code est envoyé à un compte de messagerie que vous avez enregistré auprès du serveur de compte auquel vous essayez d'accéder. Vous le configurerez le plus souvent lors de votre inscription au service multifacteur que vous utilisez. Si vous envisagez d'utiliser ce type de MFA, vous devrez vous assurer que votre compte de messagerie lui-même est sécurisé, ce qui signifie probablement que vous devez activer MFA pour accéder à votre compte de messagerie. La raison en est que les e-mails peuvent être consultés depuis n'importe où, y compris depuis le même terminal informatique sur lequel le cybercriminel tente de se connecter à votre compte.

En d'autres termes, cette méthode ne nécessite aucun accès physique à un appareil indépendant. C'est pourquoi vous devez avoir un mot de passe fort pour votre courrier électronique qui n'est utilisé nulle part ailleurs. Si vous faisiez cela, cette méthode nécessiterait essentiellement que l'attaquant connaisse deux de vos mots de passe. Cependant, les forcer à accéder à un autre appareil est une

option plus solide et plus sécurisée. Si un site Web autorise uniquement ce type de MFA, ce n'est pas un problème. Allez-y, configurez-le, puis demandez une authentification sur votre appareil mobile pour accéder à votre courrier électronique.

Jeton physique

Cette méthode était plus populaire avant l'avènement des smartphones. Un jeton physique est un petit appareil qui génère en continu des codes de la même manière qu'une application d'authentification sur votre appareil mobile. Cela fonctionne tout aussi bien, mais cela présente l'inconvénient supplémentaire que vous devez suivre cet autre appareil. De nos jours, nos vies sont liées à nos téléphones portables. Vous pouvez imaginer la possibilité de perdre un jeton sans même vous rendre compte qu'il a disparu pendant un certain temps. Si vous en possédez un, conservez-le dans un endroit sûr. Si vous devez le transporter, attachez-le peut-être à votre porte-clés.

Biométrie

L'AMF biométrique repose sur les caractéristiques physiques ou comportementales uniques de l'utilisateur, telles que la reconnaissance faciale, l'analyse des empreintes digitales, l'analyse de l'iris, la reconnaissance vocale, etc. Étant donné que chacun a une empreinte digitale et un visage uniques, cela peut être assez sécurisé. La biométrie est couramment utilisée comme MFA pour les applications contenant des données sensibles.

L'authentification multifacteur biométrique peut fournir un niveau plus élevé d'assurance que l'utilisateur est bien celui qu'il prétend être, car les données biométriques sont plus difficiles à falsifier, volé ou deviner que les mots de passe ou les jetons. Cependant, cela présente également des inconvénients, tels que des problèmes de confidentialité. Les systèmes d'authentification biométrique stockent des informations sensibles. Si ces informations tombent entre de mauvaises mains, elles peuvent être exploitées à des fins d'usurpation d'identité ou à d'autres fins malveillantes. Malgré ses défis, l'authentification biométrique est plus fiable et plus difficile à compromettre que les autres types de méthodes d'authentification, et il existe des moyens d'atténuer tout risque de sécurité potentiel en mettant soigneusement en œuvre des pratiques de sécurité renforcées supplémentaires à l'aide de la MFA, qui combine la biométrie avec d'autres facteurs d'authentification pour fournir une couche de sécurité supplémentaire.

2.5.

Authentification à deux facteurs (2FA)

L'authentification à deux facteurs est un type, ou un sous-ensemble, de MFA et constitue un moyen de permettre aux utilisateurs de s'identifier auprès des fournisseurs de services en exigeant une combinaison de deux méthodes d'authentification différentes. Il peut s'agir de quelque chose que l'utilisateur connaît (comme un mot de passe ou un code PIN), quelque chose qu'il possède (comme un jeton matériel ou un téléphone mobile), ou quelque chose qui est attaché ou indissociable de l'utilisateur (comme ses empreintes digitales).

Comment fonctionne la 2FA en ligne ?

Plusieurs services en ligne – dont Facebook, Google et X – proposent le 2FA comme alternative à l'authentification par mot de passe uniquement. Si vous activez cette fonctionnalité, vous serez invité à saisir à la fois un mot de passe et une méthode d'authentification secondaire. Cette deuxième méthode est généralement soit un code à usage unique envoyé par SMS, soit un code à usage unique généré par une application mobile dédiée qui stocke un secret (comme Google Authenticator ou Duo Mobile). Dans les deux cas, le deuxième facteur est votre téléphone portable, quelque chose que vous possédez (normalement). Certains sites Web (dont Google) prennent également en charge les codes de sauvegarde à usage unique, qui peuvent être téléchargés, imprimés sur papier et stockés dans un endroit sûr comme sauvegarde supplémentaire. Une fois que vous avez choisi d'utiliser 2FA, vous devrez saisir votre mot de passe et un code à usage unique depuis votre téléphone pour accéder à votre compte.

Pourquoi devriez-vous activer 2FA ?

2FA vous offre une plus grande sécurité de compte en vous obligeant à authentifier votre identité avec plusieurs méthodes. Cela signifie que, même si quelqu'un mettait la main sur votre mot de passe principal, il ne pourrait pas accéder à votre compte à moins de disposer pareillement de votre téléphone mobile ou d'un autre moyen d'authentification secondaire.

Y a-t-il des inconvénients à utiliser la 2FA ?

Bien que 2FA offre un moyen d'authentification plus sécurisé, il existe un risque accru de blocage de votre compte si, par exemple, vous égarez ou perdez votre téléphone, changez de carte SIM[115] ou voyagez dans un pays sans activer l'itinérance. De même, l'utilisation de 2FA signifie que vous transmettrez peut-être plus d'informations à un service que ce avec quoi vous êtes à l'aise. Supposons que vous utilisiez X et que vous vous inscriviez en utilisant un pseudonyme.[116]

Même si vous évitez soigneusement de donner à X vos informations d'identification et que vous accédez au service uniquement via Tor ou un VPN,[117] tant que vous activez SMS 2FA, X aura nécessairement un enregistrement de votre numéro de mobile. Cela signifie que s'il y est contraint par un tribunal, X peut vous associer votre compte via votre numéro de téléphone. Cela ne pose peut-être pas de problème si vous utilisez déjà votre nom légal sur un service donné, mais si le maintien de votre anonymat est important, réfléchissez-y à deux fois avant d'utiliser SMS 2FA.

Authentification universelle par facteur

L'authentification universelle, également connue sous le nom d'authentification unique (single sign-on - SSO), est une méthode de vérification d'identité réseau qui permet aux utilisateurs de naviguer d'un site à l'autre en

115 https://ssd.eff.org/en/glossary/sim-card
116 https://ssd.eff.org/en/glossary/pseudonym
117 https://ssd.eff.org/en/glossary/vpn

toute sécurité sans avoir à saisir plusieurs fois des informations d'identification. Avec l'authentification universelle, un abonné saisit un ensemble de paramètres (tels qu'un nom d'utilisateur et un mot de passe) au début de chaque session réseau. Les données d'authentification de tout site visité par la suite sont automatiquement générées pour la durée de cette session. L'un des plus grands défis en matière de sécurité Internet réside dans le fait que chaque site Web possède son propre système d'authentification. Un internaute typique qui possède deux ou trois adresses e-mail Web et fréquente une demi-douzaine de vendeurs en ligne pour acheter ou vendre des choses doit mémoriser plusieurs noms d'utilisateur et mots de passe. Cela peut être difficile à moins que les données d'authentification ne soient écrites ou stockées sous forme de fichier texte, ce qui devient alors un problème de sécurité. L'authentification universelle peut éliminer ce problème sans compromettre la sécurité ou la confidentialité.

Note!

Si vous avez le choix, choisissez l'application d'authentification ou le périphérique matériel autonome au lieu de recevoir les codes par SMS. Il est plus facile pour un attaquant de rediriger ces codes vers son propre téléphone que de contourner l'authentificateur.

2.6.

Pare-feu

Système de sécurité réseau qui protège un ordinateur contre les connexions indésirables vers où depuis les réseaux locaux et Internet, en particulier les intranets, les pare-feu peuvent être mis en œuvre à la fois sous forme matérielle et logicielle, ou une combinaison des deux. Un pare-feu[118] peut avoir des règles qui interdisent les e-mails sortants ou les connexions à certains sites Web. Les pare-feu peuvent être utilisés comme première ligne de défense pour protéger un appareil contre les interférences inattendues. Ils peuvent également être utilisés pour empêcher les utilisateurs d'accéder à Internet de certaines manières.

Pare-feu matériels et logiciels

Les pare-feu peuvent être matériels ou logiciels, mais la configuration idéale comprendra les deux. En plus de limiter l'accès à votre ordinateur et à votre réseau, un pare-feu est pareillement utile pour permettre l'accès à distance à un réseau privé via des certificats d'authentification et des connexions sécurisés.

Les pare-feu matériels peuvent être achetés en tant que produit autonome, mais se trouvent généralement dans les routeurs haut débit et doivent être considérés comme un élément important de la sécurité de votre système et de la configuration de votre réseau. La plupart des pare-feu matériels disposent d'un minimum de

118 https://ssd.eff.org/en/glossary/firewall

quatre ports réseau pour connecter d'autres ordinateurs, mais pour les réseaux plus grands, une solution de pare-feu de réseau d'entreprise est disponible.

Les pare-feu logiciels sont installés sur votre ordinateur, comme n'importe quel logiciel, et vous pouvez le personnaliser, vous permettant ainsi de contrôler son fonctionnement et ses fonctionnalités de protection. Un pare-feu logiciel protégera votre ordinateur contre les tentatives extérieures visant à contrôler ou à accéder à votre ordinateur. Les pare-feu peuvent également faire partie du système d'exploitation de votre ordinateur.

Par exemple, le pare-feu Windows est une application Microsoft Windows qui informe les utilisateurs de toute activité suspecte. L'application peut détecter et bloquer les virus, les vers et les pirates informatiques pour exécuter des activités nuisibles.

Techniques de filtrage du pare-feu

Les pare-feu sont utilisés pour protéger les réseaux domestiques et d'entreprise. Un programme de pare-feu ou un périphérique matériel typique filtre toutes les informations provenant d'Internet vers votre réseau ou votre système informatique. Il existe plusieurs types de techniques de pare-feu qui empêcheront les informations potentiellement dangereuses de passer:

- **Filtre de paquets:** examine chaque paquet[119] entrant ou sortant du réseau et l'accepte ou le rejette en fonction de règles définies par l'utilisateur. Le filtrage de paquets est assez efficace et transparent pour les utilisateurs, mais il est difficile à configurer. De plus, il est sensible à l'usurpation d'adresse IP.[120]
- **Application Gateway:** applique des mécanismes de sécurité à des applications spécifiques, telles que les serveurs FTP[121] et Telnet.[122] C'est très efficace, mais peut imposer une dégradation des performances.
- **Passerelle au niveau du circuit:** applique des mécanismes de sécurité lorsqu'une connexion TCP[123] ou UDP[124] est établie. Une fois la connexion établie, les paquets peuvent circuler entre les hôtes sans autre vérification.
- **Serveur proxy:** intercepte tous les messages entrant et sortant du réseau. Le serveur proxy masque[125] efficacement les véritables adresses réseau.

En pratique, de nombreux pare-feux utilisent simultanément deux ou plusieurs de ces techniques. Un pare-feu est considéré comme une première ligne de défense pour protéger les informations privées. Pour plus de sécurité, les données peuvent être cryptées.

119 https://www.webopedia.com/TERM/P/packet.html
120 https://www.webopedia.com/TERM/I/IP_spoofing.html
121 https://www.webopedia.com/TERM/F/ftp.html
122 https://www.webopedia.com/TERM/T/Telnet.html
123 https://www.webopedia.com/TERM/T/Telnet.html
124 https://www.webopedia.com/TERM/U/User_Datagram_Protocol.html
125 http://ebopedia.com/TERM/P/proxy_server.html

2.7.

Cryptage

Le cryptage implique le brouillage mathématique d'informations ou d'un message (chiffrer), de sorte qu'il semble dénué de sens, mais qu'il puisse néanmoins être restauré dans sa forme originale par une personne ou un appareil possédant une donnée capable de la déchiffrer (une clé de déchiffrement). Cela limite le nombre de personnes pouvant accéder aux informations ou au message, car sans la bonne clé, il est presque impossible d'inverser le cryptage et de récupérer les informations d'origine. Le cryptage est l'une des nombreuses technologies qui composent le domaine appelé cryptographie.

Le cryptage de bout en bout garantit qu'un message est transformé en message secret par son expéditeur d'origine et décodé uniquement par son destinataire final. D'autres formes de cryptage peuvent dépendre du cryptage effectué par des tiers. Cela signifie qu'il faut faire confiance à ces partis avec le texte original. Le chiffrement de bout en bout est généralement considéré comme plus sûr, car il réduit le nombre de parties susceptibles d'interférer ou de briser le chiffrement.

2.8.

Réseaux privés virtuels (VPN)

Un VPN est une méthode permettant de connecter un ordinateur en toute sécurité au réseau d'une organisation ailleurs sur Internet. Lorsque vous êtes connecté à un VPN, toutes les données de navigation Web semblent provenir du VPN lui-même, plutôt que de votre propre fournisseur d'accès Internet (FAI).[126] L'utilisation d'un VPN masque l'adresse[127] IP attribuée par votre FAI aux sites auxquels vous accédez, ajoutant ainsi une couche de confidentialité.

En plus de masquer votre adresse IP, il crypte également vos données lors de leur transit vers le site auquel vous accédez.

VPN commerciaux

Un VPN commercial est un service privé qui propose de relayer en toute sécurité vos communications Internet via son propre réseau. L'avantage est que toutes les données que vous envoyez et recevez sont cachées des réseaux locaux, elles sont donc plus à l'abri des criminels à proximité, des FAI locaux non fiables ou de tout autre personne espionnant votre réseau local. Un VPN peut être hébergé dans un pays étranger, ce qui est utile à la fois pour protéger les communications d'un gouvernement local et pour contourner la censure nationale. L'inconvénient est que le trafic est décrypté du côté du VPN commercial.[128] Cela signifie que vous devez faire confiance au VPN commercial (et au pays où il se trouve) pour ne pas espionner votre trafic. Même si un VPN commercial peut offrir de la « sécurité »,

126 https://en.wikipedia.org/wiki/Internet_service_provider
127 https://ssd.eff.org/en/glossary/ip-address
128 https://ssd.eff.org/en/glossary/commercial-vpn
129 https://www.cyberghostvpn.com/en_US/
130 https://nordvpn.com/

il ne garantit pas nécessairement la sécurité. Des exemples de ces VPN sont CyberGhost VPN,[129] NordVPN,[130] Private Internet Access VPN[131] et TunnelBear (avec un essai gratuit de 2 Go de bande passante).[132]

VPN gratuits

Un VPN gratuit est un service qui vous donne accès à un réseau de serveurs VPN, ainsi qu'aux logiciels nécessaires, sans que vous ayez à payer quoi que ce soit. Même si un VPN gratuit peut vous faire économiser de l'argent, il peut toutefois présenter un risque de sécurité, car vous perdrez le contrôle de vos données. Un exemple est Windscribe VPN, qui est gratuit avec une limite de bande passante tous les 30 jours.[133]

Note!

Avant de choisir un service VPN, lisez toujours les avis des utilisateurs pour connaître les préoccupations de ses utilisateurs. En outre, enquêtez toujours sur la réputation du fournisseur de services VPN et voyez où il se trouve – vous souhaiterez probablement ignorer tout fournisseur de services hébergé dans un pays avec un historique de sécurité douteux.

2.9.

Développer des habitudes en ligne sûres

Voici une liste d'habitudes en ligne et de mesures de sécurité à adopter pour contribuer à protéger vos données personnelles et garantir une expérience en ligne sécurisée:

- Gardez vos systèmes et logiciels à jour.
- Ayez toujours un antivirus actuel/mis à jour en cours d'exécution.
- Évitez les escroqueries par phishing.
- Utilisez un mot de passe complexe ou un gestionnaire de mots de passe.
- Faites attention à ce sur quoi vous cliquez ; un site Web peu réputé peut vous relier à des cybercriminels et à des acteurs malveillants.
- Ne laissez jamais votre ordinateur ou vos appareils sans surveillance. Verrouillez vos écrans lorsque vous vous dirigez vers les toilettes. Un système ouvert est une invitation ouverte à vos données.
- Protégez vos données.
- Pour tous les fichiers personnels, sauvegardez vos données ! Vous ne savez jamais quand vous risquez de perdre votre disque dur et si les données seront récupérables. Il existe de nombreuses options de stockage dans le cloud et un disque externe est également une option. Pensez à chiffrer vos données avant de les sauvegarder sur un périphérique de

131 https://www.privateinternetaccess.com/pages/techradar
132 https://www.tunnelbear.com
133 https://windscribe.com/

stockage externe ou sur le cloud.

- Lorsque vous effectuez des achats en ligne ou partagez des données sensibles, assurez-vous d'envoyer des informations cryptées en recherchant « https » ou l'icône de verrouillage dans votre barre d'adresse.
- Soyez intelligent sur ce que vous partagez (et ne partagez pas) sur les réseaux sociaux.
- Dans le monde physique, faites attention aux attaques d'ingénierie sociale, comme décrit ci-dessus.
- Assurez-vous de surveiller vos comptes de réseaux financiers et sociaux pour détecter toute activité suspecte.

Conseils de cybersécurité pour le travail virtuel

Le télétravail (travail à domicile), quelle qu'en soit la raison, comporte ses propres défis en matière de menaces de cybersécurité. Le travail virtuel gagne en popularité à mesure que de plus en plus de personnes et d'entreprises utilisent la technologie pour mener des activités à distance.

Voici une liste de consignes de sécurité pour le travail à distance:

Conseils pour les travailleurs à distance

- Utilisez uniquement le Wi-Fi auquel vous faites confiance. Avec une connexion non sécurisée, les personnes se trouvant à proximité peuvent espionner votre trafic.
- Pour les réseaux domestiques, chiffrez la connexion entre vos appareils et votre routeur Wi-Fi, par exemple en utilisant l'algorithme de chiffrement WEP.[134]
- Utilisez des appareils approuvés par l'entreprise.
- Mettre à jour le logiciel antivirus.
- Mettez à jour tous les logiciels et le système d'exploitation.
- N'oubliez pas de sauvegarder périodiquement. Les fichiers les plus importants doivent être sauvegardés régulièrement. Dans le pire des cas, le personnel pourrait par exemple être victime d'un ransomware. Alors tout est perdu sans sauvegarde.
- Assurez-vous que vous utilisez une connexion sécurisée à votre environnement de travail. Cela signifie utiliser un VPN ou un autre moyen sécurisé comme Teamviewer.
- Méfiez-vous des e-mails de phishing. Il faut se méfier de tout e-mail demandant de vérifier ou de renouveler vos informations d›identification, même s›il semble provenir d›une source fiable. Veuillez essayer de vérifier l›authenticité de toute demande importante ou suspecte par d›autres moyens ; ne cliquez pas sur des liens suspects et n'ouvrez pas de pièces jointes suspectes.

134 https://www.techtarget.com/searchnetworking/feature/Wireless-encryption-basics-Understanding-WEP-WPA-and-WPA2

Conseils pour les employeurs

- Concentrez-vous sur la sécurisation des systèmes qui permettent l'accès à distance, tels que les VPN. Assurez-vous que ces systèmes sont entièrement corrigés, que les pare-feu sont correctement configurés et qu'un logiciel anti-malware et de prévention des intrusions est installé.
- N'exposez jamais directement le protocole RDP (Remote Desktop Protocol) à Internet (connectez-vous d'abord au VPN).
- Mettez en œuvre l'authentification multifacteur dans la mesure du possible.
- Envisagez de restreindre l'accès aux systèmes sensibles, le cas échéant.
- Envoyez des e-mails de sensibilisation au phishing à vos employés.
- L'utilisation de logiciels non autorisés à des fins officielles (appelée shadow IT) peut augmenter lors du travail à distance, augmentant ainsi les risques en matière de sécurité et de confidentialité. Assurez-vous que le personnel est conscient de la politique, de la confidentialité et des obligations légales qui s'appliquent aux informations de votre organisation.
- Examinez vos plans de réponse aux incidents et, si nécessaire, mettez-les à jour pour tenir compte du personnel travaillant à distance.
- Passez en revue vos plans de continuité d'activité et d'urgence. Assurez-vous qu'ils sont à jour.

Vidéo Conférence

Alors que les visioconférences connaissent un essor depuis l'époque de la COVID, cette évolution a également été marquée par une recrudescence des « attentats par zoom », où des individus malveillants ont envahi les réunions et perturbé les conférences téléphoniques.

Pour éviter de tels incidents, les conseils ci-dessous mettent en évidence les mesures qui peuvent être adoptées:

- Assurez-vous que les participants peuvent se joindre uniquement sur invitation.
- Exiger un mot de passe pour rejoindre la réunion.
- Activez l'approbation de l'administrateur avant que quelqu'un puisse rejoindre la réunion.
- Ne publiez pas de liens de réunion sur les réseaux sociaux.
- Assurez-vous que les logiciels de vidéoconférence et de chat sont toujours à jour.

Outils de videoconference

- Zoom[135]
- Google Meet[136]
- Microsoft Teams[137]

135 https://zoom.us/
136 https://workspace.google.com/products/meet/
137 https://www.microsoft.com/en-us/microsoft-teams/group-chat-software
138 https://www.whatsapp.com/

- WhatsApp[138]
- Signal[139]
- Jitsi[140]
- Cisco Webex[141]

2.10.

Droits Numériques et Outils de Sécurité

Boîte à outils Ayeta sur les droits numériques [142]

La boîte à outils interactive apprend aux gens à comprendre et à identifier les risques de sécurité numérique, à définir des objectifs de sécurité, à apprendre à rester en sécurité en ligne et leur fournit un générateur de mots de passe.

Bouclier d'alimentation [143]

Une boîte à outils en ligne pour aider les défenseurs des droits humains à inverser la tendance, en documentant les abus et en démasquant les trolls.

Ripoti [144]

Une plateforme qui vous permet de signaler les violations des droits numériques. Ripoti se consacre à la sauvegarde des principes de liberté numérique.

Kuram [145]

Un site Web de réponse en ligne à la violence sexiste (OGBV) conçu pour offrir aux femmes et à d'autres groupes vulnérables un moyen de signaler les cas de violence numérique perpétrés à leur encontre.

139 https://www.signal.org/
140 https://jitsi.org/
141 https://www.webex.com/
142 https://paradigmhq.org/ayeta/game.html
143 https://feedshield.africa/en/
144 https://ripoti.africa/
145 https://kuramng.org/

CHAPITRE II | ATTÉNUATION DES MENACES

3.1.

Sécurité numérique et physique

Sécurité numérique lors des manifestations

À un moment donné de leur travail, les acteurs des droits numériques se retrouvent impliqués dans des manifestations dans le but de faire entendre leur voix. Emporter des appareils numériques lors de ces manifestations peut cependant être utilisé contre les manifestants, étant donné que les groupes chargés de l›application des lois disposent d›outils de surveillance numérique tels que de fausses tours de téléphonie mobile et une technologie de reconnaissance faciale qui pourraient être utilisés pour identifier les manifestants et surveiller leurs mouvements et leurs communications, mettant ainsi en danger leur sécurité et leur sécurité confidentialité. Avant de se rendre à des manifestations pacifiques, les manifestants doivent prendre

des mesures pour garantir leur confidentialité numérique. Vous trouverez ci-dessous quelques points à garder à l'esprit.

Garder la préparation des manifestations privée

Disposer d'un service VPN fiable pourrait aider les organisateurs de manifestations à dissimuler leur trafic Internet. Alternativement, les manifestants peuvent utiliser des outils tels que le navigateur Tor [146], qui masque l'activité en ligne d'un utilisateur en bloquant les traqueurs et en cryptant plusieurs fois son trafic réseau. Il est également essentiel de veiller à ce que l'organisation des manifestations soit menée via des applications cryptées de bout en bout plutôt que via des messages en texte brut (également appelés SMS).

Cryptage complet du disque des appareils numériques

Dans le cas où votre appareil serait confisqué par les forces de l'ordre, ou perdu ou volé, le cryptage complet du disque peut finalement contribuer à protéger les données stockées sur votre appareil. Les appareils Android[147] et iOS[148] disposent de fonctionnalités intégrées de chiffrement complet du disque. Ces appareils doivent être protégés à l'aide de mots de passe forts pour éviter toute violation par une attaque par force brute.

Installer le signal

Signal est une application disponible sur iOS[149] et Android[150] qui offre un cryptage puissant de bout en bout pour protéger à la fois les messages texte et les appels vocaux. En plus de chiffrer les communications individuelles, Signal permet des discussions de groupe cryptées. L'application a également récemment ajouté la fonctionnalité permettant de faire disparaître les messages entre 10 secondes et quatre semaines après leur première lecture. Contrairement à certains autres services comme SnapChat, ces messages éphémères ne seront jamais stockés sur aucun serveur et sont supprimés de votre appareil après avoir disparu.

Sauvegardez vos données

Prenez des précautions pour limiter les coûts potentiels liés à la perte de l'accès à votre appareil, qu'il soit perdu, volé ou confisqué par les forces de l'ordre. Sauvegardez régulièrement vos données et stockez cette sauvegarde dans un endroit sûr pour vous éviter des maux de tête plus tard.

Téléphone graveur

Pour les manifestants inquiets de voir leurs téléphones traqués, une solution temporaire, mais idéale serait de se procurer un « téléphone graveur », un appareil prépayé payé en espèces

146 https://www.torproject.org/
147 https://source.android.com/security/encryption/full-disk.html
148 https://www.apple.com/business/docs/iOS_Security_Guide.pdf
149 https://ssd.eff.org/en/module/how-use-signal-ios
150 https://ssd.eff.org/en/module/how-use-signal-android

et utilisé dans le but exprès de rester en contact avec les gens lors d'une manifestation pacifique. Les téléphones Burner peuvent offrir aux utilisateurs l'avantage de pouvoir rester en contact avec les gens – surtout si les choses deviennent risquées – sans exposer toutes les données de leur appareil quotidien. Alternativement, mettre votre téléphone en mode avion pourrait avoir le même objectif.[151]

Sécurité physique

Les menaces physiques contre les défenseurs des droits numériques sont aussi réelles que les menaces à la sécurité numérique. Ces menaces vont des arrestations, au harcèlement, à la confiscation des appareils et à la détention par des acteurs étatiques. Cela les expose à un risque potentiellement élevé, un facteur qui met en péril leur sécurité. Afin d'atténuer les menaces à la sécurité physique, les défenseurs des droits numériques sont invités à être attentifs aux signes de menaces pour leur sécurité personnelle, en tenant compte de leur environnement, des lois et du type de personnes composant la communauté. La règle générale est la suivante: pour qu'un acteur des droits numériques réussisse à protéger les autres, sa propre sécurité doit être garantie.

3.2.

Atténuer les menaces à la sécurité physique

Pour atténuer les risques, les acteurs des droits numériques sont encouragés à prendre en considération les éléments suivants:

Accepter le risque: La victime qui a besoin de protection doit pouvoir savoir qu'elle peut courir un risque dans l'exercice de ses activités. Avec une telle conscience, la personne devrait être prête à atténuer le risque ou le potentiel de risque. Par exemple, lorsque vous partez en mission humanitaire dans une zone de guerre, vous devez savoir que votre sécurité est en jeu ; vous devez donc être prêt à courir si nécessaire, à appeler à l'aide et vous devez contacter et expliquer votre mission aux combattants impliqués dans les combats afin qu'ils puissent vous accorder l'accès à la zone. De plus, lorsque vous savez que vos données peuvent être exposées à un risque de cyberattaque, vous devez créer un mot de passe fort, vérifier les plateformes numériques que vous comptez utiliser, partager vos données avec des personnes de confiance et également stocker vos données sur différents supports. périphériques de stockage.

Éviter le risque: Connaître le risque est une chose et l'éviter en est une autre. Lorsque vous découvrez un risque, vous devez l'éviter par tous les moyens; vous n'avez pas besoin de revendiquer des droits ou du pouvoir à ce moment-là. Pour éviter tout risque, votre communication et vos actions doivent refléter et changer en fonction de la situation dans laquelle vous vous trouvez. Vous devez vérifier votre langage corporel et utiliser vos mots à bon escient, vous devez évaluer l'environnement avant de commencer des activités ou de vous engager avec des gens, vous devez

151 https://ssd.eff.org/en/module/attending-protest

comprendre s'il existe un risque potentiel ou non, et enfin, lorsque cela prouve que vous êtes une cible, vous devez réagir farouchement pour résister à votre agresseur.

Présentez votre idéologie aux bonnes personnes: Votre idéologie peut présenter un risque lorsque vous la faites connaître. En tant que défenseur des droits de l'homme, vous devez savoir à qui confier vos informations ou à qui vous associer, car les gens ne sont pas obligés d'accepter vos idées.

Informations d'identification personnelles et organisationnelles: en tant que porte-parole d'une organisation ou de son représentant dans un environnement potentiellement dangereux, il est important de disposer d'informations telles que qui vous êtes, ce que vous faites et les personnes que vous représentez.

De telles preuves s'avèrent très utiles dans les cas où vous pourriez être placé en garde à vue en tant que suspect. Très souvent, la façon dont vous vous présentez, votre position et votre organisation ont une influence significative sur la façon dont vous serez traité par vos ravisseurs. Dans la plupart des cas, les suspects innocents seront libérés après s'être correctement présentés. Le langage corporel, le choix des mots et le sang-froid doivent être bien gérés pendant l'arrestation et l'enquête.

Conscience situationnelle/ environnementale: En cas de problème, vous devez rester conscient de votre environnement à tout moment, en tenant compte de votre propre rôle, de l'endroit où vous vous trouvez et de qui sont vos adversaires. Ce sont des questions importantes à prendre en compte dans une situation délicate pour garantir votre sécurité. Par exemple, un défenseur des droits de l'homme ne peut pas se trouver dans une caserne militaire et condamner les atrocités commises par les soldats.

Évitez les zones à risque: les zones telles que les limites des villes, les foules, les banques, les zones de circulation, les rassemblements publics, les zones de conflit ou de guerre sont des zones à risque et vous devez considérer les moments appropriés pour visiter ces zones, en tenant compte de votre profession et de votre position. Par exemple, il n'est pas conseillé à un militant des droits de l'homme de se rendre dans des zones de conflit sans garantie de sécurité de la part des belligérants.

Par exemple, dans les régions anglophones du Cameroun où éclate un conflit entre les séparatistes et les forces gouvernementales, pour des raisons de sécurité, les travailleurs humanitaires ne peuvent pas accéder aux zones de confrontation sans l'assurance d'un passage sûr de la part des combattants. En effet, ils risquent d'être blessés par des balles perdues, arrêtés ou kidnappés s'ils ne bénéficient pas de l'assurance de leur sécurité de la part des combattants.

Vêtements: vous devez être conscient de votre apparence et comprendre comment vous habiller lorsque vous menez des activités humanitaires. Par exemple, lorsque vous partez travailler sur le terrain, vous devez porter des chaussures légères et vous habiller de manière à pouvoir facilement vous échapper ou courir lorsque vous en avez besoin. Si votre zone

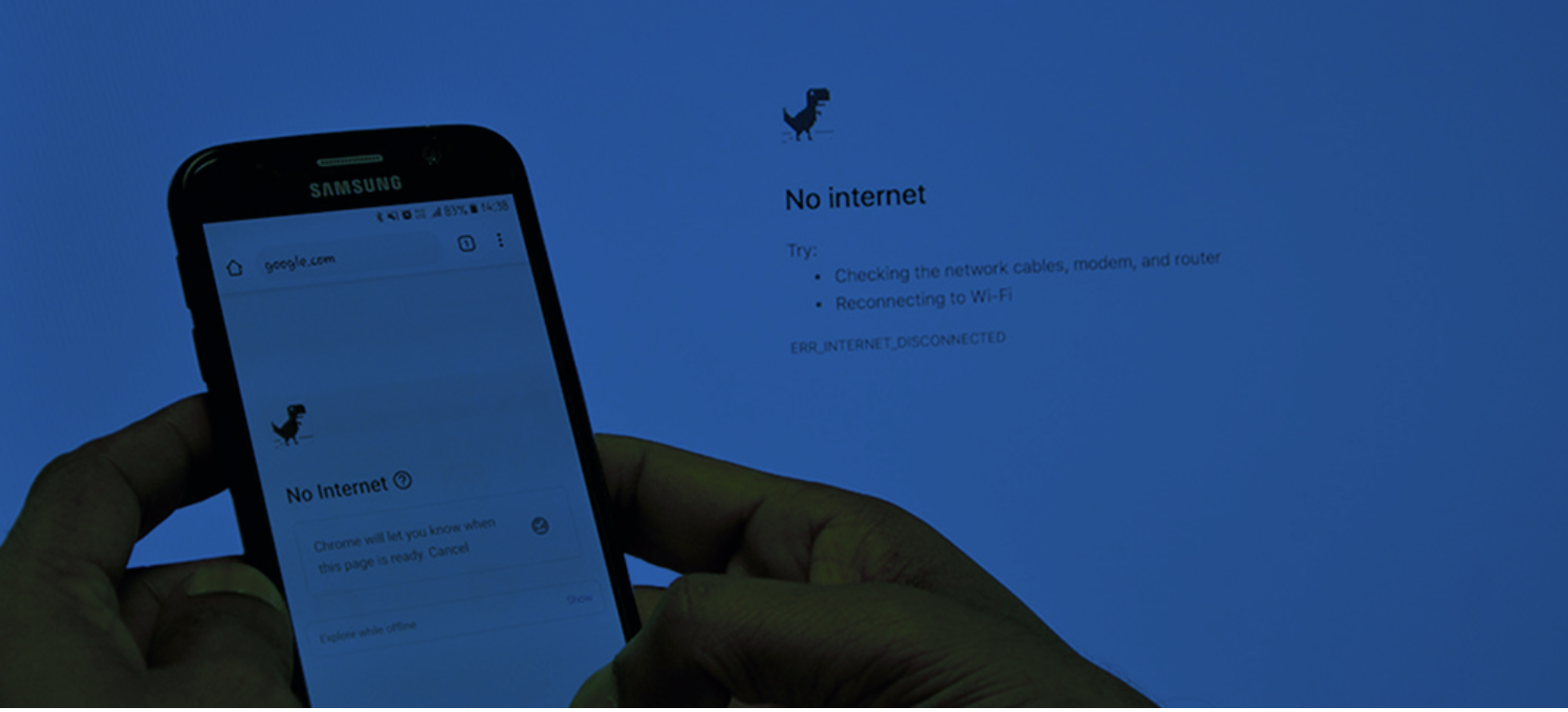
n'est pas sécurisée, évitez de vous habiller cher, car vous pourriez être ciblé en fonction de la façon dont vous vous habillez.

Ne résistez pas sous la menace d'une arme ou dans une caserne militaire: lorsque vous êtes arrêté, kidnappé ou encerclé, faites tout ce qu'on vous dit pour protéger votre vie. Ne résistez pas et pensez d'abord à votre sécurité.

Soyez prêt à tout: Chaque fois que vous partez en mission, évaluez les risques possibles et emportez avec vous une trousse de premiers secours et toutes les nécessités en quantité raisonnable en fonction de votre état de santé, de votre voyage, des conditions climatiques, de vos besoins financiers, etc, pour votre sécurité physique.

Ayez toujours un contact de confiance: dans les activités risquées telles que l'activisme en faveur des droits de l'homme, vous devez vous préparer au risque d'arrestation, d'enlèvement ou d'attaque contre vos données. À titre de mesure d'atténuation, vous devez avoir un ou plusieurs collègues de confiance avec qui vous pouvez partager vos informations, votre destination, l'heure à laquelle vous êtes censé être là, l'heure à laquelle vous êtes censé être de retour et ce qu'il faut faire en cas de problème d'urgence.

Numéros d'urgence et suivi: conservez les contacts de la police, des services d'ambulance, des pompiers, de l'hôpital, etc. dans un endroit sûr. Téléchargez et installez des applications capables de suivre votre appareil lorsque vous rencontrez des problèmes.



CHAPITRE IV | COUPURES D'INTERNET

L'article 19 de la Déclaration universelle des droits de l'homme garantit à chacun le droit à la liberté d'opinion et d'expression ; ce droit inclut la liberté d'avoir des opinions sans ingérence et de rechercher, recevoir et communiquer des informations et des idées par tous les médias et sans considération de frontières. Cependant, ces dernières années, les États africains ont eu de plus en plus tendance à perturber l'accès à l'information en ligne. Cela a transformé Internet en un espace plus volatil, et les défis posés aux militants, aux défenseurs des droits humains, aux dissidents et aux journalistes seraient en augmentation.

Les régimes autoritaires ont eu recours à des outils et tactiques numériques tels que les coupures d'Internet, la censure en ligne et la surveillance numérique pour réprimer la liberté d'expression. Selon Access Now, en 2022, au moins 35 pays ont fermé Internet au

152 https://www.accessnow.org/press-release/keepiton-internet-shutdowns-2022-africa/

moins 187 fois.[152] Il s'agit jusqu'à présent du nombre le plus élevé jamais enregistré en une seule année. En 2023, en septembre, au moins 12 coupures d'Internet ont eu lieu en Afrique subsaharienne, étouffant la liberté d'expression et limitant l'accès à l'information, en particulier pendant les élections et les périodes de protestation publique,[153] pour un coût de 200 millions de dollars. À l'échelle mondiale, les coupures d'Internet ont entraîné un coût total de 10 milliards de dollars en 2022.[154]

En outre, un rapport de Paradigm Initiative 2019[155] a révélé qu'un certain nombre de gouvernements africains ont fermé Internet pour des raisons politiques, adopté des réglementations strictes sur le contenu en ligne et/ou eu recours à des attaques ciblées de logiciels espions contre les défenseurs des droits humains. Le rapport PIN Londa 2023 a souligné que cinq des 26 pays concernés ont fermé Internet.[156]

Le rapport ajoute que l'exportation des modèles chinois et russes de tactiques dites de « primauté du droit » pour le contrôle d'Internet a entraîné un renforcement du contrôle gouvernemental et des violations des droits numériques par le biais d'une législation ostensiblement écrite pour promouvoir l'ordre public dans les sociétés africaines.

Les fermetures ont eu des conséquences économiques négatives dans les pays en question. Une étude de Deloitte[157] révèle que pour un pays hautement connecté, l›impact quotidien d›une coupure temporaire d›Internet et de tous ses services s›élèverait en moyenne à 23,6 millions de dollars pour 10 millions d›habitants. En 2023, les coupures d'Internet continueront d'être coûteuses, un pays comme l'Éthiopie perdant environ 1,59 milliard de dollars.[158] Cependant, le coût global des coupures d'Internet en 2023 a diminué de 67 % par rapport à 2022, mais a augmenté de 45 % par rapport à 2021. Les durées de coupure ont augmenté de 18 % par rapport à 2022 et une augmentation significative de 71,5 % par rapport à 2021.[159]

Malgré cette décision de divers États de réprimer les espaces numériques et, ce faisant, de limiter le travail de ceux qui sont en première ligne de la défense des droits humains et numériques, un certain nombre d'outils d'anonymat et de contournement sur Internet, tels que les VPN et les proxys Web, offrent de l'espoir aux humains. acteurs des droits, défenseurs des droits numériques, journalistes et lanceurs d'alerte.

153 https://rsf.org/en/how-internet-shutdowns-undermine-journalism-sub-saharan-africa
154 https://technext24.com/2022/12/14/internet-shutdowns-cost-sub-saharan-africa/
155 http://paradigmhq.org/download/dra19/
156 https://paradigmhq.org/londa/
157 https://www2.deloitte.com/global/en/pages/technology-media-and-telecommunications/articles/the-economic-impact-of-disruptions-to-internet-connectivity-report-for-facebook.html
158 https://www.forbes.com/sites/emmawoollacott/2024/01/04/government-internet-shutdowns-bring-huge-economic-costs/?sh=557e1b654e44
159 https://www.forbes.com/sites/emmawoollacott/2024/01/04/government-internet-shutdowns-bring-huge-economic-costs/?sh=557e1b654e44

4.1.

Contourner les coupures d'Internet et la censure

Réseau privé virtuel (Virtual Private Network - VPN)

Comme déjà évoqué au chapitre II sous la rubrique Sécurité numérique, un VPN est une méthode permettant de connecter en toute sécurité votre appareil connecté à Internet au réseau d'une organisation ailleurs sur Internet. Lorsque vous utilisez un VPN, toutes vos communications Internet sont regroupées, cryptées, puis relayées vers cette organisation, où elles sont décryptées, décompressées, puis envoyées vers leur destination. Pour le réseau de l'organisation ou tout autre ordinateur sur Internet au sens large, il semble que la demande de votre ordinateur provient de l'intérieur de cette organisation et non de votre emplacement. Les VPN sont utilisés par des particuliers pour contourner la censure locale ou pour vaincre la surveillance locale.

Navigateur Tor

Tor[160] est un logiciel gratuit et open source permettant la communication anonyme. Le nom est dérivé de l'acronyme du projet logiciel original « The Onion Router ». Tor possède des fonctionnalités intégrées qui vous protègent du suivi, de la surveillance et des empreintes digitales sur le Web.

DuckDuckGo

Un moteur de recherche Internet qui met l'accent sur la protection de la vie privée des chercheurs et évite la bulle de filtre des résultats de recherche personnalisés. DuckDuckGo[161] se distingue des autres moteurs de recherche en ne profilant pas ses utilisateurs et en affichant à tous les utilisateurs les mêmes résultats de recherche pour un terme de recherche donné.

Modification des paramètres du système de noms de domaine (Domain Name System - DNS)

En cas d'empoisonnement/usurpation d'identité DNS,[162] souvent infligé par les fournisseurs de services Internet, la modification des paramètres DNS peut aider à contourner la censure DNS. Les gouvernements sont parfois à l'avant-garde de l'empoisonnement du DNS afin de limiter le contenu auquel leurs citoyens ont accès.

4.2.

Mesurer les coupures d'Internet et la censure

L'Observatoire Ouvert des Interférences de Réseau (Open Observatory of Network Interference - OONI)

OONI est un projet de logiciel libre qui vise

160 https://www.torproject.org/download/
161 https://duckduckgo.com/
162 https://www.fortinet.com/resources/cyberglossary/dns-poisoning

à renforcer les efforts décentralisés visant à accroître la transparence de la censure sur Internet dans le monde. OONI développe un logiciel gratuit et open source[163] appelé OONI Probe pour détecter:

- Blocage de sites Web ;
- Blocage des applications de messagerie instantanée (WhatsApp, Facebook Messenger et Telegram) ;
- Blocage des outils de contournement de la censure (tels que Tor et Psiphon) ;
- Présence de systèmes (middlebox) dans votre réseau qui pourraient être responsables de la censure et/ou de la surveillance ; et
- Vitesse et performances de votre réseau.

En exécutant OONI Probe,[164] vous pouvez collecter des données qui peuvent potentiellement servir de preuve de censure sur Internet, car elles montrent comment, quand, où et par qui elle est mise en œuvre. Des informations sur les tendances de la censure sur Internet sont disponibles sur la plateforme de résultats de censure de l'OONI.[165]

Analyse des pannes Internet et de la détection (Internet Outage and Detection Analysis - IODA)

IODA surveille Internet et détecte les pannes de connectivité Internet en temps réel sur un tableau de bord interactif [166] des pannes Internet qui permet aux utilisateurs de suivre les pannes Internet dans le monde.

Laboratoire de mesure (Measurement Lab: M-Lab)

M-Lab[167] permet une mesure ouverte et vérifiable des performances du réseau mondial. Grâce à M-Lab, les utilisateurs peuvent mesurer les performances de leur connexion Internet pour vérifier la vitesse d'Internet. Cela permet de détecter la limitation des vitesses Internet.

4.3.

Plaidoyer contre les coupures d'Internet en Afrique

Outil de coût d'arrêt NetBlocks (Cost of Shutdown Tool - COST)

Un outil en ligne basé[168] sur des données pour mesurer le coût des coupures d'Internet et convaincre les gouvernements de maintenir Internet actif.

L'outil permet à quiconque – y compris les journalistes, les chercheurs, les militants, les décideurs politiques, les entreprises et bien d'autres – d'estimer rapidement et facilement les coûts économiques des coupures

163 https://github.com/ooni/probe
164 https://ooni.org/install/
165 https://explorer.ooni.org/findings
166 https://ioda.inetintel.cc.gatech.edu/dashboard
167 https://speed.measurementlab.net/#/
168 https://netblocks.org/cost/
169 https://netblocks.org/reports
170 https://www.accessnow.org/campaign/keepiton/

d'Internet, des pannes de données mobiles et des restrictions des médias sociaux à l'aide de milliers d'indicateurs régionaux de la Banque mondiale. UIT, Eurostat et recensement américain. Netblocks[169] est un site mondial de surveillance Internet qui fournit des analyses et des rapports sur les ralentissements, les arrêts et la censure d'Internet.

Campagne #KeepItOn

Cette campagne mondiale[170] menée par AccessNow vise à exhorter les gouvernements du monde entier à ne pas fermer Internet et à permettre la libre circulation de l'information.

Jeu d'arrêt d'Internet

L'Association for Progressive Communications a développé un jeu[171] interactif sur les coupures d'Internet qui met en lumière différents types de coupures d'Internet et les moyens de les contrecarrer. Le jeu s'adresse aux défenseurs des droits de l'homme, au grand public et aux professionnels du droit.

171 https://shutdowngame.apc.org/
172 https://ssd.eff.org/module/choosing-vpn-thats-right-you

GLOSSAIRE

Module complémentaire - un logiciel qui modifie d'autres logiciels en changeant leur fonctionnement ou ce qu'ils peuvent faire. Souvent, les modules complémentaires peuvent ajouter des fonctionnalités de confidentialité ou de sécurité aux navigateurs Web ou aux logiciels de messagerie. Certains modules complémentaires sont des logiciels malveillants, alors veillez à n'installer que ceux qui sont réputés et proviennent de sources officielles.

Anonymat – La condition d'être anonyme.

Antivirus - logiciel antivirus utilisé pour prévenir, détecter et supprimer les logiciels malveillants, notamment les virus informatiques, les vers et les chevaux de Troie. Quelques exemples de logiciels antivirus sont McAfee, Avast, AVG et Kaspersky.

Censure – La censure sur Internet est le contrôle ou la suppression de ce qui peut être consulté, publié ou visualisé sur Internet, édicté par les régulateurs et/ou les gouvernements.

Contournement – Utilisation de diverses méthodes et outils pour contourner la censure sur Internet.

Cryptographie – L'art de concevoir des codes secrets qui vous permettent d'échanger des messages avec un destinataire sans que d'autres puissent comprendre le message.

Hygiène numérique - Fait référence à des étapes telles que l'organisation des fichiers sur votre PC, le verrouillage de vos comptes de réseaux sociaux, l'introduction de nouvelles applications ou technologies pour rendre votre vie numérique plus facile ou plus sécurisée.

Droits numériques – Les droits numériques sont essentiellement des droits de l'homme à l'ère d'Internet.

Chiffrement - Processus qui prend un message et le rend illisible, sauf pour une personne sachant comment le « déchiffrer » pour le rendre lisible.

Clé de cryptage - Une clé de cryptage est un élément d'information utilisé pour convertir un message sous une forme illisible. Dans certains cas, vous avez besoin de la même clé de cryptage pour décoder le message. Dans d'autres, la clé de cryptage et la clé de déchiffrement sont différentes.

Pare-feu - Un outil qui protège un ordinateur des connexions indésirables vers ou depuis les réseaux locaux et Internet. Un pare-feu peut avoir des règles qui interdisent les e-mails sortants ou les connexions à certains sites Web. Les pare-feu peuvent être utilisés comme première ligne de défense pour protéger un appareil contre les interférences inattendues. Ils peuvent également être utilisés pour empêcher les utilisateurs d'accéder à Internet de certaines manières.

File Transfer Protocol (FTP) - Protocole réseau standard utilisé pour le transfert de fichiers d'un hôte à un autre sur un réseau basé sur le protocole de contrôle de transmission, tel qu'Internet.

Coupure d'Internet – Une coupure d'Internet est une interruption intentionnelle d'Internet ou des communications électroniques, les rendant inaccessibles ou effectivement inutilisables pour une population spécifique ou au sein d'un lieu, souvent pour exercer un contrôle sur le flux d'informations.

Adresse IP – Une adresse de protocole Internet est ce qui identifie de manière unique les appareils connectés sur Internet.

Malware – Logiciel malveillant : programmes conçus pour effectuer des actions indésirables sur votre appareil. Les virus informatiques sont des logiciels malveillants. Il en va de même pour les programmes qui volent des mots de passe, vous enregistrent secrètement ou suppriment vos données.

Système d'exploitation (OS) — Un programme qui exécute tous les autres programmes sur un ordinateur ou un appareil. Windows, Linux, Android, HarmonyOS et OS X et iOS d'Apple sont tous des exemples de systèmes d'exploitation.

Gestionnaire de mots de passe - Un outil qui crée et stocke des mots de passe afin que vous puissiez utiliser de nombreux mots de passe différents sur différents sites et services sans avoir à les mémoriser.

Phrase secrète - Une phrase secrète est plus longue qu'un mot de passe, qui

est généralement un seul mot.

PC (ordinateur personnel) – Un ordinateur polyvalent.

PGP - Pretty Good Privacy a été l'une des premières implémentations populaires de cryptographie à clé publique pour aider les militants et autres à protéger leurs communications.

Proxy – Une application ou un appareil serveur qui agit comme intermédiaire pour les demandes des clients recherchant des ressources auprès des serveurs qui fournissent ces ressources. Un serveur proxy fonctionne ainsi pour le compte du client lors de la demande de service, masquant potentiellement la véritable origine de la demande au serveur de ressources.

Question de sécurité – Questions liées au mot de passe dont vous seul êtes censé connaître les réponses.

Logiciel – Terme générique désignant les applications, scripts et programmes exécutés sur un appareil.

TCP (Transmission Control Protocol) — Norme de communication qui permet aux programmes d'application et aux appareils informatiques d'échanger des messages sur un réseau.

Telnet (réseau télétype) — Telnet est un protocole d'application client/serveur qui permet d'accéder aux terminaux virtuels de systèmes distants sur des réseaux locaux ou sur Internet.

Tor - Logiciel gratuit et open source permettant la communication anonyme. Le nom est dérivé d'un acronyme pour le nom original du projet logiciel «The Onion Router».

Authentification à deux facteurs - 2FA est un moyen de permettre aux utilisateurs de s'identifier auprès d'un fournisseur de services en exigeant une combinaison de deux méthodes d'authentification différentes. Il peut s'agir de quelque chose que l'utilisateur connaît (comme un mot de passe ou un code PIN), quelque chose qu'il possède (comme un jeton matériel ou un téléphone mobile), ou quelque chose qui est attaché ou indissociable de l'utilisateur (comme ses empreintes digitales).

URL (Uniform Resource Locator) — L'adresse d'une page Web.

UDP (User Datagram Protocol) — protocole de communication utilisé sur

Internet pour les transmissions particulièrement sensibles au temps, telles que la lecture vidéo ou les recherches DNS.

Réseau privé virtuel – Un VPN est utilisé pour se connecter à Internet via un tunnel crypté. Votre FAI ou toute personne reniflant le Wi-Fi gratuit que vous utilisez pour accéder au Web, ne peut voir que votre connexion au service VPN, tandis que le site Web que vous visitez n'enregistrera qu'une connexion à partir des serveurs VPN. Différentes options de VPN sont disponibles, en fonction de vos besoins.[172]

Virus - Un virus PC est un morceau de code capable de se copier et qui a généralement un effet néfaste, comme la corruption d'un système informatique ou la destruction de données.

Proxy basé sur le Web — un site Web qui permet à ses utilisateurs d›accéder à d›autres sites Web bloqués ou censurés. Habituellement, le proxy Web vous permettra de saisir une adresse Web (ou URL) sur une page Web, puis de réafficher cette adresse Web sur la page proxy. Il est plus facile à utiliser que la plupart des autres services permettant de contourner la censure.