DCAF Le Centre pour la gouvernance du secteur de la sécurité, Genève

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTÈRE DE L'EUROPE ET DES AFFAIRES ÉTRANGÈRES

DCSD
PARTENAIRE POUR UNE SÉCURITÉ DURABLE

ECOLE NATIONALE DE CYBERSECURITE A VOCATION REGIONALE

Guide pour la bonne gouvernance de la cybersecurité

Table des matières

Équipes de réponse aux incidents informatiques en Afrique

Sources : Union internationale des télécommunications (UIT), Banque mondiale, AfricaCERT, FIRST – M.A.J. septembre 2019

Afrique du Sud
- National Team: https://www.cybersecurityhub.gov.za
- The South African National Research Network : https://csirt.sanren.ac.za/
- UCT CSIRT - University of Cape Town : https://csirt.uct.ac.za/
- ECS-CSIRT - Electronic Communications Security (State Security Agency)
- SBG CSIRT - Standard Bank Group CSIRT

Algérie
- DZ-CERT : http://www.cerist.dz

Angola
- En cours de création au sein de l'Information Society Development Institute (INFOSI)

Bénin
- bjCSIRT (ANSSI-Bénin) : https://csirt.gouv.bj/

Botswana
- En cours de création au sein du Ministry of Transport and Communication (MTC)

Burkina Faso
- CIRT.BF : http://www.cirt.bf

Burundi
- En cours de création avec l'aide de l'Union internationale des télécommunications (UIT)

Cameroun
- CIRT (Agence nationale des TIC – ANTIC) : http://www.cirt.cm

Cap-Vert - Aucun

Centrafrique - Aucun

Comores - Aucun

Congo - Aucun

Congo (RDC) - Aucun

Côte d'Ivoire
- CI-CERT : http://www.cicert.ci

Djibouti
- En cours de création au sein de la Direction de la sécurité des systèmes d'information (DSSI) de l'Agence nationale des systèmes d'information de l'Etat (ANSIE)

Egypte
- EG-CERT (National Telecom Regulatory Authority – NTRA) : http://www.egcert.eg/

Erythrée - Aucun

Eswatini (Swaziland) - Aucun

Ethiopie
- Ethio-CERT (Information Network Security Agency) : http://ethiocert.insa.gov.et

Gabon
- En cours de création au sein de l'Agence Nationale des Infrastructures Numériques et des Fréquences (ANINF)

Gambie - Aucun

Ghana
- National Team: CERT-GH : https://www.cert-gh.org/
- National Communication Authority : https://nca-cert.org.gh/

Guinée
- En cours de création au sein de l'ANSSI-Guinée

Guinée-Bissau - Aucun

Guinée équatoriale - Aucun

Kenya
- National KE-CIRT / CC (The Communications Authority of Kenya) : http://www.ca.go.ke ou http://www.ke-cirt.go.ke/
- ICIRT Tespok : https://www.tespok.co.ke /
- KENET-CERT : https://cert.kenet.or.ke/

Lesotho - Aucun

Liberia - Aucun

Libye
- LibyaCERT : https://nissa.gov.ly

Madagascar - Aucun

Malawi
- En cours de création avec l'aide de l'Union internationale des télécommunications (UIT) au sein de la Malawi Communications Regulatory Authority

Mali - Aucun

Maroc
- Academia EDU-CERT : http://www.educert.ma/
- Gouvernement maCERT (DGSSI) : http://www.dgssi.gov.ma/macert.html

Maurice
- CERT-MU (National Computer Board) : http://www.cert-mu.org.mu

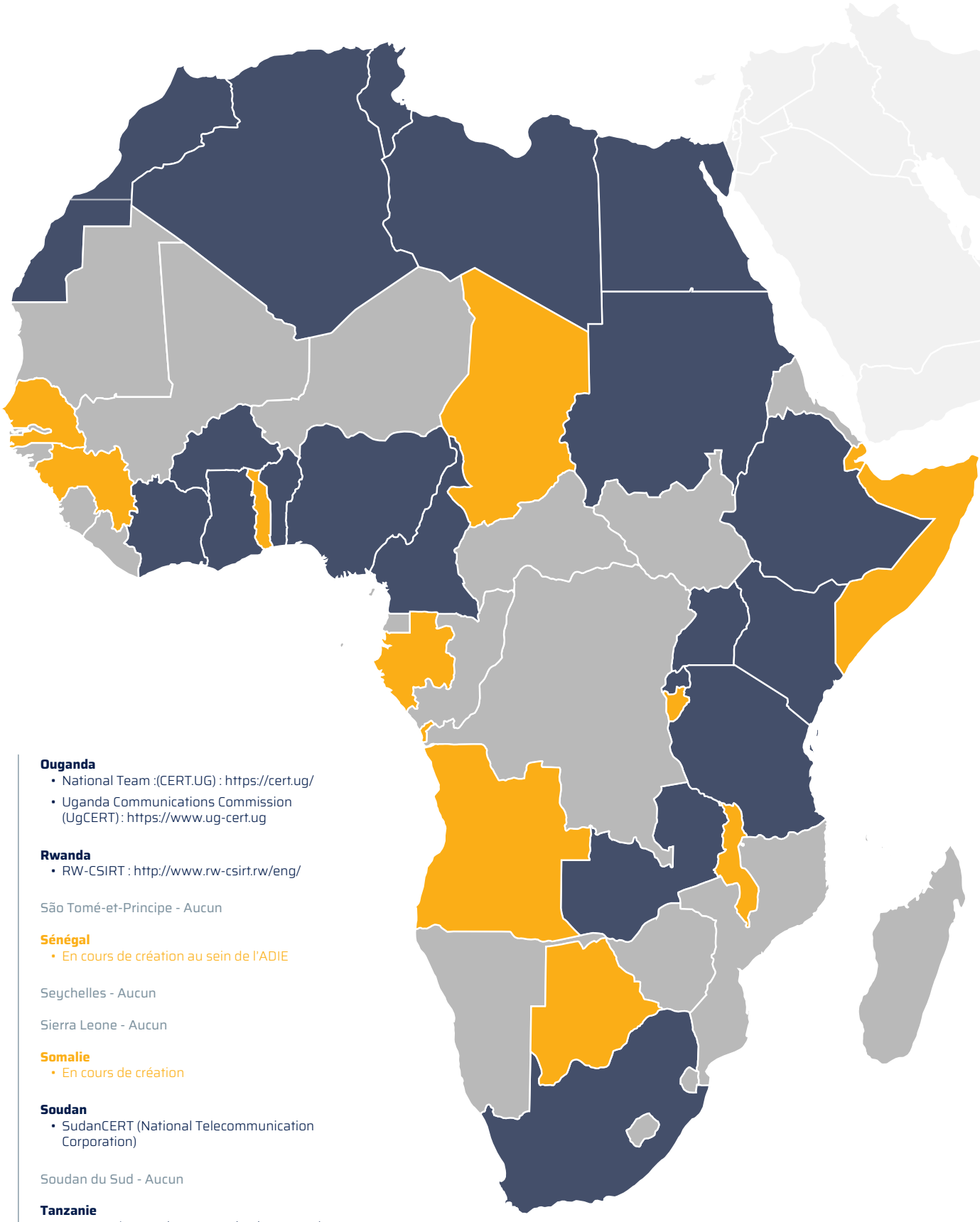
Mauritanie - Aucun

Mozambique
- Mozambique Research and Education Network, MoRENet : https://cert.morenet.ac.mz/

Namibie - Aucun

Niger - Aucun

Nigéria
- National Team – ngCERT : http://www.cert.gov.ng
- CERRTng (Office of National Security Adviser - ONSA) : http://www.cerrt.ng/



Ouganda
- National Team :(CERT.UG) : https://cert.ug/
- Uganda Communications Commission (UgCERT) : https://www.ug-cert.ug

Rwanda
- RW-CSIRT : http://www.rw-csirt.rw/eng/

São Tomé-et-Principe - Aucun

Sénégal
- En cours de création au sein de l'ADIE

Seychelles - Aucun

Sierra Leone - Aucun

Somalie
- En cours de création

Soudan
- SudanCERT (National Telecommunication Corporation)

Soudan du Sud - Aucun

Tanzanie
- TZ-CERT (Tanzania Communications Regulatory Authority) : http://www.tzcert.go.tz

Tchad
- En cours de création avec l'aide de l'Union internationale des télécommunications (UIT) au sein de l'Agence Nationale de Sécurité Informatique et de Certification Electronique (ANSICE)

Togo
- En cours de création au sein de l'Agence nationale de cybersécurité (ANCY)

Tunisie
- tunCERT : https://tuncert.ansi.tn
- CSIRT.TN (Private) : https://csirt.tn/

Zambie
- ZmCIRT (Zambia Information and Communication Technology Authority) : http://www.cirt.zm

Zimbabwe - Aucun

Introduction générale

La généralisation de l'accès au cyberespace et à ses ressources, touchant de façon croissante les utilisateurs dans leur quotidien, a un impact considérable sur notre société. Elle a déjà profondément transformé les modes de vie individuels et collectifs dans le monde entier. Si le cyberespace offre d'innombrables opportunités de développement économique, social et politique, il a également permis à des acteurs étatiques et non étatiques de disposer de nouveaux outils leur permettant de mener des opérations de surveillance, de collecter et d'exploiter une quantité sans précédent de données personnelles, d'influencer les processus démocratiques, de commettre des crimes et de modifier les moyens et les méthodes de la guerre.

Ces défis requièrent des réponses multiples, rassemblant les gouvernements, le secteur privé et la société civile afin de répondre aux enjeux de la gouvernance de la cybersécurité. Par ailleurs, les cadres législatifs, politiques et de gouvernance, devront s'adapter pour mieux respecter les droits humains, tout en luttant de manière efficace contre le développement de la cybercriminalité, des actes de cyber malveillance, des cyber-attaques et l'utilisation d'internet à des fins terroristes et de promotion de l'extrémisme violent. Seule une action énergique en ce sens permettra de promouvoir un cyberespace sûr, stable et ouvert.

C'est dans ce contexte que la direction de coopération de sécurité et de défense (DCSD) du ministère de l'Europe et des Affaires étrangères français et du Centre pour la gouvernance du secteur de la sécurité, Genève (DCAF) ont lancé en 2018 le projet de rédaction d'un guide de bonnes pratiques pour la promotion de la bonne gouvernance dans le cyberespace.

La DCSD est en effet active depuis plusieurs années dans le renforcement des capacités en cybersécurité de ses partenaires à travers le monde et notamment en Afrique. La France soutient, en partenariat avec le Sénégal, le projet d'école nationale à vocation régionale (ENVR) de formation en cybersécurité à Dakar, qui commencera ses programmes de formation en 2019 à destination des Etats africains. L'ENVR de cybersécurité proposera notamment, pour un public de hauts cadres et responsables administratifs, des formations sur la gouvernance de la cybersécurité et les enjeux juridiques de la cybersécurité pour les Etats africains. Cet enseignement portera sur les conventions internationales et régionales en matière de cybersécurité, ainsi que les politiques publiques à concevoir et mettre en œuvre dans ce domaine, qu'il s'agisse de stratégies nationales et plans d'action ou de coordination régionale.

Afin d'appuyer ce projet, la DCSD a retenu une action proposée par le DCAF visant à concevoir un guide de bonnes pratiques pour la promotion de la bonne gouvernance de la cybersécurité, qui pourra servir d'étude de référence sur le sujet, de support pédagogique pour les formations sur la gouvernance de la cybersécurité de l'ENVR et de base à une formation en ligne.

Ce guide permettra aussi de diffuser les pratiques de bonne gouvernance promues par le DCAF, auprès d'un public de décideurs et de responsables des systèmes d'information africains. A cette fin, ce guide se base sur des études de cas traitant des questions relatives à la bonne gouvernance de la cybersécurité, centrées sur l'Afrique francophone. Il se fonde également sur les problématiques rencontrées dans ce domaine au niveau de l'Union africaine et des différentes organisations sous-régionales africaines.

Cet ouvrage se compose de six chapitres qui explicitent la portée pratique des concepts de la cybersécurité appliqués à la bonne gouvernance. Chacun se fonde sur de nombreux cas pratiques tirés de l'expérience des Etats africains. Les chapitres sont dédiés aux sujets suivants :

- la bonne gouvernance du secteur de la sécurité et son application au cyberespace ;
- le lien entre cyberespace, cybersécurité et gouvernance du secteur de la sécurité ;
- les cadres juridiques internationaux et régionaux applicables au cyberespace ;
- l'application des normes internationales et régionale au plan national de cybersécurité ;
- les stratégies nationales de cybersécurité ;
- favoriser une coopération efficace entre secteur public et secteur privé dans le cyberespace.

Ce guide des bonnes pratiques de la gouvernance de la cybersécurité sera ainsi une première contribution internationale au lancement du programme de formations de l'ENVR de cybersécurité de Dakar.

Dakar / Paris / Genève, novembre 2019

CHAPITRE 1

LA BONNE GOUVERNANCE DU SECTEUR DE LA SÉCURITÉ : INTRODUCTION

Objectifs

Ce chapitre vise à renforcer les connaissances et la compréhension de certains termes clés relatifs à la bonne gouvernance du secteur de la sécurité, afin de montrer comment ces notions s'appliquent au contexte du cyberespace. À cette fin, le présent chapitre se focalise sur trois composantes essentielles de la bonne gouvernance du secteur de la sécurité qui sont également pertinentes pour le cyberespace :

- a. La responsabilité ;
- b. la transparence ;
- c. l'État de droit.

Après une introduction de ces concepts, ce chapitre souligne certains défis spécifiques liés à la promotion de l'application de ces principes de bonne gouvernance au cyberespace et il présente plusieurs bonnes pratiques en la matière.

Ce chapitre vise à améliorer la compréhension des questions clés suivantes:

- Concepts et définitions clés relatifs à la gouvernance, à la gouvernance du secteur de la sécurité et à la bonne gouvernance du secteur de la sécurité.
- Concepts sous-tendant les principes de bonne gouvernance, tels que la responsabilité, la transparence et l'État de droit.
- Principes sous-tendant la bonne gouvernance du secteur de la sécurité.
- Importance de promouvoir l'application du principe de bonne gouvernance au cyberespace.

1. Introduction

Gouvernance, gouvernance du secteur de la sécurité et bonne gouvernance du secteur de la sécurité

La gouvernance renvoie à « l'exercice du pouvoir et de l'autorité ». De manière générale, le concept de gouvernance fait référence aux règles qui régissent toute organisation, y compris les entreprises privées à but lucratif et les entités à but non lucratif. Appliquée au secteur de la sécurité, la notion de « gouvernance » renvoie à l'ensemble des décisions, processus et acteurs formels et informels qui ont un impact sur la prestation de services publics, tels que la santé, l'éducation ou la sécurité.

La gouvernance du secteur de la sécurité (GSS) renvoie à « l'exercice du pouvoir et de l'autorité dans le contexte d'un secteur de sécurité nationale en particulier[1] ». Il s'agit d'un concept analytique qui ne repose pas sur un engagement à respecter des normes ou des valeurs spécifiques.

Le concept de bonne GSS renvoie aux actions mises en œuvre pour optimiser l'efficacité et la responsabilité du secteur de la sécurité étatique dans le cadre d'un contrôle civil et démocratique et dans le respect de l'État de droit et du principe de l'État de droit[2]

> La bonne gouvernance du secteur de la sécurité renvoie spécifiquement à l'application des principes de bonne gouvernance à la prestation, à la gestion et au contrôle des services de sécurité, dans un contexte national donné.

En outre, le concept de bonne GSS repose sur l'idée selon laquelle le secteur de la sécurité doit être tenu de respecter les mêmes normes élevées que celles imposées aux autres prestataires de services du secteur public. Par conséquent, le non-respect de ces normes par le secteur de la sécurité peut nuire à la stabilité politique, économique et sociale d'un État (on parle également dans ce cas de « mauvaise GSS »).

1 DCAF, Document d'information sur la réforme du secteur de la sécurité (cf. Bibliographie).

2 Ibid.

Qu'est-ce que le secteur de la sécurité ?

En général, le secteur de la sécurité est composé de toutes les structures, institutions et personnes chargées de la prestation, de la gestion et du contrôle de la sécurité au niveau national et local[3] .

Par conséquent, le secteur de sécurité ne se limite pas aux seules prestations de services de sécurité et de justice assurées par l'État. Il arrive souvent que les individus assurent eux-mêmes la sécurité et la justice dans leurs foyers et au sein de leurs communautés, indépendamment du fait que l'État réponde, ou non, à ces besoins. Certaines communautés s'organisent pour assurer leur propre sécurité, et ce de diverses manières, par exemple par le biais d'une surveillance dans les quartiers ; d'initiatives de groupes de femmes ou de dispositifs visant à assurer la sécurité des commerces.

En outre, la prestation de services de sécurité et de justice peut être définie et assurée par d'autres acteurs et dispositifs au sein des communautés ; c'est le cas, par exemple, de certains individus qui sont investis d'une autorité coutumière leur permettant de prendre des décisions en matière de sécurité et de justice ; de mécanismes alternatifs de résolution des différends et de processus de décisions fondés sur les traditions et des règles informelles locales. Par conséquent, ces groupes communautaires relèvent également du secteur de la sécurité et de la justice au sens large.

Le secteur de la sécurité est composé de toutes les structures, institutions et personnes chargées de la prestation, de la gestion et du contrôle de la sécurité au niveau national et local. Cela regroupe notamment

- les prestataires des services de sécurité tels que les forces armées, la police, les gardes-frontières, les services de renseignement, les établissements pénitentiaires, les acteurs commerciaux et non étatiques de la sécurité, etc. ;
- les organes de gestion et de contrôle de la sécurité tels que les ministères, le Parlement, les institutions de contrôle dotées d'un mandat spécifique en la matière, certaines composantes du secteur de la justice, et les acteurs de la société civile qui, non seulement jouent un rôle important pour s'assurer que les services publics de sécurité répondent à des normes élevées, mais en sont aussi les bénéficiaires ultimes, comme les organisations de femmes, les médias, etc.

Il est important de noter que la réforme du secteur de la sécurité (RSS) repose sur une acception large du concept de secteur de la sécurité. La RSS est un processus dont l'objectif ultime est de favoriser la bonne gouvernance du secteur de la sécurité afin de promouvoir la sécurité humaine et celle de l'État.

Source : DCAF, Document d'information sur la RSS, Secteur de la sécurité (cf. Bibliographie)

3 Ibid.

Dans son acception la plus large, la notion de secteur de la sécurité inclut les prestataires de services de sécurité et de justice non étatiques, car ceux-ci ont un impact direct sur la gouvernance du secteur de la sécurité. Depuis vingt ans, les prestataires de services de sécurité privée jouent un rôle de plus en plus important dans la prestation de services de sécurité et de protection des personnes et des biens. C'est le cas, en particulier, des entreprises militaires et de sécurité privées qui opèrent sur une base commerciale et qui constituent dorénavant un acteur majeur du secteur de la sécurité.

Que recouvre la notion de réforme du secteur de la sécurité ?

Un secteur de la sécurité inefficace et ne faisant pas preuve de responsabilité n'est pas en mesure d'assurer la sécurité de tous, car il ne peut pas s'acquitter de manière crédible de ses fonctions, qu'il s'agisse de la défense nationale, de l'application de la loi ou d'assistance à la population. L'inefficacité du secteur de la sécurité entraîne un risque de gaspillage des ressources publiques, en drainant le financement d'autres services publics essentiels[4] .

La réforme du secteur de la sécurité (RSS) est un processus politique et technique qui vise à améliorer la sécurité humaine et celle de l'État en renforçant l'efficacité et la responsabilité en matière de prestation, de gestion et de contrôle de la sécurité dans le cadre d'un contrôle civil et démocratique, et dans le respect de l'État de droit et des droits humains[5] .

> **Bonnes pratiques :** Il est important de reconnaître que les individus et les communautés ont des besoins de sécurité différents, y compris dans le cyberespace.

Chaque individu qui utilise le cyberespace a des besoins de sécurité spécifiques. Dans le cyberespace, le fanatisme, la haine et les discours misogynes ciblent de manière disproportionnée les femmes et les jeunes filles. La prise en compte de cette réalité - et la mise en place de mécanismes efficaces pour signaler les incidents et mener des enquêtes pénales - peuvent contribuer à renforcer la sécurité des groupes vulnérables affectés.

4 Ibid.

5 DCAF, Document d'information sur la réforme du secteur de la sécurité, p. 2. Disponible sur : https://www.dcaf.ch/sites/default/files/publications/documents/DCAF_BG_1_La_gouvernance_du_secteur_de_la_securite.pdf

EXEMPLES DE BONNES PRATIQUES

Le Bénin a lancé une campagne annuelle sur la cybersécurité dans le cadre des initiatives menées par les autorités du pays pour sensibiliser la population à cette problématique. La campagne cible les jeunes et va être codifiée dans le document de stratégie nationale de cybersécurité.

Dans le cadre de la campagne « Mouvement contre les discours de haine », les États membres du Conseil de l'Europe ont lancé des campagnes au niveau national et ont créé des organes chargés d'adopter des procédures et de mettre en place des mécanismes nationaux de signalement des discours de haine, des crimes motivés par la haine et de cyberharcèlement.

En Autriche, le ministère de l'Intérieur pilote un mécanisme de signalement des vidéos extrémistes violentes et radicales afin d'éliminer ces discours des plateformes de réseaux sociaux.

(Source : Ministère fédéral de l'Intérieur de l'Autriche, http://bvt.bmi.gv.at/601/)

La police ukrainienne a désigné un point de contact auprès duquel les individus affectés peuvent signaler les cas de cyberharcèlement et de discours de haine et porter plainte suite à ces actes.

(Source : Conseil de l'Europe, https://www.coe.int/fr/web/no-hate-campaign/reporting-to-national-bodies#{%2237117314%22:[8]})

Au Sénégal, l'École nationale de cybersécurité à vocation régionale (ENVR) a été créée, en novembre 2018, avec le soutien de la France afin de renforcer les politiques de défense des États de l'Afrique de l'Ouest contre le piratage informatique et l'utilisation de l'Internet à des fins de financement et de propagande du terrorisme. L'école dispensera une formation aux services de sécurité, aux membres du système judiciaire et aux entreprises privées sur les modalités de lutte contre la cybercriminalité. Elle aura également un « rôle de formation professionnelle à l'échelle régionale » afin d'aider d'autres pays d'Afrique de l'Ouest.

(Source : https://www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/securite-desarmement-et-non-proliferation/le-cadre-institutionnel-de-l-action-de-la-france/la-cooperation-de-securite-et-de-defense/les-ecoles-nationales-a-vocation-regionale/article/senegal-inauguration-de-l-ecole-nationale-de-cybersecurite-a-vocation-regionale)

2. Application au cyberespace des principes de bonne gouvernance du secteur de la sécurité

Qu'est-ce qu'une bonne gouvernance du secteur de la sécurité ?

Une bonne GSS repose sur l'application des principes de bonne gouvernance à la prestation, à la gestion et au contrôle de la sécurité au niveau national. La bonne gouvernance repose sur les sept principes suivants :

- **Responsabilité** : il existe des attentes spécifiques en ce qui concerne la prestation des services de sécurité, et ce sont des autorités indépendantes qui déterminent si ces attentes sont satisfaites, et imposent, dans le cas contraire, des sanctions.
- **Transparence :** les informations doivent être disponibles librement et accessibles aux personnes affectées par des décisions et par leur mise en œuvre.
- **État de droit :** toutes les personnes et institutions, y compris l'État, doivent être soumises à des lois connues publiquement, appliquées de manière impartiale, et conformes aux normes internationales et nationales relatives aux droits humains.
- **Participation :** Les hommes et les femmes de tous horizons doivent avoir l'opportunité de participer à la prise de décision et à la prestation de services de manière libre, équitable et inclusive, soit directement, soit par le biais d'institutions représentatives et légitimes.
- **Réactivité :** les institutions doivent être attentives aux besoins spécifiques des différents groupes de la population en matière de sécurité, et doivent accomplir leurs missions dans un esprit de culture axée sur le service.
- **Efficacité :** les institutions sont tenues d'assumer leurs rôles, responsabilités et missions respectifs avec le plus grand professionnalisme.
- **Efficience :** les institutions doivent faire le meilleur usage possible des ressources publiques pour accomplir leurs rôles, responsabilités et missions respectifs.

Appliquer au cyberespace les principes de bonne gouvernance

Si le cyberespace était un État, il serait le pays le plus vaste et le plus peuplé du monde. Cependant, cet espace ne disposerait pas d'un organe décisionnel représentatif, parlementaire ou basé sur une autre forme de représentativité, ni de mécanismes chargés de l'application de la loi ou de la protection des droits humains de ses citoyens, car aucune entité n'exerce une autorité et un contrôle exclusifs sur l'ensemble de l'espace numérique[6] .

La gouvernance du cyberespace se caractérise, au contraire, par la présence d'une multitude d'acteurs divers, dont les différents rôles et responsabilités influent sur les décisions politiques et les modalités de prise de décision en matière de réglementation.

Les acteurs non étatiques présents dans le cyberespace incluent la société civile, y compris les organisations non gouvernementales ; les groupes de recherche universitaires et les médias ; le secteur privé, en particulier les entreprises privées et les organisations sectorielles ; ainsi que les organisations internationales et régionales.

Du fait de la multiplicité des acteurs impliqués, les processus d'élaboration et d'application de politiques et de cadres réglementaires au cyberespace sont souvent lourds, complexes et / ou inefficaces.

Combiné à un déficit de connaissances sur les manières d'appliquer efficacement les principes de bonne gouvernance au cyberespace, ce facteur peut conduire à une situation de mauvaise gouvernance, où le secteur de la sécurité est globalement dans l'incapacité d'assurer de manière efficace la sécurité humaine et celle de l'État. Les sections suivantes examinent de manière plus détaillée trois principes de bonne gouvernance : la responsabilité, la transparence et l'État de droit.

6 Anja Mihr (2014): Good Cyber Governance, Human Rights and Multi-stakeholder Approach, Georgetown Journal of International Affairs. Disponible sur : https://www.jstor.org/stable/43773646

ÉTUDE DE CAS: LE PROGRAMME DE SURVEILLANCE DE L'AGENCE NATIONALE DE SÉCURITÉ (NSA) DES ÉTATS-UNIS D'AMÉRIQUE

En 2013, Edward Snowden, employé de la CIA, a divulgué des documents top secrets révélant que les agences de renseignement américaines et britanniques mettaient en œuvre des programmes de surveillance de masse dans le monde entier. Ces activités consistaient notamment à : intercepter des conversations sur Internet et par téléphone transitant par des câbles à fibres optiques sous-marins ; collecter des données à partir des comptes d'utilisateurs Google et Yahoo et d'enregistrements de téléphone portable ; espionner des États étrangers ; procéder à du piratage informatique et ; contaminer des ordinateurs à l'aide de logiciels malveillants.

Par exemple, l'US Foreign Intelligence Surveillance Court (FISA, Cour de Surveillance du Renseignement Étranger des États-Unis) a ordonné à plusieurs entreprises de livrer les données de leurs clients. De plus, des pratiques d'échange de renseignements de grande ampleur entre les membres de la « Five-Eyes Alliance » et d'autres États ont été révélées. Bien que le président Obama ait réagi à cette divulgation d'informations en réformant les programmes de surveillance de la NSA ainsi que le fonctionnement de la Cour FISA afin de renforcer la transparence de leurs activités, le Congrès américain n'est toujours pas parvenu à s'accorder sur la mise en place d'un système permettant de garantir la protection effective de la vie privée tout en préservant les capacités d'enquête des agences de sécurité.

(Source : ACLU, disponible sur : https://www.aclu.org/issues/national-security/privacy-and-surveillance/nsa-surveillance?redirect=nsa-surveillance et https://www.aclu.org/blog/national-security/nsa-legislation-leaks-began?redirect=NSAreform)

2.1. Élaborer des normes et mettre en place des institutions qui favorisent et renforcent l'application au cyberespace du principe de responsabilité du secteur de la sécurité.

Une responsabilisation efficace repose sur un contrôle démocratique et civil. Celui-ci peut être exercé par les parlements nationaux et plus généralement par la société civile. Cette forme de contrôle joue un rôle clé pour assurer la responsabilité du secteur de la sécurité. Or, dans le cyberespace, le contrôle civil et démocratique du secteur de la sécurité est souvent affaibli pour diverses raisons.

Le contrôle démocratique est souvent confronté aux obstacles suivants[7] :

- **La complexité des réseaux en ligne**

La complexité des réseaux en ligne constitue un premier obstacle au contrôle

7 See Buckland, B., F. Schreier, and Th. H. Winkler, op. cit., pp. 18-19. Disponible sur: https://www.dcaf.ch/sites/default/files/publications/documents/OnCyberwarfare-Schreier.pdf

démocratique. Un très grand nombre d'États, d'acteurs privés internationaux et autres d'acteurs non étatiques participent à des initiatives de cybersécurité. De même, différents acteurs sont impliqués dans des actions qualifiées globalement de « cyberattaques ». Or, du fait de la complexité technique des réseaux en ligne, il est très difficile pour les organes de contrôle - tels que les comités parlementaires aux capacités souvent limitées - d'identifier les acteurs concernés ; d'avoir des informations sur leur existence et leurs activités ; ou même d'obtenir le mandat légal de le faire.

- **La nécessité d'acquérir des connaissances techniques pour élaborer et mettre en œuvre une réglementation efficace**

Deuxièmement, la difficulté d'assurer un contrôle de ces activités est exacerbée par la nature hautement technique du cyberespace. De ce fait, les organes de contrôle tels que les parlements manquent souvent des compétences requises pour être en mesure de comprendre les activités dans le cyberespace et d'adopter une législation capable de les réglementer efficacement. La coopération entre organes publics et privés est, de plus, entravée par le fossé qui sépare, d'une part, les experts techniques hautement rémunérés et qualifiés impliqués dans l'élaboration et la mise en œuvre d'une réglementation efficace et, d'autre part, les acteurs gouvernementaux chargés de contrôler le respect de ces normes et qui ont des salaires et un niveau d'expertise bien moindres.

- **Les complexités juridiques inhérentes au cyberespace en matière notamment de juridiction et d'attribution de compétences**

Troisièmement, les problèmes de contrôle sont aggravés par la complexité juridique en la matière. La nature interconnectée et « sans frontières » du cyberespace soulève de véritables défis pour les cadres d'application de la loi traditionnellement définis sur une base territoriale. Les données et les cyber-activités peuvent basculer de serveurs situés dans un État vers ceux situés dans un autre pays littéralement à la vitesse de la lumière. En outre, même si l'on affirme souvent que les mêmes règles devraient s'appliquer pour les activités hors ligne et en ligne, on ne sait souvent pas clairement ce que cela signifie dans la pratique. La cybersécurité pose des questions juridiques complexes liées, entre autres, au droit à la vie privée et à la liberté d'expression. Cette complexité est encore exacerbée par la coopération entre acteurs publics et privés dans le cyberespace, qui soulève quant à elle des problèmes juridiques en matière de responsabilité et de contrôle.

- **La diversité des acteurs impliqués brouille la délimitation traditionnelle entre responsabilité et contrôle**

Quatrièmement, les difficultés d'assurer un contrôle démocratique sont amplifiées par la nature différente des acteurs impliqués. Dans la plupart des cas, les institutions chargées de ce contrôle au niveau national sont organisées en agences ou selon des secteurs fonctionnels. Par exemple, un comité parlementaire peut être habilité à contrôler les services de renseignement, les forces armées ou les institutions judiciaires. Or, la coopération entre acteurs publics et privés en matière de cybersécurité transcende les frontières entre agences et, par conséquent, également entre secteurs d'expertise et mandats de contrôle. De ce fait, un grand nombre de domaines sont soumis à un contrôle insuffisant, ou y échappent totalement.

Le cyberespace entraîne également un brouillage des chaînes de responsabilité et de contrôle. En effet, les actions de tout agent gouvernemental sont normalement reliées à leurs supérieurs hiérarchiques dans le cadre de chaînes de responsabilité. Par exemple, un policier parisien est lié par l'intermédiaire de ses supérieurs hierarchiques au préfet de police (le chef de la police nommé par le pouvoir exécutif) et, au plus haut niveau de cette chaîne de responsabilité, au ministère de l'Intérieur et au pouvoir exécutif. Il existe donc un lien de responsabilité et de contrôle entre les institutions de gouvernance démocratique (telles que le parlement) et les individus ou agences appliquant les directives du pouvoir exécutif. Ces liens peuvent être rompus par l'entrée en jeu d'acteurs privés et la mise en place de mécanismes de coopération entre acteurs publics et privés. Si une entreprise informatique engagée comme sous-traitante pour le compte d'une agence publique peut sembler agir comme un simple agent de l'État, sa relation avec ce dernier est généralement beaucoup plus complexe et est brouillée par de nombreuses asymétries d'informations qui entravent la transparence et empêchent le fonctionnement efficace des mécanismes de contrôle.

- **Nécessité de comprendre le mandat de l'organe de contrôle**

En général, les organes de contrôle étatiques ont pour mandat de surveiller les agences gouvernementales dont ils ont la responsabilité directe. Les partenaires privés de ces agences peuvent ainsi échapper à leur contrôle, même dans les cas où ils sont directement financés par ces agences, ou travaillent en étroite collaboration avec elles.

ÉTUDE DE CAS : LE BUNDESTAG ALLEMAND ENQUÊTE SUR LA VENTE DE TECHNOLOGIES DE SURVEILLANCE À DES GOUVERNEMENTS ÉTRANGERS

En 2014, des membres du parlement allemand ont mené une enquête sur la vente de technologies de surveillance à des États étrangers. Répondant à cette enquête, le gouvernement allemand a déclaré qu'au cours de la décennie précédente, il avait octroyé à des entreprises allemandes des licences leur permettant d'exporter des technologies de surveillance dans au moins 25 pays, dont beaucoup commettaient depuis longtemps des atteintes aux droits humains.

À la suite de cette enquête, le gouvernement allemand a déclaré qu'il s'emploiera dorénavant à renforcer la réglementation des technologies de surveillance qui portent atteinte aux droits humains.

(Source : EDRi Protecting Digital Freedom. Disponible sur : hhttps://edri.org/germany-exports-surveillance-technologies-to-human-rights-violators/)

La complexité technique du cyberespace amplifie les difficultés auxquelles sont traditionnellement confrontés les parlementaires pour contrôler le secteur de la sécurité. Cela peut nuire aux efforts visant à garantir la responsabilité effective des acteurs de ce secteur. Cet élément - auquel s'ajoute la difficulté d'attribuer de manière fiable à un acteur spécifique la responsabilité d'une infraction à la loi commise dans le cyberespace - peut rendre difficile, voire impossible, la tâche des autorités civiles chargées d'assurer la responsabilité du secteur de la sécurité ; cette situation ne peut qu'alimenter une culture de l'impunité.

Le pouvoir judiciaire joue un rôle central dans le contrôle des actions du secteur de la sécurité. Par exemple, il peut accorder des pouvoirs spéciaux aux organes chargés de l'application de la loi et aux services de renseignement en délivrant des mandats de perquisition. Cette prérogative peut jouer un rôle particulièrement important pour les opérations d'interception de communications. Cependant, le contrôle judiciaire est souvent contourné ou limité pour des raisons de sécurité nationale et d'état d'urgence.

ÉTUDE DE CAS : CONTRÔLE PARLEMENTAIRE DE LA CYBERSÉCURITÉ EN SUÈDE : PRINCIPAUX DÉFIS ET BONNES PRATIQUES

Le parlement suédois compte quinze commissions qui assument divers rôles. Ces commissions peuvent, par exemple, organiser des audiences publiques afin de mieux comprendre certaines questions spécifiques sur lesquelles le parlement doit légiférer. Il ne semble pas y avoir une commission parlementaire spécifiquement chargée de contrôler la gouvernance en matière de cybersécurité et il est probable que diverses commissions jouent un rôle dans ce domaine en fonction des questions traitées. Par exemple, la commission de la défense peut être chargée de questions liées à la cybersécurité.

La stratégie nationale suédoise en matière de cybersécurité, adoptée en 2016, aborde un large éventail de sujets, notamment la réglementation des fournisseurs de TIC et la protection des infrastructures essentielles. Cependant, il ne semble pas qu'une commission ou sous-commission soit spécifiquement chargée de la cybersécurité. La complexité de cette question nécessite très souvent l'implication de divers ministères et il semble que ce soit également le cas en Suède. Le contrôle de ce secteur est d'autant plus difficile qu'une partie importante de la cyberprotection est assurée par des acteurs privés et que les commissions parlementaires ne disposent pas d'un mandat adéquat pour contrôler ce type d'activités. Néanmoins, contrairement aux stratégies en matière de cybersécurité adoptées par d'autres États, l'approche suédoise définit des principes stratégiques et un plan d'action susceptibles d'aider le Parlement à demander des comptes aux acteurs impliqués dans ce secteur.

La société civile joue un rôle crucial dans le contrôle du secteur de la sécurité, qui vient compléter les fonctions de contrôle confiées aux pouvoirs législatif et judiciaire. La société civile peut proposer des orientations en matière de politiques et peut offrir une expertise technique. Dans le cadre de son rôle plus général de défense des intérêts de la population, la société civile peut également faciliter le dialogue et la négociation en la matière.

La société civile contribue, en outre, à sensibiliser à diverses questions et peut orienter les politiques. Les médias, en particulier, peuvent mener des enquêtes approfondies sur certaines questions sensibles et renforcer l'accès public à l'information.

ÉTUDE DE CAS : RÔLE DES ENTREPRISES PRIVÉES DANS LA VENTE DE TECHNOLOGIES DE SURVEILLANCE À DES AUTORITÉS ÉTATIQUES

Des entreprises privées, telles que l'entreprise italienne « Hacking Team », ont vendu des systèmes d'intrusion à distance à divers États, notamment l'Égypte, le Nigéria, l'Ouzbékistan, la Turquie, le Maroc et la Colombie. Cette tendance croissante a suscité des débats sur l'utilisation potentielle de ces technologies à des fins de répression et pour commettre des violations des droits humains.

La surveillance de masse constitue un défi émergent et les entreprises privées continuent de vendre des outils et des technologies de surveillance à divers États. Des organisations de la société civile ont mené des actions pour sensibiliser l'opinion publique aux risques soulevés par cette pratique commerciale notamment en publiant une base de données publique qui a révélé que 520 entreprises de surveillance vendent ce type de matériels à des États dans le monde entier. Malgré cela, cette question reste très peu réglementée.

2.2. Élaborer des normes et créer des institutions qui encouragent et renforcent la transparence et assurent le libre accès à l'information

De manière générale, la transparence poursuit un double objectif : favoriser le partage d'informations de façon à assurer l'efficacité des institutions du secteur de la sécurité et contribuer de manière essentielle à leur responsabilisation. En outre, les technologies de l'information et de la communication (TIC) constituent, en elles-mêmes, un outil de promotion et de renforcement de la transparence qui facilite l'accès public aux informations.

La bonne gouvernance du secteur de la sécurité est un processus et elle constitue l'objectif de la réforme du secteur de la sécurité.

S'il est impossible d'atteindre une transparence absolue du secteur de la sécurité, cet objectif n'est pas nécessairement souhaitable dans certains contextes spécifiques.

Il est important de prendre en compte ce « dilemme de la transparence » lorsque l'on cherche à promouvoir une culture de la confiance et de l'ouverture parmi les prestataires de sécurité publics et privés. La transparence, cependant, doit être la règle et toute limitation en la matière doit constituer une exception clairement définie dans la législation nationale[8] .

La transparence permet également d'améliorer la compréhension des cyber-risques en matière de sécurité et aide les autorités étatiques, les entreprises privées et la société civile à se coordonner et à collaborer plus efficacement pour prévenir ces risques et y répondre.

La compréhension de ces cyber-risques peut aider les individus qui utilisent ces technologies à prendre des décisions informées. Cela est essentiel, car les individus sont souvent considérés comme le maillon faible de la chaîne de (cyber) sécurité.

8 Iulian F. Popa, Extensive Transparency as a Principle of Cyberspace Governance and Cyber Security Dilemma Prevention. Disponible sur : https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2603326

L'amélioration des canaux d'information peut favoriser un meilleur comportement en ligne (également appelé « bonne hygiène cybernétique »), ce qui peut permettre de réduire l'impact de la plupart des activités malveillantes.

À cet égard, les approches multi-acteurs peuvent également contribuer à renforcer la transparence tout en améliorant la sensibilisation aux cyber-risques.

EXEMPLES DE BONNES PRATIQUES

En 2014, l'Organisation pour la sécurité et la coopération en Europe (OSCE) a adopté un accord sur les mesures de confiance. Ces mesures volontaires prévoient que les États feront part de leurs points de vue nationaux sur la cybersécurité et partageront des informations sur leur stratégie et sur les menaces auxquelles ils sont confrontés dans ce domaine. Les membres de l'OSCE ont, en outre, convenu d'échanger des informations sur leur organisation, leurs stratégies ou leurs programmes nationaux en matière de cybersécurité et d'identifier un point de contact pour faciliter la communication et le dialogue sur les questions de sécurité relatives aux TIC.

Le Salvador a promulgué des lois relatives à la protection des données et à l'accès à l'information publique, qui établissent des normes en matière de transparence et de liberté de l'information

(Source: https://publications.iadb.org/handle/11319/7449 , p 74)

L'Organisation des États américains a publié un rapport sur les équipes d'intervention en cas d'incident de sécurité informatique (CSIRT) qui identifie différents moyens de renforcer la coopération entre les CSIRT afin de favoriser le partage d'informations.

(Source : https://www.sites.oas.org/cyber/Documents/2016%20-%20Best%20Practices%20CSIRT.pdf)

La promotion de partenariats entre acteurs publics et privés peut contribuer à créer un environnement favorisant le partage d'informations et l'accès à l'information.

2.3. Renforcer l'application du principe de l'État de droit au cyberespace.

Le cyberespace constitue également un nouvel espace propice pour les comportements illicites, tels que la diffusion de discours de haine, de pornographie enfantine, d'incitations à la violence, d'atteintes au droit d'auteur, de fraudes, de vols d'identité, de blanchiment d'argent ou d'attaques par « déni de service[9] ». Ces actes criminels ont de plus en plus un caractère transnational.

9 Conseil de l'Europe, The rule of law on the Internet and in the wider digital world, Issue paper published by the Council of Europe Commissioner for Human Rights, Executive summary and Commissioner's recommendations, 2014. Disponible en anglais sur : http://www.statewatch.org/news/2014/dec/coe-hr-comm-rule-of-law-on-the%20internet-summary.pdf

« L'environnement numérique peut, de par sa nature même, porter atteinte au droit à la vie privée et à d'autres droits fondamentaux et saper la prise de décisions responsables.[10] » De ce fait, l'érosion des droits à la vie privée et d'autres libertés fondamentales, tels que la liberté d'expression, risque de contribuer à affaiblir le principe de l'État de droit.

Le principe de l'État de droit a fait l'objet d'interprétations de la part de tribunaux internationaux, tels que la Cour européenne des droits de l'homme (CEDH). Celle-ci a mis au point un critère pour évaluer le respect de l'État de droit aux termes duquel « toutes les restrictions des droits fondamentaux doivent être fondées sur des règles juridiques claires, précises, accessibles et prévisibles, et doivent servir des objectifs clairement légitimes ; elles doivent être "nécessaires" et "proportionnées" au but légitime fixé [...] et elles doivent pouvoir faire l'objet d'un recours effectif [de préférence judiciaire] ».

Les autorités étatiques ont appelé les entreprises privées propriétaires de plateformes de médias sociaux à veiller à ce que leurs services ne soient pas détournés à des fins de propagation de messages prônant l'extrémisme violent et le terrorisme.

Le Secrétaire général des Nations Unies a expliqué le concept d'État de droit de la manière suivante :

Pour les Nations Unies, le concept d'État de droit désigne « un principe de gouvernance en vertu duquel l'ensemble des individus, des institutions et des entités publiques et privées, y compris l'État lui-même, ont à répondre de l'observation de lois promulguées publiquement, appliquées de façon identique pour tous et administrées de manière indépendante, et compatibles avec les règles et normes internationales en matière de droits de l'homme. Il implique, d'autre part, des mesures propres à assurer le respect des principes de la primauté du droit, de l'égalité devant la loi, de la responsabilité au regard de la loi, de l'équité dans l'application de la loi, de la séparation des pouvoirs, de la participation à la prise de décisions, de la sécurité juridique, du refus de l'arbitraire et de la transparence des procédures et des processus législatifs ».

(Source : Rapport du Secrétaire général des Nations Unies, « Rétablissement de l'État de droit et administration de la justice pendant la période de transition dans les sociétés en proie à un conflit ou sortant d'un conflit », S/2004/616 (23 août 2004), para 6, disponible sur : https://undocs.org/fr/S/2004/616.

Afin de répondre aux demandes des autorités étatiques, certaines entreprises privées - en particulier des entreprises de médias sociaux telles que Facebook, Google et Twitter - ont élaboré des conditions de service et des codes de conduite afin de réglementer le contenu hébergé sur leurs plateformes de médias sociaux. Ainsi, elles ont créé de facto des normes relatives à l'utilisation de l'Internet. Cependant, ces conditions de service et ces codes de conduite diffèrent en fonction des entreprises de médias sociaux, ce qui crée une ambiguïté et une incertitude juridique quant aux contenus prohibés par ces différentes plates-formes.

10 Ibid. p. 8.

ÉTUDE DE CAS : RÔLE DES ENTREPRISES DE MÉDIAS SOCIAUX DANS LA RÉGULATION DE LEURS PLATES-FORMES

Le droit des entreprises de médias sociaux de contrôler librement leurs plateformes et de fixer des « standards de la communauté » est incontestable. Cependant, lorsqu'il s'agit de terrorisme, ces entreprises agissent de facto comme des régulateurs qui peuvent décider de restreindre la liberté d'expression sur leurs plateformes, sans pour autant être tenues de respecter les obligations prévues en la matière par le droit international relatif aux droits humains. En outre, les entreprises de médias sociaux subissent de plus en plus de pressions de la part des États pour que leurs plates-formes ne tolèrent aucun discours violent incitant, glorifiant ou faisant l'apologie du terrorisme.

De ce fait, ces entreprises de médias sociaux ont actualisé leurs « standards de la communauté » pour répondre à ces demandes pressantes des États, ce qui a souvent entraîné une réglementation ambivalente.

Facebook, par exemple, exclut de sa plateforme toute organisation ou tout individu impliqué dans des activités terroristes. Les activités terroristes reposent sur la définition d'une organisation terroriste considérée comme « toute organisation non gouvernementale impliquée dans des actes de violence prémédités contre des individus ou une propriété en vue d'intimider une population civile, un gouvernement ou un organisme international et avec pour objectif d'atteindre un but politique, religieux ou idéologique ». Facebook définit un acte terroriste comme « tout acte de violence prémédité contre des individus ou une propriété, perpétré par une personne n'appartenant pas à un gouvernement en vue d'intimider une population civile, un gouvernement ou un organisme international, avec pour objectif d'atteindre un but politique, religieux ou idéologique ».

(Source : https://www.facebook.com/communitystandards/dangerous_individuals_organizations)

Twitter au contraire ne fait pas référence au terrorisme dans ses règles de fonctionnement. Twitter interdit les contenus haineux qui incitent à la violence ou qui attaquent ou menacent directement d'autres personnes en raison de leur race, leur ethnie, leur origine nationale, leur orientation sexuelle, leur sexe, leur identité sexuelle, leur appartenance religieuse, leur âge, leur handicap ou une maladie grave. De plus, Twitter interdit l'apologie de la violence sur ses plateformes ainsi que les menaces violentes. Les exemples d'apologie de la violence incluent les meurtres de masse, les attaques terroristes, les viols et les agressions sexuelles.

(Source: https://help.twitter.com/en/rules-and-policies/violent-threats-glorification)

Les révélations de Snowden ont clairement montré que les agences de renseignement écoutent et exploitent régulièrement des communications privées et les interceptent en empruntant des portes dérobées (backdoors). En d'autres termes, cela montre qu'il n'y a pas, à l'heure actuelle, de pierre angulaire permettant d'assurer le respect de

l'État de droit en matière de sécurité nationale, alors même qu'il existe des principes fondamentaux qui pourraient être à même de constituer une base pour favoriser le respect de cet élément central du cadre universel de protection des droits humains. Du fait de la multiplication des partenariats entre les services chargés de l'application de la loi et les services de renseignement et de sécurité, les actions menées par la police et le Parquet risquent d'être également affectées par cet affaiblissement de l'État de droit. L'absence de cadres juridiques clairs aux niveaux national et international constitue une menace supplémentaire pour le respect de l'État de droit sur Internet et dans l'environnement numérique au niveau mondial.

Certaines évolutions en matière de droit international remettent également en cause le principe de l'État de droit en privilégiant notamment, pour régir le comportement des acteurs du secteur de la sécurité dans le cyberespace, l'adoption de règles et de cadres réglementaires volontaires, non contraignants et à caractère ponctuel. (Pour un aperçu du cadre juridique international et régional existant, voir le chapitre 3).

ÉTUDE DE CAS : PRIVATISATION DE LA RÉGLEMENTATION DU CYBERESPACE

Internet et l'environnement numérique mondial sont en grande partie contrôlés par des entités privées (en particulier, mais pas uniquement par des entreprises états-uniennes) et cela constitue également une menace pour l'État de droit. Ces entités privées peuvent imposer - et être « encouragées » à imposer - des restrictions à l'accès à l'information sans être tenues de respecter les contraintes constitutionnelles ou internationales auxquelles les États doivent se soumettre lorsqu'ils souhaitent limiter le droit à la liberté d'expression. Ces entités privées peuvent également se voir ordonner par les systèmes judiciaires nationaux, agissant à la demande d'autres entités privées, d'effectuer des analyses très intrusives de leurs données afin de détecter des atteintes probables (ou tout simplement possibles) à des droits de propriété privée, qui concernent souvent des droits de propriété intellectuelle.

Ces entreprises privées peuvent recevoir l'ordre d'« extraire » des données, y compris des données étatiques, commerciales et personnelles, de serveurs situés dans d'autres pays, à des fins de maintien de l'ordre ou de sécurité nationale. Ces entreprises privées peuvent effectuer ces actes sans avoir obtenu le consentement des autorités de l'autre État - ou des entreprises ou des personnes concernées situées dans l'autre pays - et ce, en violation de la souveraineté de cet État tiers, de la confidentialité commerciale à laquelle les entreprises ont droit et des droits humains des personnes concernées.

La responsabilité des entreprises de médias sociaux (« responsabilité des intermédiaires ») doit être interprétée de manière très restrictive. En d'autres termes, il convient de procéder à une évaluation rigoureuse afin de déterminer si - et dans quelles circonstances - la responsabilité d'entreprises comme Google, Facebook et YouTube peut être engagée pour des contenus publiés sur leurs plateformes, car cela peut avoir

un effet direct sur la liberté d'expression et d'autres droits humains. Or, les autorités étatiques du monde entier exercent des pressions sans cesse croissantes sur ces entreprises afin qu'elles imposent un contrôle plus strict de ces contenus en ligne, ce qui favorise un climat d'« autocensure ».

EXEMPLES DE BONNES PRATIQUES

Les Principes de Manille sur la responsabilité des intermédiaires précisent que : « Les intermédiaires ne doivent pas être contraints de restreindre des contenus, sauf sur ordonnance d'une autorité juridictionnelle indépendante et impartiale, qui aurait déterminé le caractère illégal du contenu en question». Les Principes de Manille prévoient également que toute décision prise par un intermédiaire de restreindre un contenu doit être fondée sur des « preuves suffisantes pour étayer le fondement juridique qui a justifié la délivrance de la demande ». Les Principes de Manille soulignent, en outre, l'importance d'intégrer les principes de transparence et de responsabilité dans la législation, en notant que les autorités étatiques ne doivent pas recourir à des mesures extrajudiciaires pour restreindre des contenus. Ces mesures extrajudiciaires peuvent inclure les pressions collatérales visant à imposer des changements dans les conditions générales d'utilisation du service ; à promouvoir ou appliquer des pratiques soi-disant « volontaires » et à fixer des accords entravant le commerce ou la diffusion publique de contenus.

(Source : https://www.eff.org/files/2015/10/31/manila_principles_1.0_fr.pdf)

En Argentine, le projet de loi sur la responsabilité des intermédiaires précise que « la responsabilité des fournisseurs de services internet ne peut pas être engagée à l'égard de contenue créée par des tiers, sauf lorsqu'ils ont été dûment notifiés d'une décision de justice demandant de supprimer ou de bloquer un contenu ».

(Source : Comisión de Sistemas de Communicación y Libertad de Expresión, https://www.infobae.com/tecno/2017/11/21/como-es-el-proyecto-de-ley-que-regula-la-responsabilidad-de-los-intermediarios-de-internet/)

Conclusions Clés

- Il est utile de concevoir la sécurité en termes de gouvernance car cela permet de mettre en évidence la manière dont divers acteurs, aussi bien étatiques que non étatiques, exercent du pouvoir et de l'autorité en matière de sécurité, à la fois de manière formelle et informelle, aux niveaux international, national et local.
- La gouvernance est un terme générique qui peut être appliqué à la sécurité en général pour rendre compte du rôle joué par l'ensemble des acteurs internationaux, nationaux et locaux dans la formulation et la mise en œuvre des décisions en matière de sécurité.
- Les principes d'une bonne GSS sont les suivants : responsabilité, transparence, État de droit, participation, réactivité, efficacité et efficience.
- Une bonne GSS repose sur l'idée selon laquelle le secteur de la sécurité doit respecter les mêmes normes élevées que celles imposées aux autres prestataires de services du secteur public.
- Une bonne GSS repose sur un ensemble de principes. Par conséquent, les mêmes principes fondamentaux de bonne gouvernance s'appliquent différemment dans chaque secteur de la sécurité.
- Le maintien d'une bonne GSS requiert une capacité d'adaptation continue afin de pouvoir répondre à l'évolution constante des menaces à la sécurité.
- La RSS améliore la capacité du secteur de la sécurité à assurer la sécurité de l'État et de ses citoyens.
- La RSS optimise l'efficacité de l'utilisation des ressources publiques dans le secteur de la sécurité.
- La RSS réduit les risques de corruption en renforçant le contrôle et le professionnalisme
- La RSS protège l'indépendance professionnelle du personnel de sécurité, ce qui permet à celui-ci de s'acquitter efficacement de ses tâches légitimes ; elle renforce également les normes professionnelles et la responsabilité, ce qui réduit le risque d'abus commis envers la population.
- La RSS favorise la prestation de services de sécurité inclusifs ainsi que l'égalité des chances dans le secteur de la sécurité.
- La RSS prévient les conflits en promouvant les principes d'unité, de neutralité politique, d'égalité et de professionnalisme dans le secteur de la sécurité.

Bibliographie

DCAF, RSS Document d'information, La gouvernance du secteur de la sécurité. Appliquer les principes de bonne gouvernance au secteur de la sécurité. Disponible sur : https://www.dcaf.ch/sites/default/files/publications/documents/DCAF_BG_1_La_gouvernance_du_secteur_de_la_securite.pdf

DCAF, RSS Document d'information, La réforme du secteur de la sécurité.

Appliquer les principes de bonne gouvernance au secteur de la sécurité. Disponible sur : https://dcaf.ch/sites/default/files/publications/documents/DCAF_BG_2_La%20reforme%20du%20secteur%20de%20la%20securite_1.pdf

DCAF, Équipe internationale de conseil au secteur de la sécurité (ISSAT), La RSS en bref. Manuel de formation : introduction à la réforme du secteur de la sécurité. Disponible sur :

https://issat.dcaf.ch/fre/download/2970/788571/LA%20RSS%20EN%20BREF%205.4%202014-07-17%20-%20low%20res%20for%20website.pdf

DCAF-ISSAT, Introduction à la réforme du secteur de la sécurité. Un cours en ligne gratuit est disponible sur le site internet de la communauté des praticiens de DCAF-ISSAT : https://issat.dcaf.ch/fre.

Heiner Hänggi, Security Sector Reform – Concepts and Contexts in Transformation: A Security Sector Reform Reader (Pasig : INCITEGov, 2011, pp. 11–40).

Hans Born et Albrecht Schnabel (dir.), Security Sector Reform in Challenging Environments (Münster : LIT Verlag, 2009).

Global Forum on Cyber Expertise, Raising cybersecurity awareness by building trust through transparency. Disponible sur : https://www.thegfce.com/news/news/2017/05/31/raising-cybersecurity-awareness-by-building-trust-through-transparency.

Evert A. Lindquist et Irene Huse, Accountability and monitoring government in the digital era: Promise, realism and research for digital era governance (Canadian Public Administration, 2017). Disponible sur : https://onlinelibrary.wiley.com/doi/full/10.1111/capa.12243

CHAPITRE 2

QUEL EST LE LIEN ENTRE CYBERESPACE, CYBERSÉCURITÉ ET LA GOUVERNANCE DU SECTEUR DE LA SÉCURITÉ ?

Objectifs

Ce chapitre fournit un aperçu plus approfondi du cyberespace et de la cybersécurité. Il vise spécifiquement à améliorer la compréhension de ces deux notions en mettant en évidence les complexités soulevées par l'application à ces domaines des bonnes pratiques en matière de gouvernance du secteur de la sécurité.

Ce chapitre vise à améliorer la compréhension des questions suivantes :

- L'ampleur, les acteurs et les risques du cyberespace.
- La cybersécurité et son impact sur la sécurité humaine, la sécurité nationale et la fourniture de services.
- Les modalités d'application et les obstacles à la mise en œuvre des bonnes pratiques en matière de GSS au cyberespace.

1. Introduction

Comme indiqué dans le chapitre précédent, les bonnes pratiques en matière de GSS jouent un rôle essentiel pour créer un environnement responsable qui assure de manière efficace le respect des droits humains et du principe de l'État de droit. Dans la mesure où le secteur de la sécurité est composé d'acteurs étatiques et non étatiques, les principes de bonne GSS doivent donc aller au-delà des seules pratiques étatiques.

Le concept de bonne GSS appliqué au cyberespace est relativement nouveau et il a de profondes répercussions aussi bien sur les autorités étatiques que sur les individus. Étant donné que le cyberespace ainsi que les activités et services qu'il propose font désormais partie intégrante de la vie quotidienne, il est primordial d'y assurer la protection des données et des informations.

En dépit de cet impératif de protection, et peut-être en raison de ses diverses utilisations, le concept de cyberespace et ses différentes composantes ne sont pas bien définis. Pour aborder de manière adéquate la question de l'application au cyberespace des bonnes pratiques en matière de GSS, il est nécessaire de comprendre de manière plus précise la signification des termes « cyberespace » et « cybersécurité ».

Qu'est-ce que le cyberespace ?

Le manque de clarté qui entoure la signification du terme cyberespace découle du fait que ce concept semble, par nature, abstrait et apparemment non ancré dans le monde physique.

Les organisations et les États ont tendance à définir le cyberespace d'une manière qui reflète les objectifs qu'ils se sont fixés dans ce domaine et l'utilisation qu'ils en ont. Ces définitions se focalisent souvent sur les questions de sécurité, de militarisation ou sur les vulnérabilités liées à ce média - chaque organisation, État et groupe mettant l'accent sur des aspects différents. Pour autant, au-delà de ces différences, la plupart des définitions ont en commun de concevoir le cyberespace comme un environnement reposant à la fois sur des composantes physiques et des éléments virtuels qui favorisent le stockage, la modification ou l'échange de données, d'informations ou de communications.

L'Internet représente sans doute la forme de cyberespace la plus répandue et la plus facilement accessible pour tout individu mais il est loin d'en constituer le seul aspect[1]. Le cyberespace inclut tout système de réseau informatique qui vise à stocker, modifierou

1 Fred Schreier, Barbara Weekes, Theodor H. Winkler, "Cyber security: The Road Forward" DCAF Horizon 2015 Working Paper No. 4, Genève : Centre pour le contrôle démocratique des forces armées, p. 8. Disponible sur https://www.dcaf.ch/sites/default/files/publications/documents/Cyber2.pdf

changer des données[2] . Ces fonctions se retrouvent notamment dans le nombre croissant de montres, appareils et autres articles connectés dans le cyberespace (également appelé l'Internet des objets - IDO). Ces différents flux de données et d'informations constituent conjointement cette construction « virtuelle » appelée cyberespace.

Le cyberespace est un domaine mondial, qui offre de très nombreuses ressources, informations et opportunités. Il est devenu un élément tellement essentiel de la vie quotidienne que le Conseil des droits de l'homme des Nations Unies a affirmé, en 2016, que « les mêmes droits dont les personnes disposent hors ligne doivent être aussi protégés en ligne, en particulier la liberté d'expression, qui est applicable indépendamment des frontières et quel que soit le média que l'on choisisse, conformément aux articles 19 de la Déclaration universelle des droits de l'homme et du Pacte international relatif aux droits civils et politiques[3] ».

Le cyberespace est également composé d'éléments physiques, notamment des ordinateurs de bureau et portables, des tablettes et des smartphones, ainsi que des serveurs et des câbles physiques qui créent l'infrastructure de l'Internet. Le cyberespace, en tant que média, permet de mener des activités qui ressemblent assez souvent à celles effectuées dans le monde physique : les individus utilisent le cyberespace pour communiquer entre eux, effectuer des transactions commerciales, mener des recherches, pratiquer des activités de loisir et se tenir informés sur l'actualité. Cependant, tous les usages du cyberespace ne sont pas aussi innocents : ce média peut également servir de vecteur pour des activités criminelles, des attaques militaires et d'autres actes répréhensibles.

2 Benjamin Buckland, Fred Schreier, et Theodor H. Winkler, "Democratic Governance Challenges of Cybersecurity" DCAF Horizon 2015 Working Paper no. 1. Genève : Centre pour le contrôle démocratique des forces armées, p. 9. Disponible sur : https://www.dcaf.ch/sites/default/files/publications/documents/CyberPaper_3.6.pdf

3 La promotion, la protection et l'exercice des droits de l'homme sur Internet, 32e session du Conseil des droits de l'homme (27 juin 2016), A/HRC/32/L.20

Définir le cyberespace
Voici quelques exemples de définitions du cyberespace employées actuellement par les acteurs suivants :

Union internationale des télécommunications (UIT)
Le cyberespace est l'environnement qui permet une communication à travers des réseaux informatiques. Le monde entier y est connecté, d'une manière ou d'une autre.

Organisation internationale de normalisation
Environnement complexe, fondé sur les interconnexions entre personnes, logiciels et services, et rendu possible par la diffusion mondiale de dispositifs et de réseaux de technologies qui y sont connectés, qui n'existe sous aucune forme physique.

Union européenne
Le cyberespace est constitué par un ensemble de biens corporels et incorporels qui stockent et / ou transfèrent des informations électroniques dans le temps.

Afrique du Sud
Le « Cyberespace » désigne un domaine physique et non physique créé et / ou composé de tout ou partie des éléments suivants : ordinateurs, systèmes informatiques, réseaux et programmes informatiques, données informatiques, données de contenu, données de trafic et utilisateurs.

(Sources : CCDCOE, disponible sur : https://ccdcoe.org/cyber-definitions.html; ENISA, ENISA overview of cybersecurity and related terminology ver. 1. Union européenne, septembre 2017, disponible sur : https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisa-overview-of-cybersecurity-and-related-terminology; State Security Agency, "The National Cybersecurity Policy Framework of South Africa", Government Gazette no. 609 (décembre 2015),p. 8.)

EXEMPLE DE BONNE PRATIQUE

Au début du XXIe siècle, la France affichait l'un des taux de pénétration d'internet et d'ordinateurs les plus bas de l'Union européenne. Aujourd'hui, cependant, une large majorité de la population utilise le cyberespace. Pour renforcer encore davantage l'accessibilité et la facilité d'utilisation du cyberespace, la France a lancé le « Très Haut Débit », une nouvelle initiative visant à promouvoir l'accès internet à haut débit, en particulier pour les populations rurales et sous-connectées. Par le biais de partenariats avec des groupes publics et privés, la France vise à atteindre une couverture à 100% de la connexion internet haut débit et un accès numérique pour l'ensemble de sa population d'ici 2022.

Source : http://www.francethd.fr/le-plan-france-tres-haut-debit/qu-est-ce-que-le-plan-france-tres-haut-debit.html

Malgré leurs points communs, ces différentes définitions institutionnelles du cyberespace ont un caractère imprécis qui laisse toute latitude aux acteurs du cyberespace pour interpréter les critères de ces définitions d'une manière qui reflète leurs besoins et justifie leurs modes d'utilisation de cet espace. Ces définitions à géométrie variable influent tout particulièrement sur la manière d'optimiser le cyberespace et de le protéger. Les définitions de cet espace reflètent également les intérêts des États, qui le conçoivent soit comme un outil militaire, soit comme une plate-forme de distribution de services, ou encore

Aux fins du présent chapitre, le cyberespace est défini comme : l'environnement mondial en réseau qui permet l'échange, le stockage et la modification des données et des informations et qui est accessible à la fois aux acteurs étatiques et non étatiques.

Utilisation et autorité dans le cyberespace

Étant donnée l'ampleur du cyberespace, il est logique que ce média implique les utilisateurs et les usages les plus divers. Les acteurs qui utilisent le cyberespace incluent à la fois des acteurs étatiques et non étatiques. Les États utilisent le cyberespace pour organiser des élections et assurer des services à leur population, tout en considérant ce média comme un outil de protection de la sécurité et des intérêts nationaux vitaux[4]. Les acteurs non étatiques incluent une variété d'acteurs, des entreprises aux individus, chacun utilisant le cyberespace à des fins différentes. Tous ces acteurs contribuent à influencer et à façonner le cyberspace.

Le caractère mondial du cyberespace impose également aux autorités étatiques des contraintes en matière de réglementation et de gouvernance. Il est certes important de renforcer la cybersécurité dans le cadre de politiques de sécurité nationales mais il est également essentiel de soutenir l'application au cyberespace des principes de bonne GSS car cela a des effets importants sur la sécurité économique et humaine[5]. Dans un monde de plus en plus dépendant des services offerts par le cyberespace et de la liberté d'action qu'il permet, il devient impératif d'assurer la protection des droits humains, de la sécurité humaine tout autant que la sécurité nationale[6] .

4 Liaropoulos, Andrew N. 2017 "Cyberspace Governance and State Sovereignty." In Democracy and an Open-Economic World Order, publié sous la direction de George C. Bitros et Nicholas C. Kyriazis, pp. 25-35, Springer International Publishing AG.

5 Cole, Kristina et al., Cybersecurity in Africa: An Assessment. Atlanta: Georgia Institute of Technology. https://www.researchgate.net/publication/267971678

6 Benjamin Buckland, Fred Schreier et Theodor H. Winkler, "Democratic Governance Challenges of Cybersecurity" DCAF Horizon 2015 Working Paper no. 1. Genève : Centre pour le contrôle démocratique des forces armées, p. 9. Disponible sur : https://www.dcaf.ch/sites/default/files/publications/documents/CyberPaper_3.6.pdf

ÉTUDE DE CAS : SÉCURISER LA COMPOSANTE PHYSIQUE

Des initiatives ont récemment été lancées afin de renforcer la sécurité des appareils informatisés tels que les ordinateurs portables, les tablettes et les smartphones. L'Union européenne et ses États membres, ainsi que les États-Unis, ont tous commencé à faire pression sur les fabricants de technologies pour qu'ils assurent la sécurité de leurs produits.

En 2016, le ministère de la Sécurité intérieure des États-Unis d'Amérique a publié plusieurs principes stratégiques visant à sécuriser l'Internet des objets. La première étape de cette approche consiste à sécuriser les appareils au moment de leur fabrication, puis à assurer leur sécurité via des mises à jour et une gestion de leurs vulnérabilités.

Le Royaume-Uni a créé un « code de bonnes pratiques pour la sécurité » à l'intention des fabricants afin de les encourager à renforcer la sécurité des appareils durant leur phase de fabrication. À cette fin, le code de bonnes pratiques recommande que les appareils de l'Internet des objets soient dotés de mots de passe réellement spécifiques ; ce code appelle également à une plus grande transparence en cas d'atteintes à la sécurité et encourage la divulgation publique de toutes les vulnérabilités des appareils. À l'heure actuelle, ce code est d'application volontaire uniquement, mais les autorités britanniques n'ont pas exclu la possibilité de rendre ces règles contraignantes pour les appareils fabriqués dans le pays.

L'approche de l'UE visant à renforcer la sécurité des appareils est toujours en cours d'élaboration. Elle visera à créer à terme un processus de certification des appareils de l'Internet des objets à l'échelle de l'UE.

Toutes ces approches visent à inciter les autres États à développer leurs propres approches et politiques afin de sécuriser les appareils connectés au cyberespace.

Source : https://www.ft.com/content/d21079b0-8a79-11e8-affd-da9960227309

Cybersécurité

Les autorités étatiques, les individus et les entreprises utilisent sans cesse davantage le cyberespace ; de ce fait, la quantité de données et d'informations sensibles qui y circulent augmente de manière exponentielle et ces informations sont soumises à des vulnérabilités nouvelles et en constante évolution[7] . Il est essentiel d'assurer une protection efficace de ces informations afin de créer un environnement sécurisé à l'intérieur et à

7 Fred Schreier, Barbara Weekes, Theodor H. Winkler, "Cyber security: The Road Forward" DCAF Horizon 2015 Working Paper No. 4, Genève : Centre pour le contrôle démocratique des forces armées, p. 11. Disponible sur : https://www.dcaf.ch/sites/default/files/publications/documents/Cyber2.pdf

l'extérieur du cyberespace. La cybersécurité, comme son nom l'indique, fait référence aux pratiques et modalités de sécurisation des données, des informations et de l'intégrité des différentes composantes du cyberespace, y compris, sans s'y limiter, les éléments physiques de ce média[8] .

Bien que la cybersécurité soit souvent associée à des stratégies de sécurité nationale, il est important d'envisager des acceptions plus larges de ce terme. L'UIT définit la cybersécurité comme un ensemble d'outils, de politiques, de lignes directrices et d'autres approches visant à protéger l'intégrité et la nature confidentielle du cyberespace pour les organisations privées, les autorités étatiques et la société civile[9] .

La cybersécurité constitue un domaine en pleine mutation dans le cadre plus large de la sécurité et de la bonne gouvernance du secteur de la sécurité, et son développement reflète l'importance croissante du cyberespace pour les activités professionnelles, récréatives et politiques. Les normes relatives à la sécurité dans le cyberespace évoluent constamment pour répondre à l'expansion rapide des pratiques et des techniques en matière de cybersécurité et pour prendre en compte la multiplicité des acteurs impliqués[10] . Les États élaborent des approches nationales pour renforcer la sécurité du cyberespace sur leur territoire. Dans le même temps, des normes commencent à émerger pour définir la portée et les modalités d'exercice des prérogatives des États sur le cyberespace[11] .

Mesures de cybersécurité

L'analyse de ce que constitue la cybersécurité est complexifiée par le caractère large et divers des définitions du cyberespace et de la cybersécurité. L'UIT a créé un indice mondial de cybersécurité afin de mesurer l'engagement de ses États membres en faveur du renforcement de la cybersécurité. Pour ce faire, cet indice évalue cinq composantes différentes de la cybersécurité qui ont trait à des questions juridiques, technologiques, organisationnelles ainsi qu'au renforcement des capacités et à la coopération.

Cet outil permet de mesurer l'engagement des États et d'évaluer les actions qu'ils prennent en matière de gouvernance du cyberespace. Cependant, il ne prend pas en compte le rôle des acteurs non étatiques dans le cyberespace et la cybersécurité. Dans la mesure où il évalue les politiques et non les pratiques, il ne permet pas non plus d'évaluer les impacts pratiques ou l'efficacité de ces engagements.

8 https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf

9 ITU guide to develop NCSS, p. 13.

10 "International Cybersecurity Norms," Microsoft Policy Papers Microsoft. Disponible sur : https://www.microsoft.com/en-us/cybersecurity/content-hub/international-cybersecurity-norms-overview

11 Ibid.

2. L'application de la GSS au cyberespace

Le cyberespace favorise une combinaison de libertés, de restrictions et de complexités qui sont propres à la nature même de ce média. La diversité des acteurs présents dans le cyberespace et le fait que ce média peut être utilisé aussi bien à bon escient qu'à des fins répréhensibles créent des obstacles à la mise en place d'un cadre favorisant l'application de bonnes pratiques en matière de GSS. Ces obstacles diffèrent de ceux auxquels sont confrontés les États pour réguler la sécurité « territoriale » plus traditionnelle. Certains de ces défis ont été examinés dans le chapitre précédent et ils concernent principalement les éléments qui affaiblissent l'État de droit, la transparence et la responsabilité.

Lorsque l'on examine la question de l'application de GSS au cyberespace, il est important de prendre en compte les différents acteurs qui y sont impliqués ; évaluer qui contrôle quels aspects du cyberespace ; et analyser comment il est possible d'influencer ou d'optimiser les comportements et les pratiques qui contribuent à terme à favoriser une bonne GSS dans le cyberespace. La diversité des acteurs du cyberespace et de la cybersécurité soulève un défi inédit pour les décideurs politiques, car l'État n'est pas en mesure d'assurer unilatéralement et de manière efficace l'utilisation sécurisée et règlementée de ce média.

Bonne pratique : Mettre en œuvre une approche de la cybersécurité qui inclut les acteurs publics et privés impliqués dans le cyberespace

Dans la mesure où le cyberespace est une plate-forme dans laquelle interviennent aussi bien des acteurs publics que privés, il est essentiel que le processus d'élaboration et la mise en œuvre des différentes politiques ayant un impact sur la GSS incluent des entités extérieures à la sphère publique. La création d'un cyberenvironnement plus sûr passe donc notamment par la prise en compte du rôle joué par les entreprises des technologies de l'information et de la communication (TIC) ainsi que par les entreprises de cybersécurité privées en matière de formation, de protection des droits des utilisateurs et de sécurité.

EXEMPLES DE BONNES PRATIQUES

Le gouvernement du Cameroun collabore avec plusieurs partenaires du secteur privé sur des questions liées à la cybersécurité et il a instauré des liens de coopération avec d'autres pays afin de traiter et de combattre les menaces informatiques. De manière emblématique, suite à une escroquerie en ligne impliquant une entreprise de vente de produits pharmaceutiques, le Cameroun a coopéré avec la République tchèque, INTERPOL et le Nigéria pour enquêter sur ces fraudes numériques. Les autorités camerounaises soutiennent plusieurs initiatives pour renforcer la confiance dans le cyberespace et elles font la promotion d'accords de coopération internationale en partageant des informations sur des cyberincidents et des bonnes pratiques en matière de cybersécurité.

Problèmes actuels liés à l'application de la GSS au cyberespace

L'application au cyberespace de bonnes pratiques en matière de GSS peut contribuer à renforcer le respect et la protection de la sécurité humaine, de l'État de droit et d'autres aspects de la bonne gouvernance.

Comme indiqué brièvement dans le chapitre précédent, l'un des défis auxquels est confrontée l'application de la bonne gouvernance au cyberespace réside dans le manque de compréhension quant à la manière d'y appliquer des principes de gouvernance efficaces, ce qui entraîne des politiques et une réglementation inadéquates et favorise un environnement propice aux activités criminelles[12] . Ce manque de connaissances peut également avoir une incidence sur l'efficacité de la réglementation des États à l'égard des acteurs du secteur privé et donc compromettre la capacité de l'État à appliquer au cyberespace des pratiques de bonne gouvernance.

À l'heure actuelle, de nombreux services de sécurité du cyberespace sont assurés par des entités commerciales privées, ce qui soulève des difficultés pour l'application efficace des pratiques de GSS au cyberespace. La transparence constitue, à cet égard, l'un des aspects de la bonne gouvernance qu'il est de plus en plus difficile de mettre en œuvre. Une première difficulté pour répondre à ce défi tient au fait qu'il n'existe pas de définition claire de ce que constitue la transparence dans une perspective de bonne GSS. Cependant, la notion de transparence dans ce contexte est de plus en plus associée à la divulgation du moment auquel une violation des systèmes d'information a eu lieu et du degré de gravité de cet acte[13]

ÉTUDE DE CAS : IMPOSER LA TRANSPARENCE

Australie

En 2017, le Parlement australien a adopté un amendement à la Privacy Act de 1998 qui fait obligation aux entités gouvernementales fédérales, aux organisations du secteur privé et à d'autres organes spécifiques de divulguer des informations concernant les atteintes à la cybersécurité aux personnes concernées. Si ces acteurs ne respectent pas cette nouvelle réglementation, ils devront verser une indemnisation financière aux personnes affectées ; reconnaître publiquement leur responsabilité et présenter leurs excuses ; et ils peuvent faire l'objet de lourdes sanctions civiles en cas de récidive.

Source: Ben Allen, "Australia: Cybercrime – New Mandatory Data Breach Reporting Requirements" mondaq, www.mondaq.com. Disponible sur : http://www.mondaq.com/australia/x/573188/Security/Cybercrime+New+Mandatory+Data+Breach+Reporting+Requirements

États Unis d'Amérique

La Securities and Exchange Commission des États-Unis a infligé une lourde amende de 35 millions de dollars USD à Yahoo pour ne pas avoir révélé une cyberattaque ayant affecté plus de 500 millions de comptes. Il s'agissait de la première condamnation d'une entreprise à une amende pour ne pas avoir respecté les obligations de divulgation d'informations imposées aux entreprises cotées en bourse.

Source : Kadhim Shubber, "Yahoo's $35m Fine Sends a Message", Financial Times, www.ft.com. Disponible sur : https://www.ft.com/content/4c0932f0-6d8a-11e8-8863-a9bb262c5f53

12 Buzatu, SSG/SSR in Cyberspace, p. 7-8.

13 Voir, par exemple, ICANN Organization's Cybersecurity Transparency Guidelines (2018), disponible sur : https://www.icann.org/en/system/files/files/cybersecurity-transparency-guidelines-03aug18-en.pdf

L'État peut renforcer les bonnes pratiques de GSS en encourageant ou en obligeant les acteurs à divulguer les atteintes à la cybersécurité. En effet, cela renforce non seulement la transparence dans le cyberespace, mais garantit également que des mesures sont prises pour combler les lacunes dans les pratiques actuelles en matière de cybersécurité, ce qui contribue à lutter contre la propagation de cyberattaques et à améliorer les pratiques de sécurité dans le cyberespace[14] . Le manque de transparence à l'égard des cyberattaques nuit gravement à la sécurité humaine dans le cyberespace, car cela peut accroître le nombre de victimes touchées par des cyberattaques malveillantes.

La nature transnationale du cyberespace soulève également un dilemme pour les États qui souhaitent y appliquer de bonnes pratiques de GSS. Les individus sont de plus en plus impliqués dans des transactions qui dépassent les frontières territoriales internationales, ce qui réduit de manière considérable la capacité de l'État d'exercer son autorité pour lutter contre les conséquences de ces actes sur sa population. Dans la plupart des cas, les États doivent faire appel à des intermédiaires commerciaux - tels que des plateformes de médias sociaux - pour surveiller et réglementer les comportements en ligne[15] . Cela peut saper les bonnes pratiques en matière de GSS, dans la mesure où l'État ne peut généralement pas savoir comment les informations sont filtrées ou supprimées. La nature transnationale des informations diffusées sur Internet présente un autre défi car ces données peuvent être stockées sur un ou plusieurs serveurs situés dans des États différents. Les autorités étatiques doivent donc compter sur une nouvelle forme de coopération avec d'autres États pour pouvoir enquêter, poursuivre en justice et condamner les cybercriminels. Le cyberespace sape ainsi les pratiques de bonne gouvernance car il implique non seulement des acteurs relevant de la compétence d'un seul État mais il a également une incidence sur un éventail d'acteurs au niveau international.

ÉTUDE DE CAS : ENQUÊTES INTERNATIONALES

La cybersécurité a déjà donné lieu à des enquêtes internationales et des poursuites pénales. En avril 2018, Webstresser.org, un site internet vendant des services de déni de service distribué (DDoS), a été gelé et les administrateurs de ce site ont été inculpés de cybercriminalité à l'issue d'une enquête internationale menée par l'unité de la police néerlandaise spécialisée en criminalité de haute technologie et de l'Agence nationale de lutte contre la criminalité du Royaume-Uni avec le soutien de nombreuses autres organisations. Cette opération appelée « Operation Power Off » constitue un exemple parmi d'autres de la manière dont les acteurs internationaux peuvent coopérer pour créer un environnement offrant davantage de cybersécurité aux utilisateurs.

Sources : Cal Jeffrey, "Operation Power OFF pulls the plug on 'DDoS-for-hire' website" TechSpot www.techspot.com. 25 avril 2018. Disponible sur : https://www.techspot.com/news/74327-operation-power-off-pulls-plug-ddos-hire-website.html et "World's Biggest Marketplace Selling Internet Paralysing DDoS Attacks Taken Down" Europol Europol.europa.org, communiqué de presse. 25 avril 2018. Disponible sur : https://www.europol.europa.eu/newsroom/news/world%E2%80%99s-biggest-marketplace-selling-internet-paralysing-ddos-attacks-taken-down

14 Paul Smith "New mandatory data breach notifications laws to drag Australia into cyber age" Financial Review, afr.com, 23 février 2018. Disponible sur : https://www.afr.com/technology/new-mandatory-data-breach-notifications-laws-to-drag-australia-into-cyber-age-20180222-h0whxa

15 Niva Elkin-Koren; Eldar Haber, "Governance by Proxy: Cyber Challenges to Civil Liberties," Brooklyn Law Review, 82 no. 1, p. 105.

Malgré ces nombreux défis, il n'est pas impossible d'appliquer les bonnes pratiques de la GSS au cyberespace. Des cadres et normes internationaux commencent à émerger pour fournir des orientations quant à la manière d'intégrer les pratiques de GSS au cyberespace. Certes, ces pratiques et politiques internationales doivent être adaptées au contexte national. Mais l'identification des cadres internationaux et régionaux pertinents pour le cyberespace constitue une première étape pour appliquer les principes d'une bonne GSS au cyberespace.

Conclusions Clés

- Le cyberespace se manifeste aussi bien sur le plan physique que non physique et il est constitué de toute plate-forme sur laquelle des informations, des données et des communications peuvent être transférées, transformées ou modifiées d'un ordinateur à un autre. Il englobe également l'infrastructure physique d'Internet qui couvre le monde entier.
- Les autorités étatiques, les individus et les entreprises dépendent de plus en plus dans leurs activités quotidiennes des ressources fournies par le cyberespace.
- Il existe un large éventail d'acteurs impliqués dans le cyberespace et la cybersécurité.
- Les initiatives visant à appliquer les principes de la GSS au cyberespace sont confrontées à plusieurs obstacles, notamment la présence de nombreux acteurs ayant une influence sur différents aspects du cyberespace ainsi que le manque général de connaissances sur les manières d'utiliser le cyberespace en toute sécurité.
- Bien que certains États aient adopté des politiques et des cadres en matière de cybersécurité et de gouvernance du cyberespace, le manque général de connaissances en la matière constitue un obstacle à l'application adéquate des pratiques de GSS au cyberespace.

Bibliographie

Buckland, Benjamin, Fred Schreier, et Theodor H. Winkler, “Democratic Governance Challenges of Cybersecurity” DCAF Horizon 2015 Working Paper no. 1. Genève : Centre pour le contrôle démocratique des forces armées. Disponible sur : https://www.dcaf.ch/sites/default/files/publications/documents/CyberPaper_3.6.pdf

Elkin-Koren, Niva et Eldar Haber, “Governance by Proxy : Cyber Challenges to Civil Liberties”, 82 Brook. L. Rev.105 (2016)

Fred Schreier, Barbara Weekes, Theodor H. Winkler, “Cyber security: The Road Forward” DCAF Horizon 2015 Working Paper No. 4, Genève : Centre pour le contrôle démocratique des forces armées. Disponible sur: https://www.dcaf.ch/sites/default/files/publications/documents/Cyber2.pdf

Liaropoulos, Andrew N., 2017 “Cyberspace Governance and State Sovereignty.” In Democracy and an Open-Economic World Order, coordonné par George C. Bitros et Nicholas C. Kyriazis, pp. 25-35. Springer International Publishing AG.

Paul Smith, “New mandatory data breach notifications laws to drag Australia into cyber age” Financial Review, afr.com, 23 février 2018. Disponible sur : https://www.afr.com/technology/new-mandatory-data-breach-notifications-laws-to-drag-australia-into-cyber-age-20180222-h0whxa

Cole, Kristina, Marshini Chetty, Christopher LaRosa, Frank Rietta, Danika K. Schmitt et Seymour E. Goodman, Cybersecurity in Africa : An Assessment. Atlanta: Georgia Institute of Technology. Disponible sur: https://www.researchgate.net/publication/267971678

CHAPITRE 3

CADRES JURIDIQUES INTERNATIONAUX ET RÉGIONAUX APPLICABLES AU CYBERESPACE

Objectifs

Ce chapitre vise à fournir un aperçu des cadres juridiques internationaux et régionaux applicables au cyberespace et il met en évidence des approches et des initiatives intéressantes et novatrices en la matière.

Ce chapitre vise à améliorer la compréhension des questions suivantes :

- Les différentes organisations internationales et régionales traitant du cyberespace et de la cybersécurité.
- Les ressources disponibles pour soutenir la mise en œuvre des cadres juridiques internationaux et régionaux au niveau national.
- Les phénomènes de cybercriminalité, cyberterrorisme et d'utilisation d'Internet à des fins terroristes.

Introduction

L'existence de cadres juridiques efficaces - aux niveaux international, régional et national - constitue l'un des piliers de la bonne gouvernance ; il s'agit également d'une condition préalable au respect du principe de l'État de droit. De manière générale, les cadres juridiques jouent un rôle essentiel pour réglementer les comportements licites et interdire ou criminaliser les activités illégales. L'application de cadres juridiques au cyberespace joue également un rôle fondamental pour assurer le respect des droits humains.

La question de l'application des cadres juridiques au cyberespace et de leur mise en œuvre fait l'objet de vifs débats tout en suscitant beaucoup de confusion. De par sa nature, en tant qu'espace transfrontalier et centré sur le flux de données immatérielles, le cyberespace soulève des défis pour la gouvernance, traditionnellement définie par rapport à l'État territorial. En effet, si l'infrastructure matérielle du cyberespace peut être soumise à la compétence et à l'autorité de l'État, celui-ci peut, par contre, difficilement exercer un « contrôle effectif » sur le flux de données et d'informations qui y sont véhiculées et qui traversent en permanence les frontières territoriales. Cela a conduit de nombreux acteurs à appeler à l'élaboration de nouveaux régimes normatifs afin de réglementer le cyberespace.

Le fait que les principes du droit international soient applicables au cyberespace fait dorénavant consensus. Cependant, leur modalité d'application dans la pratique est beaucoup moins clairement établie. Cet écart entre la politique et la pratique suscite donc des incertitudes, voire des lacunes juridiques qui peuvent porter atteinte à la protection des droits humains des utilisateurs de l'Internet. Par conséquent, des organisations internationales et régionales ont lancé des initiatives visant à identifier les principes juridiques du droit international susceptibles de s'appliquer au cyberespace et à examiner leurs modalités d'application.

1.Cadre juridique et régional international

De nombreuses initiatives sont menées aux niveaux international et régional afin de promouvoir un comportement plus responsable dans le cyberespace et pour élaborer des cadres réglementaires et des mesures de confiance applicables au cyberespace. Vous trouverez ci-dessous un aperçu de plusieurs de ces initiatives.

Nations Unies

Il n'existe actuellement aucun instrument juridiquement contraignant au niveau international régissant le comportement dans le cyberespace. Cependant, plusieurs initiatives juridiquement non contraignantes identifient les normes susceptibles d'être appliquées au cyberespace et proposent des orientations aux États quant à leurs modalités d'application.

L'application au cyberespace du droit international - en particulier de la Charte des Nations Unies, du droit international relatif aux droits humains et du droit international humanitaire - fait dorénavant consensus.

ÉTUDE DE CAS : RAPPORT DU GROUPE D'EXPERTS GOUVERNEMENTAUX DES NATIONS UNIES

Le rapport de 2015 du Groupe d'experts gouvernementaux (GEG) des Nations Unies a formulé les recommandations suivantes pour que les États adoptent un comportement responsable contribuant à un cyberespace ouvert, sécurisé, stable, accessible et pacifique :

Normes positives :

- Les États devraient coopérer pour renforcer la stabilité et la sécurité de l'utilisation des TIC et en prévenir les pratiques préjudiciables.
- Les États devraient examiner toutes les informations pertinentes concernant l'attribution des compétences en matière de TIC.
- Les États devraient prendre les mesures appropriées pour protéger leurs infrastructures nationales critiques contre les menaces liées aux TIC et répondre aux demandes d'assistance formulées par d'autres États.
- Les États devraient prendre des mesures raisonnables pour assurer l'intégrité de la chaîne d'approvisionnement et prévenir la prolifération d'outils et de techniques malveillants en matière de TIC.
- Les États devraient encourager des procédures de signalement responsable des vulnérabilités en matière de TIC et partager les informations en la matière.

Normes imposant une limitation :

- Les États ne devraient pas sciemment permettre que leur territoire soit utilisé pour commettre des actes internationalement illicites à l'aide de TIC.
- Les États devraient adhérer aux résolutions de l'Assemblée générale des Nations Unies relatives aux droits humains.
- Les États ne devraient pas soutenir sciemment les activités liées aux TIC qui sont en violation des obligations qui leur incombent aux termes du droit international.
- Les États ne devraient pas mener ni soutenir sciemment des activités visant à porter atteinte aux systèmes d'information des équipes d'intervention d'urgence officielles.

Par exemple, depuis 2004, les Nations Unies ont créé six groupes d'experts gouvernementaux (GEG) consécutifs chargés de concevoir des normes de comportement responsable dans le cyberespace. La composition de ces groupes d'experts est basée sur une « répartition géographique équitable » et ils comprennent les « cyber-puissances » clés, tels que les États-Unis d'Amérique, la Chine, la Russie, la France, le Royaume Uni et l'Allemagne.

ÉTUDE DE CAS : INGÉRENCE ÉLECTORALE EN LIGNE : UNE SITUATION RELEVANT DU DROIT INTERNATIONAL ?

Les cas d'ingérences dans les processus politiques, ouvertement ou à couvert, marquent depuis longtemps les relations internationales. Cependant, depuis 2016, des responsables étatiques, principalement occidentaux, se sont inquiétés de cas d'ingérences dans des processus électoraux par le biais de cyber-opérations ciblées et de campagnes de désinformation.

En 2014, la Commission électorale centrale de l'Ukraine a été la cible d'opérations menées par CyberBerkut qui a réussi à interrompre les réseaux informatiques de la commission pendant près de vingt heures et qui a annoncé de faux résultats le jour du scrutin. En 2016, l'unité de piratage informatique « Fancy Bear » a ciblé le Bundestag allemand, les ministères allemands des Affaires étrangères et des Finances ainsi que les systèmes informatiques de l'Union démocrate-chrétienne. En France, en 2017, la campagne d'Emmanuel Macron, candidat à la présidence, a été l'objet de cyber-opérations qui ont cherché à implanter des programmes malveillants sur des sites internet de la campagne.

Aux termes des obligations du droit international, ces actes sont susceptibles de constituer une violation de la souveraineté des États concernés. La souveraineté étatique est généralement considérée comme un principe et une règle essentiels du droit international – et cela a été réitéré dans le rapport 2015 du GGE des Nations Unies.

« Les normes et principes internationaux qui procèdent de la souveraineté étatique s'appliquent à l'utilisation de l'outil informatique par les États ainsi qu'à leur compétence territoriale en matière d'infrastructure informatique. »

De manière générale, le principe de la souveraineté a pour objet « de permettre à un État d'exercer un contrôle total sur l'accès à son territoire et sur les activités menées dans celui-ci ».

Quelles sont les implications de ce principe dans le cas d'une ingérence électorale par le biais de cyber-opérations ?

Selon les experts en la matière, la question clé à examiner afin de pouvoir déterminer si ce type d'actions constitue une violation du principe de souveraineté n'est « pas de savoir s'il existe un lien direct entre le système ciblé et le processus électoral, mais simplement de pouvoir établir que l'opération a entraîné le préjudice recherché - une perte de fonctionnalité ». Le Manuel de Tallinn 2.0 indique que les actions susceptibles d'être qualifiées

de violation de la souveraineté sont les suivantes : une cyber-opération qui entraîne une altération du fonctionnement de la cyber-infrastructure ou des programmes ; la modification ou la suppression des données stockées dans la cyber-infrastructure sans que cela n'entraîne de conséquences physiques ou fonctionnelles, comme décrit ci-dessus ; l'introduction de logiciels malveillants dans un système ; l'installation de portes dérobées et le fait de provoquer une perte de fonctionnalité temporaire, mais significative, comme dans le cas d'une opération majeure de déni de service distribué.

Une avancée majeure a été accomplie en 2013, lorsque le Groupe d'experts gouvernementaux (GEG) des Nations Unies, qui ne comprenait à l'époque que quinze membres, a adopté par consensus un rapport qui entérine l'applicabilité du droit international au cyberespace. Cette position a été réaffirmée dans le rapport 2015 du GEG, lui aussi adopté par consensus. Ce rapport a précisé la portée du cadre normatif réglementant les cyber-capacités des États. Une section de ce rapport portant sur les « normes, règles, et principes de comportement responsable des États » est, à cet égard, particulièrement intéressante.

Malheureusement, le Groupe d'experts des Nations Unies 2016-2017 n'est pas parvenu à adopter un rapport par consensus, ce qui a provoqué une confusion au sein de la communauté internationale quant aux modalités d'application du droit international au cyberespace. Cependant, en octobre 2018, l'Assemblée générale des Nations Unies a adopté la résolution A/C.1/73/L.37 portant création d'un autre groupe d'experts gouvernementaux en 2019, qui devra rendre compte de ses travaux en 2021 lors de la 76ème session de l'Assemblée générale. Dans le même temps, l'Assemblée générale des Nations Unies a adopté la résolution A/C.1/73/L.27/Rev.1 créant un groupe de travail à composition non limitée qui se réunira en juin 2019 ; ce groupe de travail est chargé de définir les règles, normes et principes régissant le comportement responsable des États dans le cyberespace et de déterminer la mise en œuvre pratique de ces règles.

Il est généralement admis que le cadre juridique international des droits humains, et notamment la Déclaration universelle des droits de l'homme (DUDH) et le Pacte international relatif aux droits civils et politiques (PIDCP), s'applique au cyberespace. Cela a été affirmé par le Conseil des droits de l'homme (CDH) dans sa résolution A/HRC/20/L.13 qui précise que « les droits dont les personnes jouissent hors ligne doivent également être protégés en ligne[1] ». Cette résolution revêt une importance particulière car c'était la première fois que cet organe international déclarait explicitement que les droits humains s'appliquaient également au cyberéspace.

ENCADRÉ : L'ANONYMAT SUR INTERNE

Le droit à l'anonymat joue un rôle essentiel dans la protection des droits humains. Avec l'avènement de l'Internet, il apparaît clairement que le droit à l'anonymat ne peut pas se limiter à la liberté des individus de communiquer des informations et des idées mais doit également protéger les individus contre les contrôles inutiles ou disproportionnés. Cependant, à ce jour, le droit à l'anonymat en ligne n'a été reconnu que partiellement dans le droit international. Traditionnellement, la protection de l'anonymat en ligne a été liée à la protection du droit au respect de la vie privée et à la protection des données à caractère personnel (voir article 12 de la DUDH, article 17 du PIDCP).

L'anonymat est un concept essentiel de la protection de la liberté d'expression ainsi que du droit au respect de la vie privée. Dans sa forme la plus simple, l'anonymat implique le fait de ne pas être identifié et, dans ce sens, il relève de l'expérience quotidienne ordinaire de la plupart des individus, par ex. marcher au sein d'une foule ou faire la queue parmi des personnes que l'on ne connaît pas. De ce fait, une activité peut être anonyme tout en étant publique.

Source: https://www.article19.org/data/files/medialibrary/38006/Anonymity_and_encryption_report_A5_french-final-pdf.pdf

1 Assemblée générale des Nations Unies, Conseil des droits de l'homme, La promotion, la protection et l'exercice des droits de l'homme sur l'Internet, Doc. ONU, A/HRC/20/L.13, 29 juin 2012.

À la suite des révélations d'Edward Snowden[2], l'Assemblée générale des Nations Unies a décidé, en 2015, de créer le mandat de rapporteur spécial sur le droit à la vie privée afin de renforcer le droit à la vie privée à l'ère numérique et de créer un environnement numérique plus sûr. Ce rapporteur spécial a pour mandat d'effectuer des visites dans des États, de formuler des recommandations et d'examiner des plaintes individuelles.

L'Assemblée générale des Nations Unies a adopté une autre résolution importante (A/RES/57/239) qui porte sur la création d'une culture mondiale de la cybersécurité. Cette résolution reconnait que la cybercriminalité constitue un défi majeur pour la cybersécurité[3].

Les Principes directeurs des Nations Unies relatifs aux entreprises et aux droits de l'homme[4] (également connus sous le nom de « Principes Ruggie »), adoptés en 2011, sont un autre instrument pertinent pour identifier les normes applicables au cyberespace. Ces Principes proposent des orientations aux États et aux entreprises pour renforcer la protection des droits humains. Les Principes Ruggie sont basés sur le cadre des Nations Unies « Respecter, protéger et réparer ». La partie introductive de ces principes directeurs rappelle « [l]e rôle dévolu aux entreprises en qualité d'organes spécialisés de la société remplissant des fonctions particulières, tenues de se conformer à toutes les lois applicables et de respecter les droits de l'homme[5] ».

En ce qui concerne la réglementation de certains types de discours illégaux en ligne, en particulier les discours de haine, le rapport du Haut-Commissaire des Nations Unies aux droits de l'homme, entériné par le Conseil des droits de l'homme en 2013 (également appelé « Plan d'action de Rabat »), précise les critères permettant d'identifier les discours de haine et offre plus largement des orientations sur les activités en ligne [6].

ÉTUDE DE CAS : PLAN D'ACTION DE RABAT

Le plan d'action de Rabat identifie six critères pour évaluer la gravité de certaines expressions susceptibles d'être considérées comme des infractions pénales. Ces six critères sont : le contexte ; l'orateur ; l'objet ; le contenu et la forme ; l'ampleur du discours ; la probabilité y compris l'imminence.

En ce qui concerne le critère du « contexte », le Plan d'action de Rabat précise que celui-ci « est très important pour évaluer le degré de certains discours d'incitation à la discrimination, à l'hostilité ou à la violence envers un groupe visé. Le contexte peut avoir une incidence directe sur l'intention et/ou la causalité. L'analyse du contexte devrait situer l'acte verbal dans les contextes sociaux et politiques qui existent au moment où l'acte verbal a été émis et propagé ».

Source : https://www.ohchr.org/Documents/Issues/Opinion/SeminarRabat/Rabat_draft_outcome_FR.pdf

Plusieurs agences et bureaux des Nations Unies, tels que l'Institut des Nations Unies pour la recherche sur le désarmement (UNIDIR), l'Institut interrégional de recherche des Nations Unies sur le crime et la justice et l'Office des Nations Unies contre la drogue et

2 The Guardian, The NSA files, disponible sur : https://www.theguardian.com/us-news/the-nsa-files

le crime (UNODC), traitent de questions liées à la cybersécurité ; c'est le cas également du Groupe de travail sur la lutte contre l'utilisation de l'Internet à des fins terroristes qui agit sous l'égide de l'Équipe spéciale de lutte contre le terrorisme[7] .

L'Union internationale des Télécommunications (UIT), une agence des Nations Unies spécialisée dans les télécommunications, traite également de questions liées à la cybersécurité dans le cadre de son mandat. À cette fin, l'UIT a élaboré des lois types et des profils pays en matière de cybersécurité, qui sont publiquement accessibles. L'UIT apporte également un appui aux États membres des Nations Unies pour élaborer des cadres normatifs efficaces applicables au cyberespace.

ÉTUDE DE CAS : LE PROJET DE L'UNION INTERNATIONALE DES TÉLÉCOMMUNICATIONS VISANT À APPUYER L'HARMONISATION DES POLITIQUES EN MATIÈRE DE TIC EN AFRIQUE SUBSAHARIENNE (HIPSSA)

Le projet d'« Appui à l'harmonisation des politiques en matière de TIC en Afrique subsaharienne » (HIPSSA) a été lancé à la suite d'une demande d'assistance adressée à l'UIT et la Commission européenne par des organisations d'intégration économiques africaines ainsi que par des associations régionales de régulateurs qui souhaitaient harmoniser les politiques et législations en matière de TIC en Afrique subsaharienne.

Le projet HIPSSA joue un rôle clé pour l'élaboration de politiques et de cadres harmonisés panafricains en matière de TIC.

Source : https://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Pages/Projet_HIPSSA_fran%C3%A7ais.aspx

Conseil de l'Europe

Le Conseil de l'Europe (CdE) est composé de 47 États membres. Sa Convention sur la cybercriminalité (également appelée « Convention de Budapest »)[8] constitue à l'heure actuelle l'instrument juridique international qui propose le cadre juridique le plus efficace pour lutter contre la cybercriminalité. La Convention de Budapest est ouverte à l'adhésion des États membres du CdE ainsi que des États non membres. À ce jour, la Convention de Budapest a été ratifiée par 61 États[9]. La Convention de Budapest est assortie d'un Protocole additionnel relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques[10] .

La Convention de Budapest constitue un outil important car elle fournit aux États (i) une liste des attaques informatiques constitutives d'infractions pénales ; (ii) des instruments de droit procédural permettant d'optimiser l'efficacité des enquêtes sur la cybercriminalité et de renforcer la sécurité des preuves électroniques d'une infraction pénale dans le respect des garanties de l'État de droit et (iii) des modalités de coopération au niveau international entre les polices et les justices en matière de cybercriminalité et de collecte de preuves électroniques.

En outre, le CdE a élaboré une Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Convention STE n°108)[11],

11 Conseil de l'Europe, Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, STE No. 180. Disponible sur : https://rm.coe.int/16808ade9d

qui vise à « protéger toute personne physique, quelle que soit sa nationalité ou sa résidence, à l'égard du traitement des données à caractère personnel, contribuant ainsi au respect de ses droits de l'homme et de ses libertés fondamentales et notamment du droit à la vie privée[12] ».

Cette convention est le premier instrument international juridiquement contraignant en matière de protection des données. Aux termes de cette convention, les parties sont tenues d'adopter les mesures nécessaires dans leur législation nationale pour garantir le respect, sur leur territoire, des droits fondamentaux de tous les individus, eu égard au traitement des données à caractère personnel. La convention n° 108 a été actualisée, en mai 2018, pour prendre en compte les évolutions les plus récentes en matière de nouvelles technologies et de protection des données. À ce jour, cette Convention a été ratifiée par 53 États membres et non membres du CdE[13].

En outre, le CdE fournit des orientations pour interpréter les conventions et divers programmes de renforcement des capacités, tels que son programme GLACY +, qui aide les États à élaborer une législation efficace applicable au cyberespace[14].

La Convention de Budapest est le seul cadre juridique international réglementant la cybercriminalité mais les défenseurs des droits humains soulignent, en particulier, le fait que cette Convention part du principe que les États disposent déjà de mesures de protection des droits humains.

Cependant, les États non membres du CdE ne disposent pas nécessairement des mêmes dispositifs de protection des droits humains.

Union africaine

En 2014, l'Union africaine a adopté la Convention sur la cybersécurité et la protection des données à caractère personnel (également appelée « Convention de Malabo »)[15]. Cependant, cette convention n'est pas encore entrée en vigueur car elle n'a été ratifiée que par cinq États membres de l'Union africaine (Ghana, Guinée, Maurice, Namibie et Sénégal) et signée par neuf autres États membres. Son article 25 (1) précise que : « Chaque État Partie s'engage à adopter les mesures législatives et/ou réglementaires qu'il jugera efficaces en considérant comme infractions criminelles substantielles des actes qui affectent la confidentialité, l'intégrité, la disponibilité et la survie des systèmes technologies de l'information et de la communication et les données qu'ils traitent et des infrastructures réseau sous-jacentes, ainsi que les mesures procédurales qu'il jugera efficaces pour rechercher et poursuivre les contrevenants. Les États Parties s'engagent à prendre en considération le choix du langage utilisé dans les meilleures pratiques internationales ».

ÉTUDE DE CAS : LA CONVENTION SUR LA CYBERSÉCURITÉ DE L'UNION AFRICAINE ET LA CONVENTION DE BUDAPEST

La Convention de Budapest est actuellement le seul cadre international juridiquement contraignant qui réglemente la cybersécurité, le cyberespace et le rôle de l'État en la matière. Bien que seuls quelques pays africains l'aient signée ou aient été invités à y adhérer, la Convention de Budapest a servi de cadre directeur pour l'élaboration de la Convention de l'Union africaine sur la cybersécurité. C'est un exemple de la manière dont des normes internationales peuvent être adaptées et adoptées dans un contexte régional.

Source : "Comparative Analysis of the Malabo Convention of the African Union and the Budapest Convention on Cybercrime" Global Action on Cybercrime Extended. 20 (novembre 2016), 3-5.

12 Conseil de l'Europe, Convention modernisée pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, disponible sur : https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65c0

13 La convention n ° 108 a été ratifiée par le Cap Vert, Maurice, le Sénégal et la Tunisie.

14 Conseil de l'Europe, Action Globale sur la Cybercriminalité Elargie (GLACY+), disponible sur : https://www.coe.int/fr/web/cybercrime/glacyplus.

15 Union africaine, Convention sur la cybersécurité et la protection des données à caractère personnel, juin 27, 2014. Disponible sur : https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_f.pdf

Communauté économique des États de l'Afrique de l'Ouest

En 2010, la Communauté économique des États de l'Afrique de l'Ouest (CEDEAO) a adopté l'Acte additionnel relatif à la protection des données à caractère personnel dans l'espace de la CEDEAO[16] . Cet instrument, qui reflète les Directives de l'UE sur la protection des données, précise les dispositions qui devraient figurer dans la législation relative à la protection des données et fait obligation aux États membres d'établir une autorité de protection des données.

La CEDEAO a également adopté une directive portant lutte contre la cybercriminalité dans l'espace de la CEDEAO (2011) et l'Acte additionnel portant transactions électroniques dans l'espace de la CEDEAO[17] .

Organisation pour la sécurité et la coopération en Europe

L'Organisation pour la sécurité et la coopération en Europe (OSCE) traite des problèmes de cybersécurité et des questions liées à l'utilisation des TIC, en particulier dans l'objectif de lutter contre le terrorisme et la cybercriminalité. En 2013, l'OSCE a adopté des mesures de confiance applicables au cyberespace (Décision No 1106 du Conseil permanent du 3 décembre 2013[18]). Ces mesures de confiance visent à réduire les risques de conflit découlant de l'utilisation des technologies d'information et de communication.

Parmi les mesures de confiance identifiées par l'OSCE figure l'échange volontaire d'informations entre États portant sur : les cybermenaces ; la sécurité des TIC et leur utilisation ; l'organisation et les stratégies étatiques et la terminologie utilisée au niveau national. Ces mesures de confiance incluent également : la tenue de consultations afin de réduire les risques de malentendus et d'éventuelles tensions ; le partage d'informations sur les mesures prises par les États pour assurer un Internet ouvert et sécurisé ; l'échange de points de contact et l'utilisation de l'OSCE comme plateforme de dialogue.

Cependant, ces mesures de confiance reposent sur une approche volontaire et ne constituent, par conséquent, pas un instrument juridiquement contraignant.

Organisation des États américains

L'Organisation des États américains (OEA) a créé, dès 1999, un groupe de travail sur la cybercriminalité en tant que forum clé « pour renforcer la coopération internationale en matière de prévention, d'enquête et de poursuite de la cybercriminalité, faciliter l'échange d'informations et d'expériences entre ses membres, et formuler les recommandations

16 CEDEAO, Acte additionnel relatif à la protection des données à caractère personnel dans l'espace de la CEDEAO, https://apdp.ml//wp-content/uploads/pdf/Acte_add_donnA9es_personnelles_fr.pdf

17 Communauté économique des États de l'Afrique de l'Ouest (CEDEAO),
Directive C/DIR/1/08/11 du 19 août 2011 portant lutte contre la cybercriminalité dans l'espace de la CEDEAO. Disponible sur : http://www.osiris.sn/Directive-C-DIR-1-08-11-du-19-aout.html et CEDEAO, Acte additionnel A/SA.2/01/10 portant transactions électroniques dans l'espace de la CEDEAO. Disponible sur : http://www.osiris.sn/Acte-Additionnel-A-SA-SA-2-01-10,8792.html

18 Décision de OSCE No. 1202, Mesures de confiance de l'OSCE visant à réduire les risques de conflit découlant de l'utilisation des technologies d'information et de communication, PC.DEC/1202, 10 mars 2016. Disponible sur : https://www.osce.org/fr/pc/228491?download=true

nécessaires afin d'appuyer et d'assurer les efforts de lutte contre ces crimes[19] ». Ce groupe de travail se réunit deux fois par an et formule des recommandations à l'intention des États membres.

L'OEA traite également de la cybersécurité au sens large du terme. En 2004, l'Assemblée générale de l'OEA a adopté la résolution AG/RES.2004 (XXXIV-O/04) intitulée « Adoption d'une stratégie interaméricaine intégrée pour combattre les menaces à la cybersécurité » qui a confié au Secrétariat du Comité interaméricain de l'OEA le mandat de lutter contre le terrorisme. Les tâches principales de ce secrétariat sont de : favoriser la création d'équipes nationales d'intervention en cas d'incident de sécurité informatique (CSIRT) ; créer un réseau composé de ces CSIRT et soutenir l'élaboration de stratégies nationales de cybersécurité. Depuis 2007, le Secrétariat a lancé un programme complet de renforcement des capacités en proposant des ateliers, des formations techniques, des tables rondes sur les politiques, des exercices de gestion de crise et en favorisant l'échange de bonnes pratiques.

Organisation de coopération de Shanghai

L'Organisation de coopération de Shanghai (OCS), une organisation internationale regroupant six États membres (Chine, Kazakhstan, Kirghizistan, Ouzbékistan, Russie et Tadjikistan) a adopté, en 2009, un accord visant à garantir la sécurité internationale de l'information[20]. En 2011, quatre États membres de l'OCS ont soumis à l'Assemblée générale des Nations Unies un projet de code de conduite international pour la sécurité de l'information. En 2015, un nouveau projet de code de conduite international a été soumis à l'Assemblée générale des Nations Unies[21].

ÉTUDE DE CAS : PROJET DE CODE DE CONDUITE INTERNATIONAL DE L'OCS (2015)

Les États de l'OSC ont parrainé un projet de code qui vise, selon ses inspirateurs, à « faire avancer le débat international sur les normes internationales en matière de sécurité de l'information et à favoriser un consensus rapide sur cette question ».

Selon certains observateurs, ce projet de code met l'accent sur l'application au cyberespace des principes de souveraineté étatique et de territorialité et souligne les besoins des services de renseignement et les impératifs en matière de sécurité nationale et de stabilité des régimes politiques. Il ne prévoit pas de protection substantielle des droits humains et traite principalement des restrictions à la liberté d'expression que les États peuvent imposer aux termes de la loi. Il convient également de noter que ce projet de code ne fait aucune référence au droit à la vie privée.

Source : https://citizenlab.ca/2015/09/international-code-of-conduct/

19 http://www.oas.org/juridico/english/cyber_faq_en.htm#1

20 Agreement among Governments of the SCO Member States on Cooperation in the Field of Ensuring International Information Security, 2009. Disponible sur : http://www.ccdcoe.org/sites/default/files/documents/SCO-090616-IISAgreementRussian.pdf

21 Organisation de coopération de Shanghai, Draft International Code of Conduct, Letter dated 9 January 2015 to the United Nations General Assembly, A/69/723. Disponible sur : https://ccdcoe.org/sites/default/files/documents/UN-150113-CodeOfConduct.pdf

Coopération économique Asie-Pacifique

La Coopération économique Asie-Pacifique (APEC) a publié, en 2002, une Stratégie de cybersécurité qui propose des recommandations dans les domaines suivants : législation sur la cybercriminalité ; lignes directrices techniques et en matière de sécurité ; sensibilisation de la population ; formation et éducation[22]. La Déclaration de Lima (2005) vise à renforcer les infrastructures d'information pour faire progresser la société de l'information[23]. Cette déclaration aborde également la sécurité des réseaux et souligne l'importance de la création d'équipes d'intervention d'urgence informatique (CERT). La Stratégie de l'APEC visant à créer un environnement en ligne fiable, sécurisé et durable a pour objectif d'assurer la sécurité des informations et des réseaux ; d'harmoniser les cadres de sécurisation des transactions et des communications et de lutter contre la cybercriminalité. Ces objectifs reposent de plus en plus sur une coopération étroite avec le secteur privé et avec d'autres organisations internationales. Le plan d'action stratégique TEL, adopté par l'APEC pour la période 2010 – 2015, vise à « promouvoir un environnement informatique sûr, résilient et fiable », notamment dans les domaines clés suivants : renforcement de la résilience des infrastructures nationales critiques ; sécurité et gestion des risques ; renforcement des capacités en matière de cybersécurité ; sensibilisation à la cybersécurité ; initiatives en matière de cybersécurité menées conjointement avec des entreprises privées ; activités visant à promouvoir des environnements en ligne sûrs et sécurisés pour les groupes vulnérables; ainsi que l'économie de l'internet[24].

L'OCS fait référence au concept de « sécurité internationale de l'information», en mettent l'accent sur le contenu en tant que source d'une menace potentielle pour la sécurité.

Association des Nations de l'Asie du Sud-Est

L'Association des nations de l'Asie du Sud-Est (ASEAN), composée de dix États membres (Brunei, Cambodge, Indonésie, Laos, Malaisie, Myanmar (Birmanie), Philippines, Singapour, Thaïlande et Viêt Nam), a publié une Déclaration des ministres des Affaires étrangères sur la coopération en matière de cybersécurité et a examiné les questions de cybersécurité dans le cadre de la lutte contre le terrorisme et de la criminalité transnationale[25].

Commonwealth

Le Commonwealth comprend 53 États membres et se focalise sur le renforcement des capacités, le partage d'informations et l'assistance à ses États membres pour la mise en œuvre de cadres juridiques de lutte contre la cybercriminalité. Le Commonwealth compte deux plates-formes travaillant sur ces questions : le Forum sur la cybersécurité et l'Initiative sur la cybersécurité, qui relèvent de l'Organisation des télécommunications du Commonwealth. Cette dernière a adopté le Commonwealth Cybergovernance

22 APEC, Cyber Security Strategy. Disponible sur : https://ccdcoe.org/sites/default/files/documents/APEC-020823-CyberSecurityStrategy.pdf

23 APEC, Déclaration de Lima, 2005. Disponible sur : https://ccdcoe.org/sites/default/files/documents/APEC-050603-LimaDeclaration.pdf

24 https://ccdcoe.org/apec.html

25 https://ccdcoe.org/sites/default/files/documents/ASEAN-120712-ARFStatementCS.pdf

Model[26], qui a été entériné par la déclaration d'Abuja en octobre 2013 et a été lancé lors du Forum sur la cybersécurité du Commonwealth à Londres en 2014[27].

Le Commonwealth Cybergovernance Model[28] propose un projet de principes, soumis à discussion, et visant à favoriser un cyberespace mondial sûr et efficace ; soutenir le développement économique et social ; agir individuellement et collectivement pour lutter contre la cybercriminalité ; exercer ses droits et assumer ses responsabilités dans le cyberespace.

Union européenne

Les documents les plus pertinents adoptés par l'Union européenne (UE) en matière de cybersécurité sont soit des documents juridiquement non contraignants (sous forme, par exemple, de communications), soit différents types d'actes juridiquement contraignants imposant des obligations à ses États membres ou à des entités spécifiques.

En 2013, l'Union européenne a publié son premier document exhaustif – sa stratégie de cybersécurité – qui traite d'un large éventail de cybermenaces. En 2016, l'UE a adopté la Directive sur la sécurité des réseaux et des systèmes d'information (Directive NIS)[29]. Cette stratégie décrit la vision, les rôles et les responsabilités de l'UE ainsi que les actions requises dans le domaine de la cybersécurité. Il est important de noter que le document souligne que la question de la cybersécurité ne doit pas être soumise au contrôle centralisé de l'UE mais doit relever des autorités étatiques nationales qui doivent être principalement chargées d'encadrer la prévention des cyberincidents et la lutte contre ces actes au niveau national.

L'un des objectifs de la stratégie de cybersécurité de l'UE est de développer des politiques et de renforcer les capacités en matière de cyberdéfense dans le cadre de la politique de sécurité et de défense commune. Ce document dresse également une liste des actions susceptibles d'être menées conjointement par l'Agence européenne de défense et les États membres.

Les actions liées à la cybersécurité ont également été intégrées à la stratégie numérique de l'UE. Celle-ci considère que la confiance et la sécurité de l'Internet constituent des éléments essentiels pour favoriser le dynamisme de la société numérique. Le Programme européen en matière de sécurité a notamment identifié la cybercriminalité comme l'une des menaces émergentes les plus graves.

Il est important de noter que la stratégie de cybersécurité de l'UE précise qu'un « cyberincident ou une cyberattaque particulièrement sérieux pourraient constituer un motif suffisant pour qu'un État membre invoque la clause de solidarité de l'UE » (article 222 du traité sur le fonctionnement de l'Union européenne).

26 Commonwealth Cybergovernance Model. Disponible sur : https://ccdcoe.org/sites/default/files/documents/CommW-140304-CommonwealthCybergovernanceModel.pdf

27 Commonwealth Cybersecurity Forum à Londres en 2014. Disponible sur https://ccdcoe.org/sites/default/files/documents/CommW-140304-CommonwealthCybergovernanceModel.pdf

28 https://ccdcoe.org/sites/default/files/documents/CommW-140304-CommonwealthCybergovernanceModel.pdf

29 Union européenne, Directive sur la sécurité des réseaux et des systèmes d'information (Directive NIS) L 194/1, 2016. Disponible sur: https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32016L1148.

Le règlement général de l'UE sur la protection des données (RGPD) est entré en vigueur le 25 mai 2015[30]. Cette réglementation modifie fondamentalement le mode de traitement des données dans tous les secteurs - du secteur de la santé au secteur bancaire à bien d'autres domaines. Il est important de noter que le RGPD ne s'applique pas seulement aux organisations au sein de l'UE, mais également aux organisations situées en dehors de l'UE si celles-ci fournissent des biens et des services à des citoyens de l'UE, ou si elles en surveillent le comportement.

Organisation du Traité de l'Atlantique Nord

En ce qui concerne la protection des données personnelles, seuls 16 pays africains sur 55 ont promulgué une législation exhaustive en matière de protection des données personnelles, à savoir : l'Afrique du Sud, l'Angola, le Bénin, le Burkina Faso, le Cap Vert, le Gabon, le Ghana, la Côte d'Ivoire, le Lesotho, Madagascar, le Mali, Maurice et Maroc, le Sénégal, les Seychelles et la Tunisie.

L'Organisation du Traité de l'Atlantique Nord (OTAN) a élaboré sa première politique de cyberdéfense en 2008. Lors du sommet de Lisbonne de 2010, la cyberdéfense a été intégrée dans le concept stratégique de l'OTAN, et la Déclaration du sommet a accéléré l'actualisation de la politique de cyberdéfense en 2011 et la création d'un plan d'action d'accompagnement en 2012.

Une nouvelle politique de cyberdéfense renforcée a été approuvée lors du sommet du pays de Galles et ce texte précise qu'« une attaque numérique majeure contre un État membre serait couverte par l'article 5 » [du Traité de l'Atlantique Nord][31] .

Cette politique vise également à améliorer le partage d'informations et l'assistance mutuelle entre les alliés ; approfondir la formation et intensifier les capacités de réaction dans ce domaine et renforcer la coopération avec les entreprises privées. Lors du sommet de Varsovie en 2016, l'OTAN a intégré le cyberespace dans son domaine d'opérations et s'est engagée à continuer à renforcer la coopération entre l'OTAN et l'UE en matière de cyberdéfense et à consacrer davantage de ressources aux capacités de cyberdéfense. En 2018, les ministres de la Défense des États membres de l'OTAN ont convenu de créer un nouveau centre d'opérations cybernétiques au sein du Grand Quartier général des Puissances alliées en Europe (SHAPE) afin de faciliter l'intégration des questions liées au cyberespace dans la planification et les opérations de l'OTAN à tous les niveaux.

Le RGPD s'applique à toute entreprise qui traite et détient des données à caractère personnel des personnes résidant dans l'UE, quel que soit le lieu où elle a son siège.

L'OTAN a créé un Comité de cyberdéfense (anciennement appelé Comité de la politique et des plans de défense - Cyberdéfense). Ce comité est un organe consultatif de haut niveau. Il propose des orientations aux États membres de l'OTAN et est chargé d'encadrer les capacités de cyberdéfense internes de l'OTAN. L'organisation dispose, en outre, d'un Comité de gestion de la cyberdéfense (CDMB) qui relève de la Division des défis de sécurité émergents au siège de l'OTAN et qui est composé de représentants de toutes les parties prenantes clés de la cybersécurité au sein de l'OTAN. Le CDMB assure notamment la planification stratégique et la direction exécutive des réseaux de l'OTAN et il est habilité à signer les protocoles d'accord avec les États membres afin de faciliter l'échange d'informations et de coordonner les actions d'assistance.

En outre, le Bureau des C3 (consultation, commandement et contrôle) de l'OTAN constitue le principal comité de consultation sur les aspects techniques et de mise en œuvre de la cyberdéfense.

30 Règlement général sur la protection des données. Disponible sur : https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=celex%3A32016R0679.

31 Traité de l'Atlantique nord, 1949. Disponible sur https://www.nato.int/cps/fr/natolive/official_texts_17120.htm

Le groupe des sept (G7)

Le G7 est un groupe informel de sept États (Allemagne, Canada, États-Unis d'Amérique, France, Italie, Japon et Royaume-Uni – l'UE ayant un statut d'observateur) qui se réunit régulièrement pour débattre sur des questions politiques et économiques importantes. Depuis 2016, le G7 a produit plusieurs documents sur la cybersécurité et celle-ci est devenue une thématique majeure parmi les sujets évoqués dans plusieurs déclarations de sommets[32].

ENCADRÉ : LIGNES DIRECTRICES SUR LA PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL POUR L'AFRIQUE

En mai 2018, l'Internet Society et la Commission de l'Union africaine ont lancé les Lignes directrices sur la protection des données à caractère personnel pour l'Afrique lors du sommet africain de l'Internet à Dakar, au Sénégal.

Ces lignes directrices formulent 18 recommandations axées sur trois questions :

1. Recommandations visant à créer la confiance, protéger la vie privée et assurer l'utilisation responsable des données à caractère personnel.
2. Recommandations d'action adressées aux autorités étatiques et décideurs, aux autorités de protection des données, aux contrôleurs de données et aux responsables du traitement des données.
3. Recommandations pour des solutions multi-acteurs afin d'assurer le bien-être du citoyen numérique et adopter des mesures d'habilitation et de soutien.

Source : https://www.internetsociety.org/fr/blog/2018/05/the-internet-society-and-african-union-commission-launch-personal-data-protections-guidelines-for-africa/

2. Initiatives lancées par des acteurs non étatiques

Du fait de la réticence des États à expliciter leur doctrine et leurs pratiques eu égard au cyberespace, il n'y a pas de consensus sur les modalités d'application du droit international au cyberespace. Cela a incité certains acteurs non étatiques à chercher à combler ce vide juridique. Les entreprises des TIC privées et les organisations de la société civile, en particulier, ont pris l'initiative de proposer des normes respectueuses des droits humains pour réguler le cyberespace et contribuer ainsi à l'instauration d'un Internet plus sûr, plus sécurisé et plus fiable.

Un groupe d'universitaires et d'experts du droit international humanitaire a rédigé le Manuel de Tallinn relatif à l'applicabilité du droit international aux cyberopérations[33]. Même s'il s'agit d'un travail universitaire, ce document réaffirme la nécessité d'appliquer au cyberespace les principes fondamentaux du droit international humanitaire, tels que le principe de distinction, de proportionnalité et de nécessité. En outre, ce groupe d'experts a publié le Manuel de Tallinn 2.0, qui traite du droit applicable en temps de paix au cyberespace[34].

32 Groupe du G7, Communiqué du sommet du G7 de Charlevoix. Disponible sur : https://www.consilium.europa.eu/fr/press/press-releases/2018/06/09/the-charlevoix-g7-summit-communique/

33 Manuel de Tallinn. Disponible sur https://ccdcoe.org/tallinn-manual.html

34 Manuel de Tallinn 2.0 Factsheet. Disponible sur https://ccdcoe.org/sites/default/files/documents/CCDCOE_Tallinn_Manual_One-pager_web.pdf

ÉTUDE DE CAS : LES NOTIONS D'« ATTAQUE ARMÉE» ET D'« UTILISATION DE LA FORCE » DANS LE CYBERESPACE – TROUVER UNE TERMINOLOGIE COMMUNE AUX COMMUNAUTÉS JURIDIQUE, POLITIQUE ET TECHNIQUE

Il est important de bien distinguer les différents régimes de droit international : (i) ius ad bellum (qui fixe les conditions dans lesquelles un État peut recourir à la force en tant qu'instrument de sa politique nationale), et (ii) ius in bello (qui établit les règles du droit international humanitaire (DIH) régissant la conduite des opérations armées dans le cadre d'un conflit).

Pour ce qui est du ius ad bellum, l'article 51 de la Charte des Nations Unies prévoit qu'une attaque armée peut justifier la légitime défense. Par conséquent, la question primordiale est de savoir à quel moment une cyber-opération constitue une attaque armée à laquelle un État peut légalement riposter en recourant à la force par des opérations cybernétiques ou cinétiques. Le terme important en l'occurrence est celui d'« attaque armée » ; en effet, la Cour internationale de Justice a statué, dans l'arrêt Nicaragua, qu'il existe des « mesures qui ne sont pas constitutives d'une attaque armée, mais peuvent néanmoins impliquer un recours à la force ».

Par conséquent, les États peuvent être confrontés à une cyber-opération qui constitue un recours à la force sans être toutefois légalement habilités à se défendre car ces cyber-opérations ne constituent pas une attaque armée. Afin de résoudre ce dilemme, un certain nombre de spécialistes du droit international préconisent d'interpréter la notion d'« attaque armée » dans le cyberespace comme englobant tout acte ayant des conséquences analogues à celles causées par des actions cinétiques (conséquences physiques).

En ce qui concerne le ius in bello, le DIH ne peut s'appliquer qu'en cas d'attaque, définie là aussi en référence aux conséquences de cet acte.

Microsoft, une entreprise transnationale privée, a proposé en février 2017 que les États adoptent une « Convention de Genève numérique » qui identifierait les normes applicables au cyberespace en temps de paix. Microsoft publie régulièrement des documents d'orientation et des articles de blog qui visent à renforcer le climat de confiance entre les différentes parties prenantes du cyberespace. Cependant, si les États se félicitent généralement des initiatives lancées par des acteurs non étatiques, beaucoup demeurent sceptiques quant au caractère réaliste de ces propositions[35].

Dans le même temps, les entreprises des TIC exhortent de plus en plus les États à prendre des mesures pour prohiber certains comportements malveillants dans le cyberespace. Microsoft a ainsi appelé le Congrès des États-Unis d'Amérique à adopter une réglementation limitant l'utilisation de la technologie de reconnaissance faciale[36].

35 Microsoft Policy Paper, A Digital Geneva Convention to protect cyberspace. Disponible sur : https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW67QH ; voir aussi Microsoft cyber security guidelines. Disponible sur : https://www.microsoft.com/en-us/cybersecurity/default.aspx

36 Natasha Singer, The New York Times (13 juillet 2018): Microsoft Urges Congress to Regulate Use of Facial Recognition. Dis-

D'autres instruments juridiques non contraignants, tels que les Principes de Manille sur la responsabilité des intermédiaires[37], ont également été élaborés et fournissent aux États des orientations sur les politiques régissant la responsabilité juridique des intermédiaires en matière de contenus publiés sur leurs plateformes. Les acteurs non étatiques, en particulier les entreprises des TIC et les organisations de la société civile, ont aussi proposé des normes applicables au cyberespace. Microsoft a joué un rôle de précurseur en la matière ces dernières années[38].

Les organisations de la société civile ont également lancé des initiatives pour combler le vide juridique laissé par les États dans le cyberespace, en proposant des normes visant à y promouvoir les droits humains. Par exemple, Article 19 (une organisation non gouvernementale (ONG) basée à Londres) a soutenu, avec plusieurs autres ONG, les Principes de Camden sur la liberté d'expression et l'égalité sur Internet[39]. Par ailleurs, des instruments juridiques non contraignants tels que les Principes de Manille sur la responsabilité des intermédiaires ont été adoptés.

La Global Network Initiative est une initiative multi-acteurs qui élabore des normes mondiales applicables à l'Internet. Ses Principes sur la liberté d'expression et la protection de la vie privée proposent des orientations et des conseils au secteur des TIC et à ses parties prenantes pour assurer la protection et la promotion du respect des droits humains dans le monde entier[40].

ENCADRÉ : RESPONSABILITÉ DES INTERMÉDIAIRES

Toutes les communications impliquant Internet sont facilitées par des intermédiaires. Compte tenu de la complexité d'Internet, il existe différents types d'intermédiaires :

- Les fournisseurs de services Internet (FSI) qui assurent un accès à l'Internet.
- Les fournisseurs d'hébergement Internet (« hôtes »), à savoir toute personne ou entreprise qui contrôle un site ou une page internet et permet à un tiers d'y poster et de télécharger des contenus.
- Les plateformes de médias sociaux telles que Facebook, Twitter, YouTube, etc., qui incitent les individus à se connecter et à interagir avec d'autres utilisateurs et à partager des contenus.
- Les moteurs de recherche, tels que Google, qui sont des logiciels utilisant des algorithmes pour récupérer des données, des fichiers ou des documents en réponse à une requête d'informations.

Les fournisseurs d'accès Internet, les réseaux sociaux et les moteurs de recherche sont donc des intermédiaires. La responsabilité des intermédiaires renvoie aux politiques qui régissent la responsabilité légale des intermédiaires eu égard au contenu de ces communications.
Source: https://www.manilaprinciples.org/fr et https://www.article19.org/data/files/Intermediaries_ENGLISH.pdf

Des entreprises de médias sociaux, à savoir Facebook, Twitter, YouTube et Microsoft, ont formé une coalition dans le cadre du forum de lutte contre le terrorisme[41] afin de prévenir les messages prônant l'extrémisme violent sur Internet. Dans le cadre de cette initiative, ces géants de l'internet élaborent des règles normatives visant à réglementer l'extrémisme violent sur leurs plates-formes respectives.

En règle générale, les entreprises des TIC privées doivent faire preuve - de manière proactive et inclusive - d'une diligence raisonnable en matière de droits humains, notamment en instaurant un réel dialogue avec les individus dont les droits humains sont susceptibles d'être affectés par leurs opérations.

Les Principes directeurs relatifs aux entreprises et aux droits de l'homme précisent qu'il incombe aux entreprises de respecter les droits humains. En ce qui concerne

ponible sur : https://www.nytimes.com/2018/07/13/technology/microsoft-facial-recognition.html

37 Principes de Manille sur la responsabilité des intermédiaires. Disponible sur : https://www.manilaprinciples.org/fr

38 Microsoft policy paper, A Digital Geneva Convention to protect cyberspace. Disponible sur : https://www.microsoft.com/en-us/cybersecurity/content-hub/a-digital-geneva-convention-to-protect-cyberspace

39 Article 19, The Camden Principles on Freedom of Expression and Equality. Disponible sur : https://www.article19.org/data/files/pdfs/standards/the-camden-principles-on-freedom-of-expression-and-equality.pdf

40 De plus amples informations sur la Global Network Initiative sont disponibles sur : https://globalnetworkinitiative.org/

41 Google public policy, Update on the Global Internet Forum to Counter Terrorism, 4 December 2017. Disponible sur : https://www.blog.google/around-the-globe/google-europe/update-global-internet-forum-counter-terrorism/

les entreprises du secteur des TIC, cela implique de prendre en compte des problèmes spécifiques à leur secteur, tels que la liberté d'expression, le droit à la vie privée et la sécurité. Il convient de noter que les défis les plus urgents à relever en matière de respect de l'obligation de diligence raisonnable incombant à ces entreprises sont liés aux conditions d'utilisation des produits, services, technologies et applications mis à la disposition des utilisateurs par les entreprises ainsi qu'aux actions des autorités étatiques visant à limiter les droits des utilisateurs.

Conclusions Clés

- Lorsque les cadres juridiques nationaux présentent des lacunes en matière de criminalisation des actes répréhensibles, cela crée des refuges pour les délinquants, ce qui peut affecter la situation d'autres pays du monde.
- Les différences en matière de criminalisation d'actes répréhensibles commis dans le cyberespace soulèvent des défis pour la coopération internationale en matière pénale, en particulier en ce qui concerne le principe de la double incrimination.
- Une analyse comparative des infractions en matière de cybercriminalité permet de dégager les bonnes pratiques que les États peuvent adopter pour élaborer une législation nationale respectueuse des normes internationales en vigueur.

Bibliographie

https://manypossibilities.net/african-undersea-cables/

https://socialsciences.exeter.ac.uk/media/universityofexeter/collegeofsocialsciencesandinternationalstudies/lawimages/research/Schmitt_-_Virtual_Disenfranchisement_ECIL_WP_2018-3.pdf

CHAPITRE 4
APPLICATION DES NORMES INTERNATIONALES ET RÉGIONALES AU PLAN NATIONAL

Objectifs

Ce chapitre examine la manière dont les cadres juridiques internationaux et régionaux, présentés dans le chapitre précédent, ainsi que d'autres normes relatives au cyberespace, peuvent être appliqués au niveau national, notamment par le biais de législations, de politiques et de stratégies de mise en œuvre.

Ce chapitre vise à améliorer la compréhension des questions suivantes :

- Les cadres et autres normes relatifs au cyberespace et leur applicabilité au contexte national.
- La nécessité d'adopter des législations, politiques et stratégies nationales relatives au cyberespace.
- Les modalités d'élaboration ou de modification des législations, des politiques et des stratégies nationales applicables au cyberespace, fondées sur les bonnes pratiques en matière de la GSS.

Introduction

Les individus, les autorités étatiques et les entreprises utilisent de manière sans cesse croissante le cyberespace, que cela soit à des fins de consommation d'informations, de prestation et de réception de services publics et privés, ou pour le maintien de processus opérationnels. Tous ces acteurs sont, de ce fait, davantage exposés au risque d'atteintes à leurs systèmes informatiques et de cyberattaques et cette vulnérabilité menace les droits humains ainsi que la sécurité nationale et humaine.

Aux niveaux international et régional, plusieurs normes ont été adoptées à la fois pour faire du cyberespace un espace plus sûr et pour établir un cadre général énonçant les obligations juridiques en matière de respect des droits humains qui doivent s'y appliquer. Dorénavant, c'est la nécessité d'adopter des approches cohérentes et exhaustives au niveau national qui est de plus en plus mise en avant comme une priorité pour relever les défis du cyberespace. Du fait de la dépendance croissante à l'égard du cyberespace, il est de plus en plus nécessaire d'adopter des législations, des politiques et des stratégies nationales efficaces pour protéger les données, les informations et les connaissances qui y sont transmises et utilisées et pour y renforcer la sécurité des citoyens.

Nous avons examiné dans le chapitre précédent les cadres internationaux ou régionaux - consistant en des résolutions, des rapports, des conventions et des accords relatifs aux droits humains - qui réglementent le cyberespace. Ces cadres ont créé un ensemble de normes que les États sont tenus de respecter lorsqu'ils modifient leurs législations, politiques et stratégies en matière de cyberespace et de cybersécurité et ils peuvent fournir des orientations aux autorités étatiques pour élaborer ou modifier leurs politiques et stratégies nationales en matière de cyberespace et de cybersécurité. Par ailleurs, des entreprises privées et des organisations non gouvernementales ont cherché à développer ces cadres et ces normes afin de mieux préciser les approches existantes en matière de cybersécurité. Les États peuvent s'appuyer sur ces diverses initiatives pour mettre en place une gouvernance globale du cyberespace et de la cybersécurité, fondée sur les principes de bonne gouvernance du secteur de la sécurité.

Les bonnes pratiques proposées dans le présent chapitre mettent en lumière les aspects réglementaires clés que les États devraient prendre en compte et renforcer lorsqu'ils élaborent ou modifient leur stratégie nationale de cybersécurité[1].

En outre, les politiques et stratégies nationales devraient inclure une dimension internationale ou être assorties de politiques et de stratégies traitant spécifiquement de la coopération internationale, afin d'éviter que l'impact de ces initiatives en matière de cyber-réglementation et de cybersécurité ne se cantonne aux frontières nationales.

Bonne pratique 1 : Les autorités étatiques devraient élaborer et adopter des législations, des politiques et des stratégies nationales pour réglementer le cyberespace.

Bien que le cyberespace soit un média mondial, en l'absence d'une autorité de gouvernance mondiale, ce sont les États qui ont l'obligation juridique de le réglementer et d'assurer sa bonne gouvernance[2]. Cela découle également du fait « les droits dont les personnes jouissent hors ligne doivent également être protégés en ligne[3] ». Ainsi, le fait de permettre aux entreprises des TIC d'opérer en dehors d'un cadre réglementaire adéquat peut déboucher sur des pratiques qui ne répondent pas à l'intérêt public et risque d'entraîner des atteintes aux droits humains[4]. Par conséquent, il incombe en premier lieu à l'État, en sa qualité de gardien de l'intérêt public, de faire respecter les obligations en matière de droits humains. L'État doit donc adopter des mesures législatives qui prennent en compte les avancées technologiques les plus récentes afin de limiter les conséquences potentiellement néfastes des actions du secteur privé. Pour assurer de bonnes pratiques en matière de gouvernance, il est par conséquent essentiel d'élaborer des législations, des politiques et des stratégies nationales et d'impliquer le secteur de la sécurité dans les actions visant à réglementer le cyberespace et assurer la cybersécurité.

Par ailleurs, les cadres et normes internationaux et régionaux sont de nature plutôt générale. Il est donc essentiel que la législation, les politiques et les stratégies nationales répondent aux besoins et aux spécificités en matière de cyberespace et de cybersécurité identifiés au niveau national.

De plus, les cadres et normes adoptés aux niveaux international et régional constituent un ensemble de principes pour la plupart juridiquement non contraignants ; ils ne permettent donc pas, à eux seuls, de protéger l'État contre des violations par des États tiers et leur respect par des acteurs privés et publics sur le territoire même de l'État n'est pas non plus garanti[5]. Enfin, l'adoption ou la modification de législations nationales relatives au cyberéspace et à la cybersecurité ainsi que la mise en place de politiques et de stratégies pour assurer la bonne gouvernance du cyberespace et de la cybersécurité peuvent constituer un moyen plus exhaustif et plus cohérent de garantir le respect de la loi et des droits humains dans le cyberespace au sein de l'État concerné.

Toute législation relative à la cybercriminalité doit être élaborée en tenant compte des exigences suivantes :

- Elle doit être suffisamment neutre (sur le plan technologique) pour pouvoir tenir compte de l'évolution constante de la technologie et des formes de criminalité et éviter ainsi le risque d'être obsolète dès son entrée en vigueur.

- Les autorités chargées de l'application de la loi doivent être tenues de respecter

2 UIT, Guide pour l'élaboration d'une stratégie nationale de cybersécurité, p. 26.

3 Assemblée générale des Nations Unies, Conseil des droits de l'homme, La promotion, la protection et l'exercice des droits de l'homme sur l'Internet, Doc. ONU, A/HRC/20/L.13, 29 juin 2012, para. 1.

4 Mihr, Anja. "Good Cyber Governance: The Human Rights and Multi-Stakeholder Approach." Georgetown Journal of International Affairs, (2014): 34, (http://www.jstor.org/stable/43773646).

5 Wolfgang Ischinger, "Foreword" in International Cybersecurity Norms: Reducing Conflict in an Internet-dependent World, Microsoft (2014), 1.

certaines mesures de protection afin de veiller à l'application du principe de l'État de droit et des obligations en matière de droits humains.

- La législation doit être suffisamment harmonisée ou au moins compatible avec les lois d'autres pays pour permettre une coopération internationale et répondre, par exemple, aux critères de double incrimination.

EXEMPLES DE BONNES PRATIQUES

Il est essentiel d'adopter des législations et des politiques nationales en matière de cybercriminalité. Les États africains qui élaborent une législation en la matière peuvent s'inspirer, notamment, de la Convention de l'Union africaine sur la cybersécurité et la protection des données à caractère personnel, adoptée à Malabo en juin 2014[6].

Depuis 1997, l'Algérie s'est progressivement donné les moyens de lutter contre la cybercriminalité. Elle a ainsi adopté une législation qui vise essentiellement à lutter contre la criminalité tout en respectant de nombreux principes fondamentaux ; cependant, la réalisation de ces deux objectifs demeure confrontée à certains défis. La législation algérienne inclut la plupart des dispositions de la Convention de Budapest adoptée par le Conseil de l'Europe, en utilisant parfois une terminologie différente. Elle inclut les infractions suivantes : accès frauduleux et rétention dans un système ; interception de communications et de paroles échangées en privé ou de manière confidentielle ; suppression ou modification des données contenues dans le système suite à un accès frauduleux ou à une rétention ; modification du fonctionnement d'un système à la suite d'un accès frauduleux ou d'une rétention ; abus de dispositif ; pornographie infantile ; et infractions liées à des atteintes à la propriété intellectuelle et à des droits connexes.

Source : (https://www.coe.int/en/web/octopus/)

Bonne pratique 2 : Les autorités étatiques devraient actualiser leur législation nationale pour prendre en compte l'évolution constante des défis soulevés par le cyberespace

Lorsqu'ils élaborent et adoptent une législation nationale relative au cyberespace et à la cybersécurité (que ce soit en actualisant la législation en vigueur ou en en créant une nouvelle), les législateurs et les décideurs politiques doivent prendre en compte l'évolution constante des défis soulevés par le cyberespace.

Tout d'abord, le rythme des avancées technologiques dans le cyberespace est beaucoup plus rapide que le processus législatif. Par conséquent, même les lois les plus modernes en la matière peuvent - et risquent probablement - d'être dépassées par les développements technologiques les plus récents. Deuxièmement, la législation relative au cyberespace requiert des connaissances et une expertise informatiques considérables dont le secteur public ne dispose que rarement car ce type d'expertise est bien mieux rémunéré dans la sphère privée. Troisièmement, même si un État parvient

à adopter des lois réglementant de manière appropriée le cyberespace, l'application de cette législation se révèle complexe - et parfois impossible - en raison du caractère transnational des questions traitées.

La rapidité des innovations technologiques contraste radicalement avec la lenteur et la durée parfois très longue des processus législatifs nationaux[7]. C'est la raison pour laquelle un grand nombre de technologies et d'outils informatiques sont utilisés sans être réglementés de manière adéquate. Le recours à l'intelligence artificielle (IA) offre un exemple emblématique de ce vide réglementaire. Alors que les États dans leur grande majorité ne sont pas parvenus à adopter une législation réglementant de manière adéquate les contenus hébergés par des entreprises de médias sociaux qui font appel à des individus chargés de modérer ces contenus, des outils reposant sur l'intelligence artificielle ont déjà été déployés pour effectuer cette tâche[8].

Les États doivent néanmoins éviter de légiférer de manière précipitée et sans coordination. La rapidité des progrès technologiques suscite certes des inquiétudes au sein de la population, ce qui peut inciter les décideurs politiques à adopter une législation afin de démontrer la compétence et la réactivité des institutions étatiques. Cependant, le fait d'adopter une série de lois dans la précipitation peut avoir un effet plus dommageable que de laisser temporairement les entreprises privées opérer sans réglementation exhaustive tant que les nouvelles technologies sont encore en phase d'essai. Les États devraient ainsi prévoir une période d'observation des nouvelles technologies, identifier les nouvelles tendances et ne décider de légiférer qu'à l'issue d'un processus d'examen minutieux incluant toutes les parties prenantes, y compris les acteurs du secteur privé et de la société civile.

En outre, lorsqu'ils élaborent une législation en la matière, les États devraient éviter d'avoir une approche trop prescriptive car cela pourrait entraver le processus d'innovation et de recherche et décourager les petites entreprises des TIC qui pourraient ne pas être en mesure de respecter les normes élevées d'une législation excessivement normative. Cela étant dit, lorsqu'ils doivent décider de l'opportunité de légiférer - ou non - sur une question spécifique relative au cyberespace, les États doivent envisager d'autres options que la législation. Ainsi, par exemple, l'adoption de codes de conduite volontaires ou d'un ensemble de principes directeurs non contraignants peut permettre d'atteindre l'objectif réglementaire souhaité. En outre, ces instruments juridiques non contraignants sont plus faciles à modifier et donc plus à même de prendre en compte les développements technologiques les plus récents.

7 Cour des comptes européenne, Défis à relever pour une politique de l'UE efficace dans le domaine de la cybersécurité. Document d'information, mars 2019 (https://www.eca.europa.eu/lists/ecadocuments/brp_cybersecurity/brp_cybersecurity_fr.pdf.).

8 Assemblée générale des Nations Unies, Rapport du Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression, A/73/348, 29 août 2018, para. 18.

EXEMPLES DE BONNES PRATIQUES

Le Ghana dispose d'une réglementation spécifique pour les établissements bancaires financiers - qui constituent le secteur le plus touché par la cybercriminalité. Les autorités étatiques ont ainsi adopté, en 2008, une Directive sur la cybersécurité à l'intention des institutions financières de la Banque du Ghana. Cette directive fait obligation à la direction et au conseil d'administration de ces institutions de s'impliquer activement dans des initiatives visant à renforcer la cybersécurité. Toutes les banques du pays sont tenues de nommer un Responsable sécurité des systèmes d'information (RSSI) chargé d'orienter la direction et le conseil d'administration de ces institutions sur les questions de cybersécurité et de proposer également des mesures appropriées pour gérer les risques liés à la sécurité de l'information et aux cyber-risques.

(Source: https://www.bog.gov.gh/privatecontent/Public_Notices/CYBER%20AND%20INFORMATION%20SECURITY%20DIRECTIVE.pdf)

De nombreux États africains ont renforcé leurs dispositifs en matière de cybersécurité. En Afrique du Sud, la loi sur la protection des informations personnelles (POPI), adoptée en 2013, a créé un organe chargé de la régulation de l'information (Régulateur d'informations) afin de garantir la confidentialité des données. En 2017, cet organe de régulation a ouvert une enquête sur la fuite de données la plus importante cette année-là dans le pays, au cours de laquelle les données personnelles de 30 millions d'individus ont été volées. Cet organe a également demandé aux entreprises concernées de fournir des explications sur ces faits.

(Source : http://www.justice.gov.za/inforeg/)

Bonne pratique 3 : Les autorités étatiques devraient renforcer leur expertise en matière de cyberespace.

Le secteur public manque d'expertise et de connaissances informatiques et cela constitue un autre obstacle important pour l'adoption d'une législation nationale adéquate sur les questions liées au cyberespace[9]. Pour résoudre ce problème, il faut absolument que les États renforcent leur expertise en la matière. Cet objectif peut être atteint de nombreuses façons, la plus simple étant que l'État recrute un nombre suffisant de personnels possédant une expertise en informatique. Cependant, les États ont généralement des ressources financières et autres beaucoup plus limitées que les entreprises des TIC privées et peuvent éprouver des difficultés à attirer et à retenir des experts sur des questions pointues telles que la cybersécurité, l'intelligence artificielle ou l'analyse de données.

Ce problème peut être en partie résolu en recourant à des dispositifs alternatifs de réglementation, de façon à bénéficier de l'expertise du secteur privé. L'État peut ainsi décider d'impliquer dans une certaine mesure le secteur privé dans le processus de réglementation tout en conservant cependant la responsabilité générale de cette question. Dans la mesure où les entreprises privées possèdent une expertise de pointe

9 Raymond, Mark. "Managing Decentralized Cyber Governance: The Responsibility to Troubleshoot." Strategic Studies Quarterly10, no. 4 (2016) : 137, (http://www.jstor.org/stable/26271532).

et disposent du savoir-faire nécessaire sur les questions relatives au cyberespace, cette coopération avec le secteur privé peut permettre de combler le fossé traditionnel entre avancées technologiques et processus législatif. En outre, ces modalités de co-réglementation peuvent se révéler beaucoup moins politisées que les processus législatifs habituels.

EXEMPLES DE BONNES PRATIQUES

Dans certains pays, l'expertise informatique au niveau national a pu être renforcée en coordination avec le secteur privé et des multinationales étrangères[10].

Au Kenya, dans le cadre d'initiatives menées par le secteur privé en matière de cybersécurité, une société panafricaine de consultants en entreprises et en cybersécurité appelée Serianu a créé, en mars 2018, à Nairobi, un Cyber Immersion Centre. Ce Centre fournit aux entreprises un environnement leur permettant d'expérimenter et de tester leurs capacités en matière de cybersécurité. Il met également à disposition des modules d'enseignement pour former des professionnels de la cybersécurité. Un centre similaire a été ouvert à Maurice mi-2017.

(Source : https://www.serianu.com/acic.html)

Au Nigéria, Microsoft s'est associé à Paradigm Initiative Nigeria (PIN) pour sensibiliser la population à la cybercriminalité et créer des opportunités économiques. La Commission nigériane contre les délits économiques et financiers (EFCC) a annoncé, en octobre 2009, avoir fermé environ 800 sites internet impliqués dans des cas de cybercriminalité et arrêté 18 gangs de cybercriminalité. L'EFCC a précisé que son action avait pu s'appuyer sur des « technologies intelligentes » fournies par Microsoft.

(Source : https://paradigmhq.org/about/)

Bonne pratique 4 : Les autorités étatiques devraient élaborer et actualiser les lois protégeant le droit à la vie privée et les données à caractère personnel.

La protection du droit à la vie privée et des données à caractère personnel est une dimension essentielle de la cybersécurité et des avancées concrètes ont été réalisées pour assurer cette protection, en particulier au sein de l'Union européenne (UE). Le règlement général de l'UE sur la protection des données (RGPD - voir le chapitre 3), entré en vigueur en mai 2018, a créé un cadre réglementaire régional visant à assurer à tous les individus le contrôle de leurs données personnelles. Ce règlement a également engendré un certain nombre de lois sur la protection des données et le respect de la vie privée au niveau national.

En 2014, l'Union africaine a adopté la Convention de Malabo sur la cybersécurité et la protection des données à caractère personnel (voir chapitre 3). Cette convention n'est pas encore entrée en vigueur. La Convention de Budapest est donc actuellement le seul cadre

10 Nir Kshetri (2019) Cybercrime and Cybersecurity in Africa, Journal of Global Information Technology Management, 22:2, 77-81, DOI: 10.1080/1097198X.2019.1603527

international juridiquement contraignant réglementant la cybersécurité, le cyberespace et le rôle de l'État en la matière. Bien que seuls quelques États africains l'aient signée ou aient été invités à y adhérer, la Convention de Budapest a servi de cadre directeur pour l'élaboration de la Convention de l'Union africaine sur la cybersécurité.

EXEMPLES DE BONNES PRATIQUES

Au Kenya, un nouveau projet de loi sur la protection des données a été soumis pour examen au Parlement en novembre 2018. Ce projet de loi intègre de nombreux éléments du règlement général de l'UE sur la protection des données (RGPD). Le projet de loi fait ainsi obligation aux organisations concernées d'informer les utilisateurs des raisons pour lesquelles leurs données sont collectées et utilisées et de préciser la durée pendant laquelle celles-ci seront stockées. Le projet de loi comprend également une disposition qui donne aux consommateurs le droit de demander à ces organisations de supprimer leurs données. En outre, ces organisations ne sont autorisées à stocker des données que si elles respectent un certain nombre de normes de sécurité.

(Source : http://www.ict.go.ke/wp-content/uploads/2016/04/Kenya-Data-Protection-Bill-2018-14-08-2018.pdf)

La France a promulgué, en juin 2018, la loi relative à la protection des données personnelles afin de mettre la législation nationale française en conformité avec le règlement général de l'UE sur la protection des données. Prenant appui sur la loi française relative à la protection des données de janvier 1978, la loi de 2018 étend le mandat de protection des données confié à la Commission nationale de l'informatique et des libertés (CNIL) en la dotant des pouvoirs suivants :

• Son autorité réglementaire a été renforcée afin de faire appliquer les réglementations de sécurité ainsi que les codes de conduite et d'élaborer des documents de référence et des recommandations. En outre, la CNIL est habilitée à agréer des organismes de certification et à certifier la conformité des produits, des personnes et des procédures aux dispositions du RGPD et de la législation française.

• Ses pouvoirs de contrôle ont été renforcés, ce qui habilite les agents de la CNIL à accéder à tout document non protégé par le secret professionnel. De plus, les agents de la CNIL peuvent recourir à de nouveaux types de sanctions et le montant des amendes administratives a été fortement augmenté. Une entreprise qui ne protégerait pas ses données personnelles pourrait devoir verser des amendes susceptibles d'aller de 10 ou 2% de son chiffre d'affaires mondial, jusqu'à 20 millions ou 4% de son chiffre d'affaires mondial (le montant le plus élevé étant choisi) pour les plus graves infractions.

(Source : https://www.francecompetences.fr/Protection-des-donnees-personnelles.html)

Bonne pratique 5 : Les autorités étatiques devraient élaborer et actualiser les lois protégeant les infrastructures critiques.

Les infrastructures critiques jouent un rôle essentiel pour assurer le bien-être de la population. Ces infrastructures regroupent les biens, les systèmes et les réseaux (physiques et virtuels) essentiels pour assurer des fonctions sociales vitales, notamment la santé, la sécurité et le bien-être économique et social - et dont la perturbation ou la destruction aurait un impact négatif substantiel pour la population.

Voici des exemples d'infrastructures critiques :

- Centrales électriques
- Approvisionnement en eau et en nourriture
- Sécurité publique : forces de sécurité, organisations de secours, défense civile
- Santé publique : hôpitaux et soins médicaux, laboratoires
- Administration publique
- Transports (par exemple, transport routier, ferroviaire et aérien)
- Élimination des déchets (déchets et eaux usées)
- Services financiers (p. e. banques, sociétés d'assurance)
- Réseaux de technologies de l'information et de la communication

Une proportion importante des infrastructures critiques opère en s'appuyant sur de nouvelles technologies. Si cette modernisation a contribué à optimiser l'efficacité de la prestation de biens et de services publics à la population, elle expose également ces infrastructures à des vulnérabilités qui peuvent potentiellement avoir des effets dévastateurs pour les populations locales.

Les États ont le devoir de protéger, à l'intérieur de leurs frontières, les infrastructures critiques contre les cyberattaques. Cette protection doit constituer une priorité des stratégies nationales de cybersécurité. À cette fin, les États doivent élaborer et mettre en œuvre des mesures de cyberdéfense afin de protéger les points vulnérables au sein des systèmes d'information des infrastructures critiques. Ces mesures doivent permettre de détecter les cyberattaques, se défendre contre elles et les neutraliser.

EXEMPLES DE BONNES PRATIQUES

En mars 2019, le Parlement sud-africain a adopté une législation sur les infrastructures critiques qui vise notamment à : permettre l'identification et la qualification de certaines installations en tant qu'infrastructures critiques ; élaborer des lignes directrices et définir les facteurs à prendre en compte pour garantir l'identification et la qualification en toute transparence de certaines installations en tant qu'infrastructures critiques ; et prévoir des mesures pour assurer la protection, la préservation et la résilience de ces infrastructures critiques. La loi a également mis en place un Conseil chargé des infrastructures critiques ; donné au ministre de la Police le pouvoir discrétionnaire de qualifier certaines installations en tant qu'infrastructures critiques et ; prescrit la manière dont celles-ci doivent être protégées dans l'intérêt de la sécurité nationale.

(Source : http://www.policesecretariat.gov.za/downloads/bills/CIP_Bill_for_Publication.pdf)

Conclusions Clés

- Les cadres internationaux et régionaux proposent un ensemble de normes pour l'élaboration, l'adoption et la révision de la législation, des politiques et des stratégies relatives à la cybersécurité.
- Il incombe en premier lieu aux autorités étatiques d'assurer la bonne gouvernance en matière de cybersécurité.
- Les autorités étatiques devraient élaborer, adopter et mettre à jour les législations, politiques et stratégies nationales pour réglementer le cyberespace et répondre à des nouveaux défis, notamment en ce qui concerne la protection de la vie privée et des données personnelles, et la protection des infrastructures critiques.
- Le renforcement de l'expertise sur le cyberespace, par l'éducation et le partage de connaissances favorisés notamment par les partenariats publics-privés (PPP), est essentiel pour assurer la bonne gouvernance en matière de cybersécurité.

Bibliographie

The Rule of Law Checklist. Commission de Venise du Conseil de l'Europe, 2016.

Cybersecurity Policy Framework. A Practical guide to the development of national cybersecurity policy. Microsoft (2018).

International Cybersecurity Norms: Reducing Conflict in an Internet-dependent World, Microsoft (2014).

Commission de l'Union africaine et Symantec, Cyber crime and cyber security trends in Africa Report (2017) https://www.thegfce.com/documents/publications/2017/03/10/report-cyber-trends-in-africa

CHAPITRE 5
STRATEGIES NATIONALES DE CYBERSECURITE

Objectifs

Ce chapitre fournit un aperçu général des stratégies nationales de cybersécurité (SNCS). Il présente, en particulier, les éléments clés d'une SNCS et propose des exemples de bonnes pratiques en la matière.

Ce chapitre vise à améliorer la compréhension des questions suivantes :

- Les stratégies nationales de cybersécurité en général.
- Les éléments clés d'une stratégie nationale de cybersécurité.
- Les ressources disponibles pour aider les législateurs et les décideurs politiques au niveau national à élaborer des stratégies nationales de cybersécurité.

Introduction

La création du cyberespace a fourni de nouvelles opportunités de développement économique, technologique et social. Cependant, dans le même temps, les menaces transnationales - telles que le cyberespionnage pour le compte d'États, les cyberactivités à caractère militaire, la cybercriminalité, le cyberterrorisme et l'utilisation d'Internet à des fins de terrorisme – n'ont cessé de croître. Ces risques sécuritaires sont liés au cyberéspace ou favorisés par lui et ils doivent être pris en compte de manière adéquate dans le cadre de stratégies et de plans d'action exhaustifs. Dans le cas contraire, les États peuvent se retrouver dans l'incapacité d'assurer la sécurité nationale et humaine et de maintenir la croissance économique.

Pour faire face à un environnement du cyberespace marqué par des menaces en constante évolution, les États de toutes les régions du monde ont élaboré et adapté des stratégies, soit en adoptant de nouvelles politiques, soit en modifiant les politiques de sécurité en vigueur. Les stratégies de sécurité nationale, qui se focalisent sur l'environnement des cybermenaces, sont appelées stratégies nationales de cybersécurité (SNCS).

Les SNCS peuvent prendre différentes formes et, selon la cyberpréparation de l'État concerné, elles sont plus ou moins exhaustives. Étant donné que ce type de stratégies nationales doit être adapté au contexte, il n'est pas possible de proposer un modèle unique pour l'élaboration d'une SNCS efficace. On peut néanmoins identifier un ensemble de priorités stratégiques qui se retrouvent dans la majorité des SNCS. Ces priorités incluent la mise en place de cadres réglementaires, la protection des infrastructures critiques, la coopération internationale et la collaboration entre acteurs publics et privés, ainsi qu'un investissement en matière de recherche et de développement.

Il n'existe pas de définition communément acceptée des SNCS. L'Union internationale des télécommunications (UIT) propose la définition suivante :

- Une expression de la vision, des objectifs de haut niveau, des principes et des priorités qui guident un pays dans la lutte contre les cybermenaces.

- Une vue d'ensemble des parties prenantes chargées d'améliorer la cybersécurité du pays, de leurs rôles et responsabilités respectifs.

- Une description des étapes, programmes et initiatives qu'un pays s'emploiera à suivre pour protéger sa cyber-infrastructure nationale et, par là même, accroître sa sécurité et sa résilience[1].

La portée et les stratégies des SNCS ont dû être adaptées à l'évolution rapide des cybermenaces. Alors que les stratégies de sécurité portaient auparavant sur la seule protection des individus et des organisations considérés comme des acteurs distincts, elles traitent dorénavant de la protection de la société dans son ensemble.

De manière générale, une SNCS poursuit deux objectifs interdépendants :

- 1. Renforcer la cybersécurité dans l'économie de l'Internet afin de favoriser la prospérité économique et sociale.
- 2. Protéger les sociétés cyber-dépendantes des cyber-menaces.

La cybersécurité constitue un défi complexe dont les multiples dimensions relèvent aussi bien de la gouvernance et de politiques, que de questions opérationnelles, techniques et juridiques. Les politiques nationales fixent en général les modalités à mettre en œuvre pour atteindre les objectifs définis comme des priorités nationales.

Bonne pratique 1 : La stratégie nationale de cybersécurité devrait être intégrée dans la politique de sécurité nationale.

Les SNCS doivent être envisagées comme l'un des outils à disposition des États pour réaliser leurs priorités nationales stratégiques. Par conséquent, il est important que les autorités étatiques intègrent la SNCS dans leur stratégie nationale de sécurité. Cela contribue, en outre, à une approche globale de la sécurité nationale.

Le fait d'intégrer la cybersécurité dans la stratégie de sécurité nationale souligne leurs relations réciproques et démontre que l'État prend acte de l'importance de la cybersécurité pour toutes les dimensions de la sécurité nationale.

EXEMPLES DE BONNES PRATIQUES

En Suède, la stratégie nationale de cybersécurité précise que cette stratégie est « fondée sur les objectifs de la sécurité suédoise : protéger la vie et la santé de la population, le fonctionnement de la société et notre capacité [de la Suède] à défendre des valeurs essentielles telles que la démocratie, l'État de droit ainsi que les droits et libertés fondamentales ».

(Source : https://www.government.se/4ac8ff/contentassets/d87287e088834d9e8c08f28d0b9dda5b/a-national-cyber-security-strategy-skr.-201617213)

Dans le cadre de la mise en œuvre de sa stratégie nationale de cybersécurité, la Finlande applique les principes et procédures établis dans sa stratégie de sécurité pour la société.

(Source : https://www.defmin.fi/files/2378/Finland_s_Cyber_Security_Strategy.pdf)

Pour élaborer une SNCS exhaustive, il est important de traduire la vision et les objectifs nationaux en actions concrètes qui permettront, en définitive, de réaliser les buts et les objectifs qui ont été définis.

L'UIT a schématisé le cycle de vie d'une SNCS afin d'orienter la réflexion stratégique des acteurs chargés de l'élaboration de ce type de stratégies au niveau national (voir ci-dessous) :

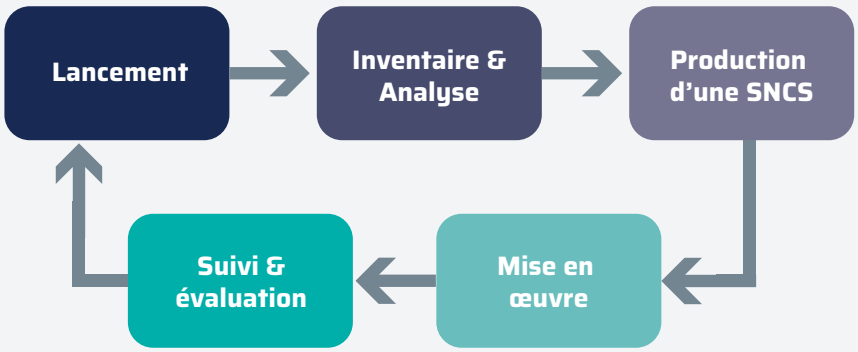


Schéma 1 : Cycle de vie du SNCS proposé par le Guide de l'UIT pour l'élaboration d'une stratégie nationale de cybersécurité

Avant d'élaborer une SNCS, il est essentiel que les autorités étatiques identifient les objectifs et le but visés par cette stratégie et qu'ils définissent clairement leur vision de la cybersécurité.

ÉTUDE DE CAS : MISSION D'ASSISTANCE TECHNIQUE DE L'OEA AU MEXIQUE

En 2017, l'Organisation des États américains (OEA) a mis en place - dans le cadre de son programme de cybersécurité et à la demande des autorités étatiques mexicaines - une commission d'experts internationaux chargée de : partager avec les entités mexicaines les bonnes pratiques en la matière et améliorer la compréhension de la situation actuelle de la cybersécurité au Mexique ; identifier le niveau actuel de cyber-maturité et ; promouvoir l'élaboration d'un cadre national de cybersécurité.

La commission d'experts internationaux était composée de représentants d'autres États, du secteur privé, d'organisations internationales, d'experts techniques et de membres de la société civile.

(Source : http://www.oas.org/en/media_center/press_release.asp?sCodigo=E-049/17 and http://www.oas.org/documents/eng/press/Recommendations-for-the-Development-of-the-National-Cybersecurity-Strategy.pdf)

Bonne pratique 2 : L'élaboration de la stratégie nationale de cybersécurité devrait être pilotée par une autorité chargée du processus et impliquer un large éventail de parties prenantes.

Avant de lancer le processus d'élaboration de la SNCS, il faut tout d'abord identifier un acteur qui sera chargé de piloter ce processus. Cet acteur peut être une entité préexistante ou une agence créée à cette fin. Cet acteur doit être chargé de coordonner le processus de manière neutre. Il doit également identifier les parties prenantes clés qui devraient être impliquées dans l'élaboration de la SNCS et assurer des échanges continus avec les parties prenantes afin de veiller à ce que les connaissances et l'expertise nécessaires soient mobilisées lors du processus d'élaboration de la SNCS.

ÉTUDE DE CAS : COMITÉ INTERMINISTÉRIEL CHILIEN

Au Chili, un comité interministériel composé de représentants du ministère de l'Intérieur et de la Sécurité publique et du ministère de la Défense nationale a piloté le processus d'élaboration de la stratégie nationale de cybersécurité.

Ce comité interministériel a organisé et coordonné les sessions des groupes de travail chargés d'examiner les thèmes relevant de la stratégie nationale de cybersécurité. Les différents thèmes examinés par ces groupes de travail étaient les suivants : infrastructure de l'information ; prévention et sanctions ; éducation et sensibilisation ; coopération et relations internationales ; institutionnalisation. Les membres permanents de ces groupes de travail étaient les sous-secrétariats des ministères de l'Intérieur, de la Défense, de la Justice, de l'Économie, des Télécommunications ainsi que du Secrétariat général de la présidence et de l'Agence nationale de renseignements.

(Source : http://www.ciberseguridad.gob.cl/media/2015/12/Documento-Bases-Pol%C3%ADtica-Nacional-sobre-Ciberseguridad.pdf)

En outre, cet acteur devrait également être chargé de définir clairement les rôles et les responsabilités de ces parties prenantes clés.

Il est évident que le secteur privé joue un rôle essentiel pour garantir la cybersécurité. Cependant, la coopération entre les secteurs publics et privés n'est toujours pas institutionnalisée.

La coopération entre acteurs publics et privés est également déterminante pour assurer la protection des infrastructures nationales critiques, car la plupart de celles-ci sont détenues et exploitées par des entités privées. Ces dernières devraient donc être activement impliquées dans la planification de la protection de ces infrastructures contre les cybermenaces.

Il est essentiel d'impliquer le plus grand nombre possible de parties prenantes dans le processus d'élaboration de la SNCS afin d'assurer l'appropriation de la stratégie par ces acteurs. Cette appropriation joue un rôle essentiel pour assurer la mise en œuvre effective de la stratégie. En outre, l'implication de toutes les parties prenantes concernées permet au processus de pouvoir bénéficier de la meilleure expertise possible et assure donc son efficacité.

EXEMPLES DE BONNES PRATIQUES

Afin d'optimiser le processus d'élaboration de sa SNCS, le Royaume-Uni a créé sur son site internet un processus de consultation ouvert à tous et permettant à chacun de faire part de ses commentaires sur ce projet de stratégie.

Source : https://www.gov.uk/government/consultations/developing-the-uk-cyber-security-profession

Le gouvernement canadien a lancé un processus de consultation publique en ligne visant à recueillir les points de vue de la population en général ainsi que du secteur privé, du monde universitaire et d'autres parties prenantes concernées sur l'environnement de la cybersécurité au Canada. Un rapport présentant les conclusions de ce processus de consultation a ensuite été publié en ligne.

Source : https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2017-cybr-rvw-cnsltns-rprt/index-en.aspx

La stratégie de cybersécurité du Royaume-Uni précise que l'objectif d'un Internet sûr ne peut être atteint qu'en assurant la coopération de tous les acteurs concernés : le secteur privé, les particuliers et les autorités étatiques. De même que nous bénéficions tous de l'utilisation du cyberespace, il nous incombe à tous de contribuer à le protéger.

La coopération entre le secteur public et le secteur privé est le plus souvent institutionnalisée sous la forme de partenariats publics-privés, mais ces derniers continuent à être confrontés à certains défis qui ont trait, en particulier, à la définition du mandat de ces partenariats, au manque de clarté concernant les rôles et les responsabilités de chacun, à la méfiance entre les parties prenantes, aux obstacles au partage d'informations, au manque d'incitation à travailler ensemble et à des procédures de contrôle déficientes, ce qui entrave la mise en œuvre d'une responsabilité effective.

ÉTUDE DE CAS : IDENTIFIER LES PARTIES PRENANTES PERTINENTES

Il n'est pas forcément nécessaire d'impliquer l'ensemble des parties prenantes dans tous les débats, mais il est important d'identifier celles qui sont directement concernées par une question et dont l'expertise peut enrichir ces réflexions.

Vous trouverez ci-dessous une liste des parties prenantes susceptibles d'être impliquées dans l'élaboration de la SNCS. Cette liste n'est pas exhaustive mais elle fournit un bon aperçu des acteurs concernés.

- **Autorités étatiques :** Ministères concernés (TIC, Économie, Communications,

etc.), organes de réglementation, pouvoir judiciaire et agences chargées de l'application de la loi, services de défense et de sécurité.

- **Secteur privé :** Entreprises de TIC, entreprises de sécurité de l'information, association d'entreprises.
- **Société civile :** Associations travaillant sur des questions spécifiques (telles que la défense des droits humains ou la protection en ligne des enfants), groupes fondés sur l'identité (confession religieuse, minorités, droits de la femme), réseaux d'organisations de la société civile.
- **Universitaires :** Universités, entités de recherche, groupes de réflexion, chercheurs indépendants.
- **Communauté technique :** Équipes d'intervention en cas d'urgence informatique, équipes d'intervention en cas d'incident informatique, organisations chargées de la standardisation des systèmes de noms de domaine.
- **OI :** Organisations régionales et internationales (telles que l'UA, l'OSCE, l'OEA, le Conseil de l'Europe), institutions internationales (par exemple, la Banque mondiale, l'UIT).

Source : https://www.gp-digital.org/wp-content/uploads/2018/06/Multistakeholder-Approaches-to-National-Cybersecurity-Strategy-Development.pdf

Bonne pratique 3 : Le processus d'élaboration de la stratégie nationale de cybersécurité devrait reposer sur un inventaire exhaustif des forces et des faiblesses d'un pays en matière de cybersécurité.

La phase suivante du processus d'élaboration de la SNCS consiste à procéder à une évaluation et à une analyse de l'environnement de la cybersécurité au niveau national afin d'identifier les forces et les faiblesses du pays en la matière. Dans le cadre de cet inventaire et de ce travail d'analyse, il est important de cartographier et d'examiner le cadre réglementaire national (y compris les lois, réglementations, politiques et programmes liés à la cybersécurité) ; les infrastructures nationales critiques et les partenariats publics-privés ; ainsi que les capacités techniques et institutionnelles dont dispose le pays pour prévenir les cyber-risques (telles que la mise en place d'équipes d'intervention en cas d'urgence informatique) et pour se protéger contre les cybermenaces (telles que la désignation de responsables de la protection des données).

Ce processus d'inventaire et d'analyse vise à évaluer le niveau de cyber-maturité afin de veiller à ce que la SNCS réponde aux besoins réels du pays.

ÉTUDE DE CAS : MODÈLE D'ÉVALUATION DE LA CYBER-MATURITÉ, MINISTÈRE DES COMMUNICATIONS DU GHANA

Afin d'examiner ses capacités en matière de cybersécurité, le Ghana a mis au point un modèle d'évaluation de son niveau de cyber-maturité en prenant en compte cinq dimensions :

- Politique et stratégie de cybersécurité
- Cyber culture et société
- Éducation, formation et compétences en matière de cybersécurité
- Cadres juridiques et réglementaires
- Normes, organisations et technologies.

Cette évaluation visait à aider les autorités étatiques ghanéennes à mieux comprendre les forces et les faiblesses du pays en matière de cybersécurité afin d'investir plus efficacement dans le renforcement de ses capacités.

Source : https://moc.gov.gh/cybersecurity-capacity-maturity-model-assessment-held

Les enseignements tirés de cette évaluation permettent d'orienter le processus d'élaboration de la SNCS. Celle-ci devrait être pilotée par un acteur spécifiquement dédié à cette tâche en s'appuyant sur une mobilisation de l'ensemble des parties prenantes clés. Dans l'idéal, des groupes de travail devraient être chargés de certaines dimensions spécifiques de la SNCS en fonction de leur expertise. Par ailleurs, il est considéré comme une bonne pratique de soumettre, avant son adoption, le projet de SNCS à l'examen d'un large éventail de parties prenantes sous la forme de consultations en ligne ou dans le cadre d'ateliers de travail. Cela contribue à faire en sorte que la SNCS reflète une vision commune des enjeux de la cybersécurité.

Le Parlement ou le pouvoir exécutif doivent ensuite entériner la SNCS, selon le processus en vigueur dans le pays. Une fois adoptée, la SNCS doit être publiée dans le journal officiel ou sur le site internet d'un ministère, afin de permettre à la population de prendre connaissance de son existence et de son contenu, de se familiariser avec les priorités des autorités étatiques en matière de cybersécurité, et de contribuer activement à la réalisation des priorités stratégiques identifiées.

Il n'existe pas d'approche unique pour encadrer le processus d'élaboration de la SNCS. Les bonnes pratiques varient en fonction de la portée de cette stratégie, du nombre de parties prenantes impliquées et des formalités techniques en vigueur.

Au Chili, au Kenya et au Mexique, la version préliminaire de la SNCS a également été publiée en ligne pour permettre aux différentes parties prenantes de formuler des commentaires et favoriser l'appropriation du processus.

Bonne pratique 4 : La SNCS devrait inclure les priorités stratégiques suivantes : renforcement de la coordination gouvernementale aux niveaux politique et opérationnel, consolidation de la coopération entre acteurs publics et privés, renforcement de la coopération internationale et respect des droits fondamentaux.

La majorité des SNCS soulignent l'importance du rôle joué par la coopération internationale pour promouvoir la cybersécurité et mettent l'accent sur la nécessité de renforcer les alliances et les partenariats avec des pays partageant la même vision en matière de cybersécurité, notamment pour favoriser le renforcement des capacités. Par ailleurs, la plupart des SNCS reconnaissent que le respect des droits fondamentaux, en particulier le droit à la vie privée et les libertés d'expression et d'opinion, ainsi que la libre circulation de l'information jouent un rôle essentiel pour favoriser la sécurité du cyberespace.

En outre, la majorité des SNCS identifient la prévention de la cybercriminalité comme un objectif prioritaire.

EXEMPLES DE BONNES PRATIQUES

Au Canada, la stratégie nationale de cybersécurité reflète les valeurs du pays telles que le respect des principes relatifs à l'État de droit, à la responsabilité et au droit à la vie privée.

(Source : https://www.enisa.europa.eu/topics/national-cyber-security-strategies/SNCS-map/strategies/canadas-cyber-security-strategy)

Au Malawi, la stratégie nationale en matière de technologies de l'information et de la communication affirme l'engagement continu des autorités étatiques à prendre des mesures pour assurer un environnement propice à l'implication des secteurs publics et privés dans le développement, le déploiement et l'utilisation des TIC dans les communautés urbaines et rurales.

(Source : http://www.malawi.gov.mw/Publications/Malawi_2013_Malawi_ICT_Policy.pdf)

Bonne pratique 5 : Identifier les infrastructures nationales critiques qui devraient être prises en compte dans la SNCS.

Il est fondamental d'identifier les infrastructures nationales critiques afin d'élaborer des politiques permettant de les protéger contre les cyber-menaces. Sans une définition claire et une liste de ce type d'infrastructures, il est difficile d'assurer leur sécurité contre les cyber-risques.

Le fonctionnement d'un nombre croissant d'infrastructures critiques repose sur les technologies de l'information et de la communication. Il est dès lors vital d'assurer la protection de ces infrastructures contre les cybermenaces car cela peut avoir des effets dans la vie réelle. Par conséquent, dans de nombreux États, les stratégies nationales de cybersécurité considèrent la protection de ces infrastructures comme une priorité.

Un nombre croissant d'États ont donc procédé à l'identification de leurs infrastructures nationales critiques et la majorité d'entre eux y ont inclus les infrastructures liées à l'eau et l'électricité et les hôpitaux.

La « directive 2008/114/EC du Conseil de l'Union européenne du 8 décembre 2008 concernant le recensement et la désignation des infrastructures critiques européennes ainsi que l'évaluation de la nécessité d'améliorer leur protection » constitue un document important à cet égard. Cette directive européenne définit les infrastructures critiques comme « un point, système ou partie de celui-ci, situé dans les États membres, qui est indispensable au maintien des fonctions vitales de la société, de la santé, de la sûreté, de la sécurité et du bien-être économique ou social des citoyens, et dont l'arrêt ou la destruction aurait un impact significatif dans un État membre du fait de la défaillance de ces fonctions ».

EXEMPLES DE BONNES PRATIQUES

L'article 17 du projet de loi relatif à la protection des infrastructures critiques en Afrique du Sud énumère les facteurs à prendre en compte pour qualifier une installation d'infrastructure critique. Ces facteurs sont par exemple : le secteur dans lequel cette infrastructure exerce ses principales fonctions ; son importance stratégique, notamment l'impact potentiel de la destruction, de la perturbation, de la défaillance ou de la dégradation de cette infrastructure ou de l'interruption d'un service susceptible de porter atteinte à la capacité des autorités étatiques de fonctionner, de fournir des services publics de base, ou de maintenir l'ordre public ; la catégorie de risque que représente cette infrastructure ; les ressources dont dispose l'acteur chargé de gérer cette infrastructure ; les effets - ou le risque - d'une destruction, d'une perturbation, d'une défaillance ou d'une dégradation de ce type d'infrastructures ; la taille et l'emplacement de toute population à risque ; les cas de destruction survenus dans le passé ; le niveau de risque ou de menaces auquel cette infrastructure est exposée ; les caractéristiques ou les attributs spécifiques de cette infrastructure ; dans quelle mesure la qualification d'une installation en tant qu'infrastructure critique sert l'intérêt général ; et tout autre facteur identifié par le ministre.

Source : https://www.parliament.gov.za/storage/app/media/Docs/bill/8e3d69b4-509f-4108-b6ec-d0f44bb8632c.pdf

La stratégie de l'Allemagne relative aux infrastructures nationales critiques, adoptée en 2009, définit les infrastructures critiques comme « des structures et des installations organisationnelles et physiques d'une importance vitale pour la société et l'économie d'un pays si bien que leur défaillance ou leur dégradation entraînerait des pénuries d'approvisionnement, une perturbation significative de la sécurité publique, ou d'autres conséquences dramatiques ».

Source:https://www.bmi.bund.de/SharedDocs/downloads/EN/publikationen/2009/kritis_englisch.pdf?__blob=publicationFile&v=1

La France a défini les infrastructures critiques comme « des établissements, ouvrages ou installations qui fournissent les services et les biens indispensables à la vie de la Nation ». Ce sont les opérateurs eux-mêmes qui proposent la liste de leurs infrastructures critiques qui peuvent être, par exemple, des sites de production, des centres de contrôle, des nœuds de réseau, des centres informatiques, etc.

Source : http://www.sgdsn.gouv.fr/uploads/2016/10/plaquette-saiv.pdf

La Suisse a décidé que les secteurs suivants relevaient des infrastructures critiques : les services gouvernementaux, l'énergie, l'élimination des déchets, les finances, la santé, l'eau et l'alimentation, l'information et la communication, les transports, la sécurité publique.

Source : https://www.babs.admin.ch/fr/aufgabenbabs/ski.html

Bonne pratique 6 : La stratégie nationale de cybersécurité devrait prévoir un plan de mise en œuvre, y compris en matière de R & D.

L'efficacité de la SNCS repose sur sa mise en œuvre effective. Pour cela, il faut qu'elle s'appuie sur un plan de mise en œuvre (parfois appelé plan d'action) qui permet de transformer la stratégie en actions et en politiques concrètes, en coordonnant les actions et les ressources mobilisées.

Il est essentiel que ce plan de mise en œuvre soit assorti d'indicateurs clés permettant d'assurer le suivi et l'évaluation des résultats atteints par la SNCS. Le processus de suivi permet aux autorités étatiques de s'assurer que la SNCS est mise en œuvre conformément à son plan d'action. La phase d'évaluation permet de vérifier que la mise en œuvre de la SNCS reflète effectivement les objectifs et les priorités fixés ou s'il est nécessaire de réajuster ces derniers[2].

Le plan de mise en œuvre devrait, en outre, inclure la mise en place d'un mécanisme de signalement des incidents et prévoir des modalités pour sensibiliser la population aux cyber-risques et aux cybermenaces. Le signalement des incidents de sécurité informatique joue un rôle essentiel pour renforcer la cybersécurité au niveau national. Le signalement des incidents permet d'actualiser et d'adapter la liste des mesures de cybersécurité à prendre, en fonction de l'évolution de l'environnement des menaces. Le signalement des incidents repose sur la coopération entre les secteurs publics et privés. Par conséquent, il est essentiel d'instaurer un climat de confiance afin de favoriser le partage d'informations sur les cyber-risques et les cybermenaces. La mise en place d'une équipe d'intervention en cas d'incident informatique (CIRT) est considérée comme primordiale pour assurer la gestion efficace des incidents.

Pour garantir l'efficacité du plan de mise en œuvre, il est nécessaire de sensibiliser les individus en tant qu'utilisateurs aux menaces et aux vulnérabilités liées à la cybersécurité. Il est essentiel de veiller à ce que chaque utilisateur sache comment se

protéger contre les cyber-risques susceptibles d'affecter la cybersécurité au niveau national.

Il est également important d'encourager la recherche et le développement (R & D) et d'y investir des ressources pour élaborer de nouveaux outils permettant de parer à tous les types de cybermenaces, pour s'en protéger, les détecter et s'y adapter.

EXEMPLES DE BONNES PRATIQUES

La SNCS du Kenya poursuit l'objectif suivant : « Le gouvernement du Kenya s'engage à assurer la sécurité, la sûreté et la prospérité de notre nation et de ses partenaires. Nous considérons la cybersécurité comme un élément clé de cet engagement et prenons des mesures à cet effet afin de renforcer la confiance des organisations et des individus dans les transactions en ligne et sur mobile, pour encourager les investissements étrangers et proposer un plus large éventail d'opportunités commerciales sur le marché mondial. La mise en œuvre réussie de la stratégie permettra également au Kenya d'atteindre ses objectifs économiques et sociaux grâce à un environnement en ligne sécurisé permettant aux individus, aux entreprises et à ses partenaires étrangers de mener des activités commerciales » (p. 4).

La stratégie nationale du Nigéria en matière de cybersécurité identifie les utilisateurs individuels comme étant le maillon faible de la chaîne de cybersécurité. Par conséquent, la stratégie prévoit « des initiatives et des mesures afin de contribuer à protéger les utilisateurs d'Internet, et à fournir des matériels et des outils permettant de protéger les citoyens nigérians contre les cyber-menaces et les actes malveillants ».

(Source : Nigeria, National Cyber Security Strategy, Chapitre 11)

La politique nationale du Malawi en matière de TIC est assortie d'une stratégie de mise en œuvre, de suivi et d'évaluation détaillée ; par ailleurs, la mise en œuvre de la politique en matière de TIC fait également l'objet d'un suivi et d'une évaluation de son efficacité et de sa réactivité une fois par an ou chaque fois que cela s'avère nécessaire. (Source : Malawi, National ICT Policy, 2013, p 11)

La stratégie nationale de cybersécurité de la Mauritanie inclut un plan de mise en œuvre détaillé de cette politique. (Source : Mauritanie, Stratégie nationale de modernisation de l'administration et des TIC, 2012- 2016)

En Pologne, la stratégie nationale de cybersécurité identifie comme prioritaire la nécessité de mieux sensibiliser les utilisateurs aux méthodes et aux mesures de sécurité dans le cyberespace. (Pologne, Stratégie nationale de cybersécurité, 2013)

La Tunisie, l'Afrique du Sud et le Kenya ont mis en place des équipes d'intervention en cas d'urgence informatique (CERT).

Bonne pratique 7 : La mise en œuvre de la SNCS devrait être assortie de campagnes de sensibilisation du grand public sur la cybersécurité dotées des moyens nécessaires.

Toute personne connectée à Internet est exposée à des cybermenaces – qu'il s'agisse d'un acteur étatique, du propriétaire d'une entreprise, d'acteurs du secteur financier et commercial, du grand public ou d'enfants.

De manière générale, il est communément admis que la cyber-sécurité n'incombe pas à une seule agence, une seule entité ou un seul individu, mais constitue une responsabilité partagée de toutes les personnes qui sont connectées à Internet ou utilisent ses applications.

L'Organisation des États américains (OEA) précise que « la cybercriminalité regroupe un large éventail de techniques et de comportements différents - notamment le vol d'identité, l'exploitation des enfants, le cyber-harcèlement, les menaces internes, le phishing et le spear phishing et bien d'autres - qui doivent être combattues[3] ».

Étant donné que tout individu peut être affecté par différents types de cybercriminalité, il est primordial d'informer le public sur ces cyber-risques et cybermenaces.

ÉTUDE DE CAS : BOÎTE À OUTILS DE L'OEA POUR UNE CAMPAGNE DE SENSIBILISATION À LA CYBERSÉCURITÉ - ANALYSE DE LA SITUATION

Afin d'élaborer des campagnes de sensibilisation efficaces, il est essentiel de bien comprendre le contexte et l'environnement des cybermenaces.

À cet égard, l'OEA a élaboré des questions permettant d'orienter l'analyse de la situation :

- Comment votre pays est-il connecté à Internet ?
- Où et comment la population se connecte-t-elle à Internet?
- Qui est connecté ?
- Avec quels types d'appareils ?
- Quels sont les types de systèmes d'exploitation et de canaux de communication utilisés ?
- Pour quels types de produits et services ?
- À quelles fins les entreprises utilisent-elles Internet ?
- Quelle est la taille de ces entreprises (p.e. entreprises individuelles, coopératives agricoles, petites et moyennes entreprises, industries légères, etc.) ?
- Quels sont les cyber-risques auxquels votre pays est confronté ?

- À quels types de cybercriminalité les consommateurs sont-ils confrontés ?
- À quels types de cybercriminalité vos entreprises sont-elles confrontées ?
- Ces cybercrimes peuvent-ils être classés en différentes catégories ?
- Quels risques encourent vos infrastructures essentielles ?
- Y a-t-il eu des cas de vols de données majeurs – à l'encontre d'acteurs étatiques ou d'entreprises - dans un passé récent ?
- Y a-t-il des risques futurs d'infractions majeures ?
- Quelles sont les pertes économiques effectives ou potentielles en cas de cybermenaces ?

Source : OAS, Cybersecurity Awareness Campaign Toolkit 2016. Disponible sur : https://www.thegfce.com/initiatives/g/global-campaign-to-raise-cybersecurity-awareness/documents/publications/2015/10/01/cybersecurity-awareness-campaign-toolkit

Pour être efficace, une campagne de sensibilisation doit transmettre des messages faciles à comprendre et cibler des destinataires spécifiques ; elle doit être planifiée et élaborée dans le cadre d'un processus multi-acteurs associant des représentants des autorités étatiques, des entreprises privées (telles que des fournisseurs de services internet, des entreprises de télécommunications) ainsi que des représentants de la société civile (tels que les organisations non gouvernementales, les médias et les universités).

EXEMPLES DE BONNES PRATIQUES

En 2015, la Jordanie a adopté une loi sur la lutte contre la cybercriminalité et a créé une unité spécialisée appelée « unité de lutte contre la cybercriminalité ». Cette unité a produit, avec le soutien de l'Office des Nations Unies contre la drogue et le crime, une vidéo de sensibilisation aux risques, aux types et aux conséquences juridiques de la cybercriminalité.

Source : https://www.unodc.org/middleeastandnorthafrica/en/web-stories/jordan_-releasing-a-video-on-cyber-security-awareness-raising.html

L'initiative StaySafeOnline, créée par la National Cyber Security Alliance, vise à promouvoir une culture de la cybersécurité. À cette fin, elle a publié sur son site internet une infographie expliquant comment s'assurer que tous les membres du foyer, y compris les enfants et les adultes plus âgés, utilisent Internet de manière sûre et responsable.

Source : https://staysafeonline.org/wp-content/uploads/2018/09/NCSAM-2018-Week1.pdf

Conclusions Clés

- Afin de faire face aux menaces actuelles et émergentes en matière de cybersécurité, les États doivent évaluer et adapter en permanence leurs stratégies nationales de cybersécurité en fonction de l'évolution de l'environnement des menaces.
- Pour assurer la mise en œuvre efficace de la stratégie nationale de cybersécurité, il est essentiel de définir des objectifs spécifiques et des priorités stratégiques.
- Les stratégies de cybersécurité devraient reconnaître que le respect des droits fondamentaux, tels que le droit à la vie privée et les libertés d'expression et de croyance, ainsi que la libre circulation de l'information, constituent des éléments essentiels pour promouvoir un cyberespace libre et ouvert.
- La cybersécurité est un problème qui relève de plusieurs secteurs et de différentes responsabilités au sein des organes publics. Par conséquent, la mise en œuvre efficace de la stratégie nationale de cybersécurité doit reposer sur une coopération étroite entre les différentes autorités étatiques ainsi qu'avec le secteur privé.
- Afin d'élaborer des outils innovants pour parer aux nouveaux types de cybermenaces, pour s'en protéger, les détecter et s'y adapter, les autorités étatiques doivent investir davantage de ressources dans la recherche et le développement.
- Afin de protéger les infrastructures nationales critiques contre les cybermenaces, il est important de commencer par définir ce qu'est une « infrastructure nationale critique » dans un contexte donné.

Bibliographie

UIT, Guide pour l'élaboration d'une stratégie nationale de cybersécurité, 2018. Disponible sur : https://www.itu.int/en/ITU-D/Cybersecurity/Documents/NCS%20Guide_f.pdf

https://www.enisa.europa.eu/publications/SNCS-good-practice-guide

Microsoft, Developing a National Strategy for Cybersecurity: Foundations for Security, Growth and Innovation. Disponible sur : https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/REVoNi

Global Partners Digital: Multistakeholder Approaches to National Cybersecurity Strategy Development, juin 2018. Disponible sur : https://www.gp-digital.org/wp-content/uploads/2018/06/Multistakeholder-Approaches-to-National-Cybersecurity-Strategy-Development.pdf

Organization for American States, Cybersecurity Awareness Campaign Toolkit, 2016. Disponible sur : https://www.thegfce.com/initiatives/g/global-campaign-to-raise-cybersecurity-awareness/documents/publications/2015/10/01/cybersecurity-awareness-campaign-toolkit

CHAPITRE 6

FAVORISER UNE COOPÉRATION EFFICACE ENTRE LE SECTEUR PUBLIC ET LE SECTEUR PRIVÉ DANS LE CYBERESPACE

Objectifs

Ce chapitre présente un aperçu des avantages et des défis liés aux partenariats public-privé dans le cyberespace, en particulier en ce qui concerne les partenariats entre les agences chargées de l'application de la loi et les entreprises privées dans le cadre d'enquêtes sur des infractions pénales et sur des contenus illégaux diffusés sur Internet.

Ce chapitre vise à améliorer la compréhension des questions suivantes :

- Les concepts d'initiatives multi-acteurs et de partenariats public-privé.
- La coopération entre les agences chargées de l'application de la loi et les entreprises privées.
- Les dimensions à prendre en compte pour favoriser des approches multi-acteurs efficaces en matière de cybersécurité.

Introduction

La cybersécurité a une dimension transversale. De ce fait, toutes les stratégies nationales de cybersécurité (SNSC) ont en commun de chercher à favoriser la collaboration entre les acteurs privés et publics impliqués dans le cyberespace afin de renforcer la cybersécurité. Les approches multi-acteurs en matière de cyberespace et de cybersécurité - également appelées partenariats public-privé (PPP) - jouent un rôle de plus en plus essentiel pour assurer la gouvernance de la cybersécurité, à la fois en raison du rôle considérable joué par les entreprises privées et du fait de la nature transnationale du cyberespace. L'application des normes internationales au cyberespace tout comme la mise en œuvre effective des SNSC dépendent en grande partie de la collaboration efficace entre toutes les parties prenantes – y compris les autorités étatiques, le secteur des TIC, le monde universitaire et la société civile.

Le recours de plus en plus important à des dispositifs publics, privés-publics et privés pour assurer la cybersécurité est symptomatique d'une transformation radicale des relations internationales. La coopération entre de multiples parties prenantes - États, entreprises et société civile - peut en ce sens être considérée comme une réponse pragmatique pour s'adapter à cette nouvelle donne et combler certains vides de gouvernance que les approches réglementaires traditionnelles ne sont plus en mesure de traiter. En effet, ces initiatives visent à renforcer l'efficacité de la gouvernance en veillant à ce que les acteurs commerciaux opèrent dans le respect de l'État de droit et des droits humains. Des groupes composés de diverses parties prenantes peuvent élaborer conjointement des approches et trouver des solutions plus adéquates que celles qui résulteraient d'actions isolées.

1. Comprendre les partenariats public-privé

Vue d'ensemble

Les partenariats public-privé impliquent la mise en commun des ressources (biens, compétences, expertise et financement), des risques et des avantages entre diverses parties prenantes. Dans le domaine de la cybersécurité, les PPP impliquent une collaboration entre, d'une part, les autorités étatiques et les institutions publiques et, d'autre part, les entreprises des TIC, le monde universitaire et la société civile, l'objectif étant de sensibiliser aux questions de cybersécurité, d'en atténuer les risques et de renforcer les capacités nationales en matière de cybersécurité. Cette coopération couvre des dimensions multiples, et peut notamment viser au renforcement des capacités de cyberdéfense et au partage d'informations. Les PPP peuvent également

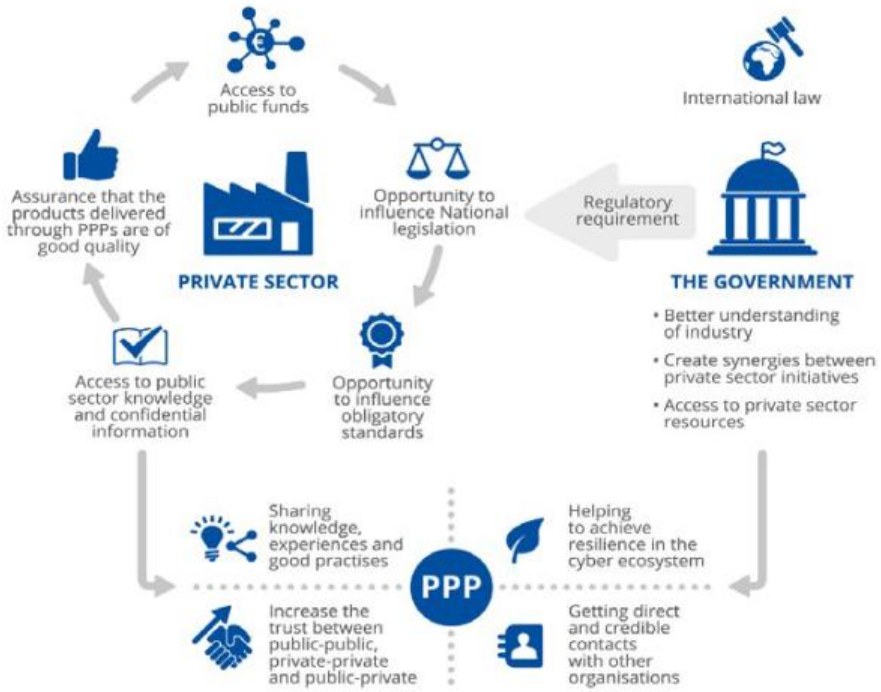
être justifiés par des intérêts économiques, des besoins en matière de règlementation et des relations publiques. Dans les pays en développement, les PPP en matière de cybersécurité visent principalement à améliorer la sensibilisation à la cybersécurité ou à renforcer les capacités nationales en matière de cybersécurité.

Les PPP peuvent renforcer la cybersécurité à de nombreux égards. Ces partenariats peuvent en effet :

- Contribuer à sensibiliser à la cybersécurité et à améliorer la compréhension des questions qu'elle soulève au sein des diverses organisations impliquées et dans la société en général ;
- Renforcer les cyber-compétences au niveau national grâce au lancement d'initiatives conçues pour identifier des personnes susceptibles de devenir des professionnels de la cybersécurité, les inciter à s'impliquer dans ce domaine et leur faire acquérir les compétences requises ;
- Doter les professionnels de la cybersécurité des ressources financières et techniques nécessaires, par le biais d'initiatives spécifiques ;
- Renforcer la recherche et le développement dans le domaine de la cybersécurité ;
- Améliorer la prévention de la criminalité et des actions frauduleuses ;
- Contribuer à la certification et à l'accréditation en matière de cybersécurité ;
- Établir et favoriser la collaboration entre les entités publiques et privées travaillant sur les questions de cybersécurité.

Les PPP en matière de cybersécurité peuvent être classés selon les quatre catégories suivantes :

- Les PPP institutionnels : créés aux termes d'un acte juridique lié à la protection des infrastructures critiques. Ce type de partenariat opère le plus souvent sous la forme de groupes de travail, de groupes d'intervention rapide et de communautés à long terme.
- Les PPP poursuivant des objectifs spécifiques : créés pour instaurer une culture de la cybersécurité par le biais d'une plate-forme ou d'une entité centrale réunissant les secteurs privé et public dans le but de favoriser l'échange de connaissances et de bonnes pratiques. Ce type de partenariats porte sur une thématique ou un objectif spécifique.
- Les services de cybersécurité externalisés : ces services sont mis en place lorsque les autorités étatiques ne sont pas en mesure de répondre efficacement aux besoins du secteur privé qu'ils ont identifiés. Les PPP agissent en tant qu'acteur tiers autonome, mais répondent spécifiquement aux besoins des



Raisons d'être des partenariats public-privé

Source : Public-Private Partnerships in Cyberspace, ENISA, novembre 2017, p. 14

entreprises et soutiennent les autorités étatiques pour l'élaboration ou la mise en œuvre des politiques.

- Les PPP hybrides : Ce type de PPP mobilise des équipes d'intervention d'urgence informatique (CERT). Les autorités étatiques confient à ces PPP la tâche de fournir à l'administration publique ou à l'ensemble du pays des services qui sont assurés par des CERT.

2. Rôles des autorités étatiques et des autres parties prenantes

Les institutions publiques doivent jouer un rôle clé dans les collaborations multi-acteurs

La responsabilité d'élaborer des SNSC efficaces incombe en premier lieu aux autorités étatiques. Les législateurs et les décideurs politiques sont donc tenus de créer des cadres adéquats qui respectent les obligations de l'État aux termes du droit international et national. Les autorités étatiques collaborent avec des acteurs privés tels que les entreprises des TIC pour veiller à ce que les processus de co-régulation et d'autorégulation respectent le droit international des droits humains et le droit national.

Au-delà de cette approche purement légaliste, les autorités étatiques peuvent jouer un rôle important de coordination et nouer des liens avec le secteur des TIC et la société civile en créant et en soutenant des plates-formes collaboratives. Celles-ci peuvent se révéler particulièrement utiles dans le cadre de l'action menée par les unités nationales de signalement des contenus sur internet. Ces unités recherchent et signalent les contenus en ligne suspects ; puis elles demandent leur suppression en les renvoyant à cet effet aux entreprises des TIC concernées. Les plates-formes collaboratives peuvent fournir des informations précieuses aux autorités étatiques et favoriser un processus de prise de décision plus inclusif. Des canaux de communication ouverts entre les parties prenantes concernées peuvent également permettre d'identifier et de combler les lacunes sur des questions critiques de cybersécurité et désamorcer les conflits d'intérêts potentiels. Les efforts institutionnalisés et coordonnés peuvent aussi inciter les différentes parties prenantes à mener d'autres actions dans ce domaine en aidant à canaliser les ressources humaines et financières nécessaires à cette fin.

ÉTUDE DE CAS : ÉQUIPES D'INTERVENTION D'URGENCE INFORMATIQUE

Les Équipes d'intervention d'urgence informatique (CERT) sont des unités d'experts qui ont pour mandat de porter assistance aux individus ou aux institutions qui sont l'objet de cyberattaques. Ces équipes sont principalement chargées d'identifier les logiciels malveillants hostiles et de prévenir leur propagation dans le réseau tout en atténuant les conséquences de l'attaque. Ces équipes travaillent souvent au sein d'entreprises privées ou d'institutions publiques, mais elles peuvent également être dotées, au niveau national, d'un statut d'agences gouvernementales spécifiquement chargées d'offrir leur assistance à un large éventail d'entités privées et publiques.

Bien que les CERT nationaux soient des agences publiques, ils constituent un bon exemple de coopération entre le secteur public et le secteur privé. Chaque CERT est avant tout chargé de recueillir des informations sur les cyber-vulnérabilités identifiées et de partager les mises à jour et les correctifs logiciels appropriés. La plupart des CERT nationaux ont mis en place un formulaire public en ligne qui permet de les informer de cyber-risques ou d'incidents informatiques. En outre, certains CERT nationaux disposent d'équipes mobiles qui peuvent se déplacer, le cas échéant, pour porter assistance à une institution qui est la cible d'une cyberattaque.

La coopération entre les secteurs privés et publics joue un rôle essentiel pour maintenir un cyber-environnement stable et sécurisé. Les institutions publiques ne peuvent pas assurer, à elles seules, la cybersécurité pour deux raisons principales. Premièrement, le secteur privé contrôle l'essentiel du cyberespace et il joue un rôle moteur pour stimuler l'innovation dans ce domaine. Deuxièmement, même les infrastructures cybernétiques essentielles détenues ou contrôlées par l'État dépendent en grande partie des produits et des services fournis par des entreprises privées pour assurer leur protection.

En outre, les autorités étatiques sont tenues de respecter et de protéger les droits humains de leurs citoyens en ligne et doivent donc veiller à ce que les actions des entreprises privées et des CERT nationaux respectent les droits humains, en particulier le droit à la vie privée et à la liberté d'expression. Il faut pour cela que les CERT agissent en toute indépendance, sans interférence politique, et qu'ils ne soient pas un outil au service de l'État pour porter atteinte aux systèmes informatiques et à la confidentialité des réseaux et des communications.

Lorsqu'elles créent des CERT nationaux, les autorités étatiques doivent tenir compte des trois aspects de la dimension humaine de la cybersécurité : confidentialité, accessibilité et intégrité. Cela signifie que l'objectif fondamental de la cybersécurité n'est pas la sécurisation des réseaux, mais le renforcement de la sécurité humaine. Le droit à la vie privée doit ainsi être l'un des principes directeurs des opérations visant à protéger et à renforcer la confidentialité des données. De même, pour garantir l'accessibilité des données, il est essentiel d'assurer le respect et la protection de la liberté d'expression et d'information.

Source : https://www.africacert.org/african-csirts/

ÉTUDE DE CAS : UNITÉS DE SIGNALEMENT DES CONTENUS SUR INTERNET AU NIVEAU DE L'UE ET AU NIVEAU NATIONAL

L'unité de signalement des contenus sur Internet (IRU) de l'Union européenne (EU) relève du Centre européen de lutte contre le terrorisme d'EUROPOL et comprend une équipe d'experts du terrorisme à caractère religieux ainsi que des spécialistes multi-lingues, des développeurs de technologies de l'information et de la communication, et des agences chargées de l'application de la loi spécialisées dans la lutte antiterroriste[1]. Cette unité a commencé ses travaux en 2015 et a reçu le mandat suivant :

- Soutenir les autorités européennes compétentes en fournissant des analyses stratégiques et opérationnelles ;
- Signaler les contenus en ligne terroristes et extrémistes violents et partager ces informations avec les parties prenantes concernées ;
- Détecter et demander la suppression des contenus diffusés sur Internet par les réseaux de passeurs pour attirer des migrants et des refugiés ;
- Procéder sans délai au renvoi de ces contenus vers les entreprises concernées et coopérer étroitement avec elles afin de les supprimer[2].

Le rapport sur la transparence, publié en 2017, par l'UE IRU indique que « la coopération avec le secteur privé joue un rôle fondamental en matière de prévention[3] ». Depuis sa création en juillet 2015 jusqu'en décembre 2017, l'IRU de l'UE a évalué 46 392 éléments à contenu terroriste qui ont donné ieu à 44 807 décisions de signalement avec un taux de retrait de 92%[4].

1 https://www.europol.europa.eu/about-europol/eu-internet-referal-unit-eu-iru
2 https://www.europol.europa.eu/about-europol/eu-internet-referal-unit-eu-iru
3 https://www.europol.europa.eu/publications-documents/eu-internet-referral-unit-transparency-report-2017
4 https://www.europol.europa.eu/publications-documents/eu-internet-referral-unit-transparency-report-2017

Comme cela est précisé dans le mandat de l'UE IRU et dans son rapport sur la transparence, cette unité est chargée d'évaluer les contenus en ligne et de les signaler à l'entreprise des TIC concernée à des fins de suppression. L'UE IRU se focalise sur les contenus publiés par Al-Qaeda et Daesh et les groupes qui lui sont affiliés et évalue ces contenus à la lumière du mandat d'Europol, conformément aux principes énoncés dans la Directive de l'UE relative à la lutte contre le terrorisme. Cette Directive prévoit des garanties en matière de suppression de contenus, précisées à l'article 21 (3) :

Les mesures visant à supprimer des contenus et à bloquer leur accès doivent être établies à la suite de procédures transparentes et fournir des garanties suffisantes, en particulier pour veiller à ce que ces mesures soient limitées à ce qui est nécessaire et proportionné, et que les utilisateurs soient informés de la raison de ces mesures. Les garanties relatives à la suppression ou au blocage incluent aussi la possibilité d'un recours juridictionnel[5].

Si le contenu évalué relève du mandat d'Europol, il est signalé à l'entreprise informatique qui l'héberge. Cependant, la décision de supprimer – ou non – un contenu est laissée à la discrétion de l'entreprise, qui l'évalue à l'aune de ses conditions de service. L'UE IRU n'a aucun pouvoir juridique pour supprimer un contenu.

Des unités de signalement de contenus similaires existent au Royaume-Uni, en France et aux Pays-Bas et Europol a indiqué que des mécanismes parallèles ont été mis en place en Belgique, en Allemagne et en Italie[6].

En outre, l'UE IRU organise des journées d'action conjointes de signalement de contenus (« joint Referral Action Days ») avec des entreprises du secteur des TIC telles que Google, Twitter et Telegram. Ces journées conjointes réunissent des unités chargées de l'application de la loi issues de plusieurs IRU au niveau national, ainsi que des représentants de l'UE IRU et d'entreprises des TIC. Des spécialistes de l'application de la loi évaluent alors plusieurs centaines de contenus potentiellement terroristes hébergés sur une plate-forme donnée, dans l'objectif de déterminer si cette plate-forme est utilisée de manière récurrente pour véhiculer des messages provenant de groupes extrémistes terroristes et violents. Les constats de cet examen sont ensuite partagés avec les entreprises des TIC présentes, qui examinent le contenu détecté à l'aune de leurs propres termes et conditions. La décision finale de supprimer le contenu détecté appartient à l'entreprise. Les journées d'action conjointes de signalement de contenus favorisent une approche coordonnée entre les autorités étatiques et les entreprises des TIC pour lutter contre les contenus extrémistes et terroristes violents sur Internet[7].

5 https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32017L0541

6 Voir https://www.europol.europa.eu/newsroom/news/referral-action-day-six-eu-member-states-and-telegram

7 Voir https://www.europol.europa.eu/newsroom/news/eu-law-enforcement-and-google-take-terrorist-propaganda-in-latest-eu-ropol-referral-action-days; https://www.europol.europa.eu/newsroom/news/referral-action-day-six-eu-member-states-and-telegram

Initiatives pilotées par les entreprises des TIC et par la société civile

Les entreprises des TIC sont très souvent confrontées à des problèmes de co-régulation et d'autorégulation de leurs plateformes, en particulier lorsqu'il s'agit d'assurer la protection des droits humains tels que la liberté d'expression et le droit à la vie privée. Ces défis sont exacerbés par le fait que les plates-formes de médias sociaux sont devenues des outils essentiels de discussion, de partage et d'accès à l'information. Afin de relever ces défis, le secteur des entreprises des TIC a lancé des initiatives, notamment pour assurer le partage des connaissances et de technologies entre entreprises ; et mettre en place des plates-formes facilitant l'élaboration de ressources et d'outils interactifs pour assurer la modération des contenus. Par ailleurs, les grandes entreprises ont organisé des sessions de formation sur les modalités de suppression de contenus à l'intention d'entreprises de plus petite taille. Ces actions peuvent constituer des outils efficaces pour renforcer la cybersécurité.

ÉTUDE DE CAS : INHOPE

Présente dans 43 pays, l'Association internationale de services d'assistance en ligne (INHOPE) vise à contribuer à un Internet « exempt d'abus et d'exploitation sexuels contre des enfants[8] ». Sa mission est de « renforcer les actions internationales de lutte contre les matériels pédopornographiques[9] ». INHOPE travaille en partenariat avec un éventail de parties prenantes, notamment Interpol, Europol, Twitter, Crisp, Microsoft, Google, Facebook et Trend MICRO.

INHOPE dispose de 48 services d'assistance en ligne qui permettent à la population de signaler un contenu ou une activité en ligne suspectés d'être illégaux. INHOPE classe les activités illégales en deux catégories : d'une part, les activités criminelles illégales susceptibles de faire l'objet d'une enquête et de poursuites par les forces chargées de l'application de la loi et sur lesquelles se focalise l'action menée par INHOPE et, d'autre part, les activités civiles illégales pouvant faire l'objet de poursuites par des organes civils.

INHOPE se focalise sur la recherche de matériels pédopornographiques, notamment les sollicitations en ligne à des fins sexuelles, mais elle prend également en compte les discours de haine et les contenus xénophobes en ligne. Bien qu'INHOPE fournisse une définition du discours de haine, elle reconnaît qu'il s'agit là d'une question « extrêmement complexe » et que, bien souvent, la diffusion de ce type de discours n'est pas illégale au regard du droit pénal. Par conséquent, chaque information faisant état de discours de haine est évaluée à la lumière de la législation nationale, c'est-à-dire de la législation applicable dans le pays où le contenu est hébergé[10].

8 http://88.208.218.79/gns/home.aspx
9 http://88.208.218.79/gns/who-we-are/our-mission.aspx
10 http://88.208.218.79/gns/internet-concerns/overview-of-the-problem/hate-speech.aspx

Tous les contenus signalés anonymement sont examinés par un analyste qui est chargé d'évaluer si le contenu est illégal. Si cet analyste parvient à cette conclusion, l'emplacement de ce contenu est repéré. Si le contenu est hébergé par un site situé dans le même pays, le contenu est signalé aux autorités nationales chargées de l'application de la loi et / ou à l'entreprise des TIC à des fins de suppression. Si le matériel est hébergé dans un pays étranger, il est renvoyé au membre du réseau d'INHOPE dans le pays concerné.

INHOPE a également élaboré un code de pratique pour ses services d'assistance en ligne qui précise que les membres d'INHOPE doivent respecter les principes de transparence, de responsabilité et de fiabilité et doivent consulter régulièrement les parties prenantes clés, notamment les autorités étatiques, les agences chargées de l'application de la loi, les entreprises des TIC ainsi que les institutions de protection de l'enfance.

INHOPE accorde également une grande importance à la santé physique et psychologique des personnes chargées d'examiner les contenus suspects et elle est consciente du fait que l'examen de contenus pédopornographiques, extrémistes ou terroristes violents peut avoir un impact psychologique sur ces individus. La plateforme française de signalement de contenus illicites sur Internet, Point de Contact, a élaboré et publié un Livre blanc qui vise à identifier un ensemble commun de bonnes pratiques en matière de gestion et de traitement opérationnels de contenus préjudiciables et potentiellement illégaux susceptibles de mettre en danger la sécurité physique et le bien-être psychologique des professionnels chargés de procéder à l'analyse de ces contenus[11].

2. Créer des PPP en matière de cybersécurité

Bonne pratique 1 : Instaurer un environnement favorable est une condition préalable à la mise en place de PPP efficaces.

Pour mettre en place des PPP efficaces, il faut absolument instaurer au préalable un environnement favorisant ce type de coopération. Cela repose sur quatre dimensions clés : la formulation de politiques ; un cadre juridique et réglementaire ; des dispositions institutionnelles et un soutien / des investissements financiers. Par ailleurs, les Lignes directrices de l'UE soulignent qu'il est important que toutes les parties prenantes impliquées fassent preuve de flexibilité et de transparence. Ces Lignes directrices mettent également l'accent sur la nécessité d'une reconnaissance mutuelle des besoins et des objectifs des différentes parties prenantes impliquées[12].

11 http://88.208.218.79/Libraries/External_reports_Library/White_Paper__PointdeContact.sflb.ashx

12 Lignes directrices de l'UE https://www.europol.europa.eu/about-europol/eu-internet-referal-unit-eu-iru

Pour instaurer un environnement favorable il faut également que les parties prenantes s'accordent sur le fondement juridique du PPP. Les institutions publiques devraient jouer un rôle moteur dans la création de PPP ou de plans d'action nationaux. Pour ce faire, il faut allouer des ressources suffisantes aux mécanismes de coordination et de collaboration internes des PPP et adopter une approche pragmatique afin de résoudre les éventuels problèmes de coordination et de collaboration. Il est également important d'encourager la participation du secteur privé, en particulier des petites et moyennes entreprises afin de créer un environnement favorable qui incite à la coopération et la collaboration entre les parties prenantes concernées. Enfin, les parties prenantes à un PPP devraient établir une communication ouverte avec le grand public.

Bonne pratique 2 : Des lignes de responsabilité claires devraient être établies afin de protéger les droits humains.

Il est essentiel d'établir des lignes de responsabilité et de redevabilité claires entre toutes les parties prenantes, notamment pour prévenir les atteintes aux droits humains. Cet objectif peut être particulièrement difficile à atteindre dans le cas des PPP qui sont mis en place afin de mettre en œuvre une SNSC. Cela peut s'expliquer par plusieurs raisons, notamment la réticence des décideurs politiques à assumer la responsabilité d'une législation stricte en matière de cybersécurité ainsi que l'aversion du secteur privé à assumer quelque responsabilité que ce soit en matière de sécurité nationale. Du fait de ces obstacles, ce type de partenariats peut ne pas reposer sur des lignes de responsabilité claires. L'inclusion dans les accords de PPP d'informations précises sur les lignes de responsabilités et les mécanismes de redevabilité est donc essentielle pour réduire les risques et garantir que toutes les parties prenantes comprennent bien leurs rôles et leurs responsabilités.

Bonne pratique 3 : La confiance entre les parties prenantes doit être instaurée et maintenue.

L'instauration et le maintien d'un climat de confiance entre les entités publiques et privées constitue l'un des défis majeurs auxquels sont confrontés les PPP. Il s'agit là d'un processus continu, qui dépend du contexte culturel et des relations interpersonnelles. Il ne peut y avoir de climat de confiance sans un environnement favorable. Les autres défis à relever incluent le manque de ressources humaines dans le secteur public comme privé ; l'insuffisance des allocations budgétaires et des ressources fournies par le secteur public par rapport aux attentes du secteur privé ; et une compréhension et un dialogue insuffisants entre les secteurs publics et privés concernant le concept même de PPP.

Les agences publiques et les entités privées doivent être fondées sur la transparence, l'équité et le respect mutuel. À cet égard, le partage d'informations entre membres d'un PPP constitue un test de confiance important. Les membres d'un PPP doivent avoir le sentiment que leur participation à ce partenariat leur permet d'avoir accès à des informations dont ils ne disposeraient pas sinon et ils doivent, dans le même temps, avoir la certitude que les informations qu'ils partagent sont sûres et sécurisées.

ÉTUDE DE CAS: FORUM GLOBAL SUR LA CYBER EXPERTISE

Le Global Forum on Cyber Expertise (GFCE) est une plate-forme permettant aux États, aux organisations internationales et aux entreprises privées d'échanger de bonnes pratiques et une expertise en matière de renforcement des capacités liées au cyberespace.

Lancé en avril 2015, le GFCE avait pour principal objectif d'instaurer une plate-forme informelle à l'intention des décideurs politiques, des praticiens et des experts de différents pays et régions, afin de faciliter le partage d'expériences, d'expertises et d'évaluations sur des problèmes régionaux et thématiques clés liés au cyberespace. Depuis son lancement, l'action du GFCE s'est transformée pour devenir une plate-forme de coordination. Initialement, le renforcement des capacités et des compétences était focalisé sur les questions de cybersécurité, de cybercriminalité, de protection des données et de cybergouvernance. En 2019, le GFCE a mené des actions afin de faciliter et coordonner le partage des connaissances et des compétences pour favoriser le renforcement des capacités liées au cyberespace. De plus, les différents groupes de travail du GFCE œuvrent à la mise en place d'un mécanisme d'échange d'informations.

Source : 'History', the GFCE

Conclusions Clés

- Dans le domaine du cyberespace et de la cybersécurité, la collaboration entre groupes composés de diverses parties prenantes est souvent plus efficace que les actions isolées. Les approches multi-acteurs, également appelées partenariats public-privé (PPP), permettent d'élaborer conjointement des modalités d'action et des solutions plus adéquates. Ces partenariats jouent un rôle de plus en plus indispensable pour assurer la gouvernance du cyberespace et résoudre les problèmes de cybersécurité.
- Les PPP s'articulent autour d'accords de collaboration entre institutions publiques et privées.
- Les autorités étatiques peuvent jouer un rôle important dans la coordination et la collaboration avec le secteur des TIC et la société civile en créant et en soutenant des plateformes de collaboration.
- Des acteurs privés tels que le secteur des TIC peuvent également piloter des initiatives multi-acteurs efficaces en matière de cybersécurité.

- Les autorités étatiques devraient adopter des approches pragmatiques afin de mettre en place des PPP reposant sur une communication ouverte, une participation inclusive et une implication croissante du secteur privé.

Bibliographie

Public-Private Partnerships in Cyberspace, ENISA, novembre 2017. Disponible sur : https://www.enisa.europa.eu/publications/public-private-partnerships-ppp-cooperative-models/at_download/fullReport

Public-private partnerships in national cyber-security strategies. Disponible sur : https://www.chathamhouse.org/sites/default/files/publications/ia/INTA92_1_03_Carr.pdf

US National Council for Public Private Partnerships Definition of PPPs (2016)

Public Private Partnerships in the EU: Widespread shortcomings and limited benefits. Disponible sur:

http://publications.europa.eu/webpub/eca/special-reports/ppp-9-2018/en/

CERT africains. Disponible sur : https://www.africacert.org/african-csirts/

EU IRU. Disponible sur : https://www.europol.europa.eu/about-europol/eu-internet-referal-unit-eu-iru

www.dcaf.ch