Plan

Objectifs du module

Bienvenue dans le module de connaissances sur la cyberdiplomatie et la coopération internationale, dans le cadre du projet GFCE-Afrique.

Ce module de connaissances traite des risques émergents de cybersécurité pour la paix et la sécurité internationales, présente le cadre international existant pour un comportement responsable des États dans le cyberespace, cartographie les principaux processus diplomatiques et multipartites qui façonnent ce programme et passe en revue les expériences liées à la mise en place de capacités nationales de cyberdiplomatie.

Le thème de la politique et de la stratégie de cybersécurité peut être vu comme le « fondement » des autres thèmes identifiés dans le programme mondial du GFCE pour le renforcement des capacités en matière de cybersécurité.

Reconnaissant l'importance des cybernormes et de la cyberdiplomatie, le groupe de travail A du GFCE, qui examine les questions de politique et de stratégie, a créé un groupe de travail « mesures de confiance, mise en œuvre des normes et cyberdiplomatie ».

En savoir plus :
https://thegfce.org/working-groups/working-group-a/

À la fin de ce module, vous serez en mesure de répondre et de trouver des ressources supplémentaires pour les questions suivantes :

- Comment les cyberattaques peuvent-elles impacter les économies nationales et les relations politiques ? Pourquoi les cyberattaques sont-elles utilisées à des fins militaires et politiques ? Les États développent-ils leurs cybercapacités offensives ?
- Quelles sont les « règles de conduite » actuelles pour les États dans le cyberespace ? (Comment) le droit international s'applique-t-il au cyberespace ?
- Quelles sont les normes ? Comment interagissent-elles avec le droit international ? Comment les mettre en œuvre dans tous les États africains ?
- Quelles sont les mesures de confiance (MDC) ? Quelle est l'importance des MDC régionales ? Quels sont les principes fondamentaux de renforcement des cybercapacités fixés par l'ONU ?
- Quel est le lien entre les droits de l'homme et les cybernormes ? Quel est l'impact de la cybersécurité sur le développement économique et les ODD ?
- Quels sont les antécédents de négociations et de dialogue sous l'ONU ? Quels sont les éléments actuels et éventualités futures du dialogue institutionnel ? Quels autres principaux processus diplomatiques et politiques ont des composants de cybersécurité à l'ordre du jour ?
- Quels sont les principaux instruments développés au niveau régional ? Comment ces outils peuvent-ils aider les développements africains ?

- Quelle est l'utilité des discussions multipartites pour les initiatives de cyberdiplomatie ? Quelles sont les instances multipartites les plus pertinentes avec lesquelles les États africains devraient dialoguer ?
- La cyberdiplomatie concerne-t-elle uniquement la cybersécurité ?
- Quel rôle jouent les acteurs non étatiques dans la cyberdiplomatie, notamment au niveau régional ? Pourquoi l'inclusion des acteurs est-elle importante pour parvenir à des accords significatifs ?
- Quelles sont les compétences requises par les cyberdiplomates ? De quelles compétences les autres acteurs ont-ils besoin pour contribuer aux cyberprocessus ? (Pourquoi et comment) les diplomates et les non-diplomates devraient-ils travailler ensemble ? Quel est le rôle des autres acteurs ?

1 Risques pour parvenir à la paix internationale et la cyberstabilité

> *Je suis absolument convaincu que, contrairement aux grands affrontements du passé, qui commençaient par des tirs d'artillerie ou des bombardements aériens, la prochaine guerre commencera par une cyberattaque massive pour détruire les moyens militaires... et paralyser les infrastructures de base comme les réseaux électriques.*
> António Guterres, secrétaire général de l'ONU (Reuters, 2018)

On craint de plus en plus que les cyberattaques ne soient utilisées ou dégénèrent en conflits transfrontaliers. Dans cette partie, nous nous pencherons sur les cas majeurs de cyberattaques qui ont eu des conséquences économiques et politiques, le rôle des cyberattaques et de la désinformation dans le cadre de la guerre hybride, et les tendances avec le cyber-armement des pays.

1.1 Cyberattaques et géopolitique

- *Comment les cyberattaques peuvent-elles impacter les économies nationales et les relations politiques ?*

Des dizaines de cas de cyberattaques ont eu de graves conséquences sur les économies mondiales et régionales, le bien-être et les relations politiques. Il s'agit notamment des attaques et des piratages par déni de service distribué (DDoS) qui paralysent les infrastructures nationales essentielles, des cas d'espionnage politique et économique, des opérations de ransomware, le vol de quantités massives de données personnelles, des opérations de surveillance, ainsi que des actes de provocation régionale, des cyberattaques menées pour soutenir la guerre, et les frappes conventionnelles en réponse aux cyberattaques.

L'illustration 1 cartographie des exemples clés des événements majeurs des 20 dernières années. Il ne s'agit pas d'une étude approfondie, mais d'une illustration de quelques exemples importants, de types d'attaques et d'effets potentiels.

Intégrer : https://dig.watch/processes/un-gge/#In-context
Illustration 1 : Carte interactive de quelques cyberattaques majeures avec contexte et conséquences politiques (DiploFoundation, 2022)

Point de réflexion

Existe-t-il des exemples pertinents dans votre région ? Quelles étaient les cibles ? Quelles en ont été les conséquences politiques et économiques ?

Laissez votre commentaire ci-dessous.

1.2 Cyber dans le cadre de la guerre hybride

- *Pourquoi les cyberattaques sont-elles utilisées à des fins militaires et politiques ?*

La Conférence de Munich sur la sécurité a perçu les cyberattaques comme un élément important de la guerre hybride en 2015 (Conférence de Munich sur la sécurité, 2015).

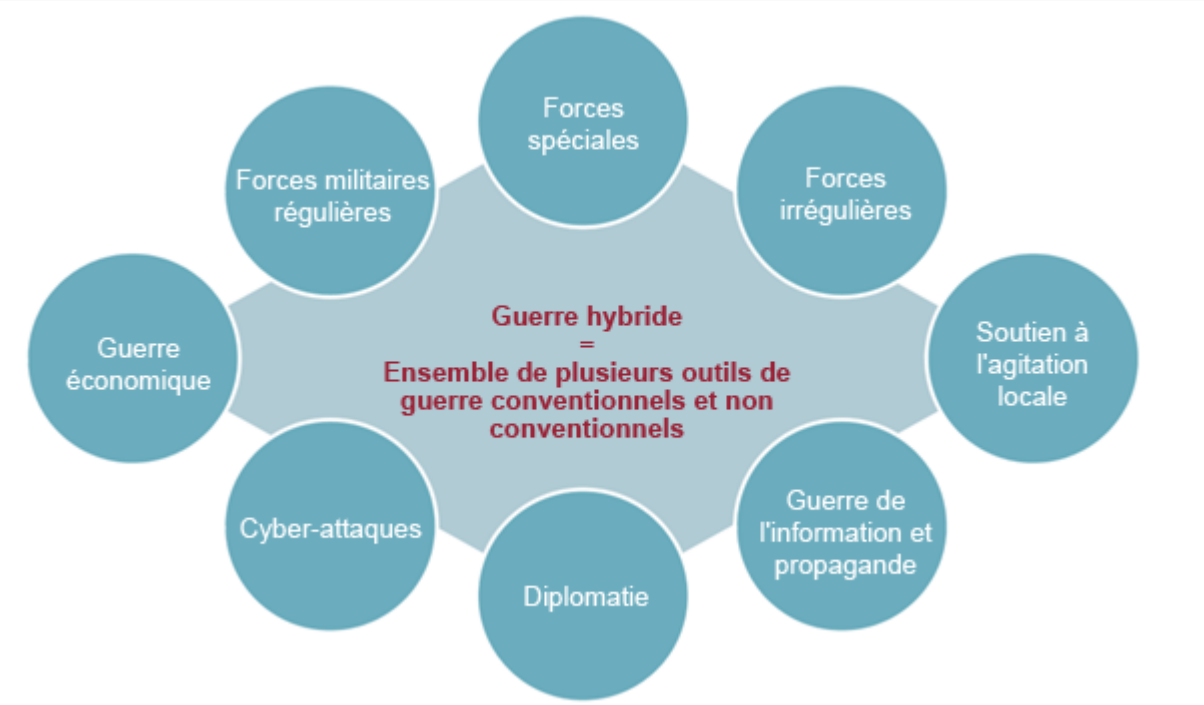

Illustration 2 : Les cyberattaques sont l'une des composantes importantes de la guerre hybride (Source : Conférence de Munich sur la sécurité, 2015)

D'une part, cela signifie que les cyberattaques pourront, à l'avenir, être utilisées en association avec des opérations conventionnelles. D'autre part, les cyberattaques deviennent des moyens populaires pour affaiblir les adversaires ; en particulier en « temps de paix » (en deçà des critères d'attaque armée dans la conception traditionnelle) ; car elles peuvent être adaptées pour des activités spécifiques (de l'espionnage à la perturbation des systèmes numériques sans causer de dommages physiques, jusqu'à la désactivation

d'installations industrielles physiques, mais sans faire de victimes), et plus encore en raison de la négation (haute complexité d'attribution).

En plus de mener des cyberattaques, les États se tournent vers la guerre de l'information en utilisant des plateformes numériques. Dans la pratique, il s'agit souvent de campagnes de désinformation ciblant l'ingérence dans les élections, les initiatives de lutte contre les maladies (comme en témoigne la pandémie de COVID-19) ou provoquant des clivages et des troubles politiques. Alors que l'utilisation trompeuse d'informations à des fins hostiles existe depuis longtemps, Internet, et en particulier les médias sociaux, permettent un ciblage et une manipulation quasi instantanés des populations à des coûts relativement faibles. Certains pays ont déjà intégré les menaces d'influence malveillante et les campagnes d'information, la propagande et la désinformation dans leurs stratégies nationales.

1.3 Cyber-armement

- *Les États développent-ils leurs cybercapacités offensives ?*

Les incidents de cybersabotage ou de cyberespionnage ont accéléré le cyber armement. L'OTAN considère que le cyber constitue l'un des cinq domaines militaires (avec la terre, la mer, l'air et l'espace). De nombreux pays ont établi des budgets importants pour le renforcement des cybercapacités militaires, à la fois offensives et défensives. La cartographie des documents accessibles au public, tels que les stratégies nationales, les doctrines militaires, les déclarations officielles et les sources médiatiques fiables, présente des preuves et des indications que des cybercapacités offensives (OCC) existent ou sont en cours de construction dans plus de 50 États (illustration 3).

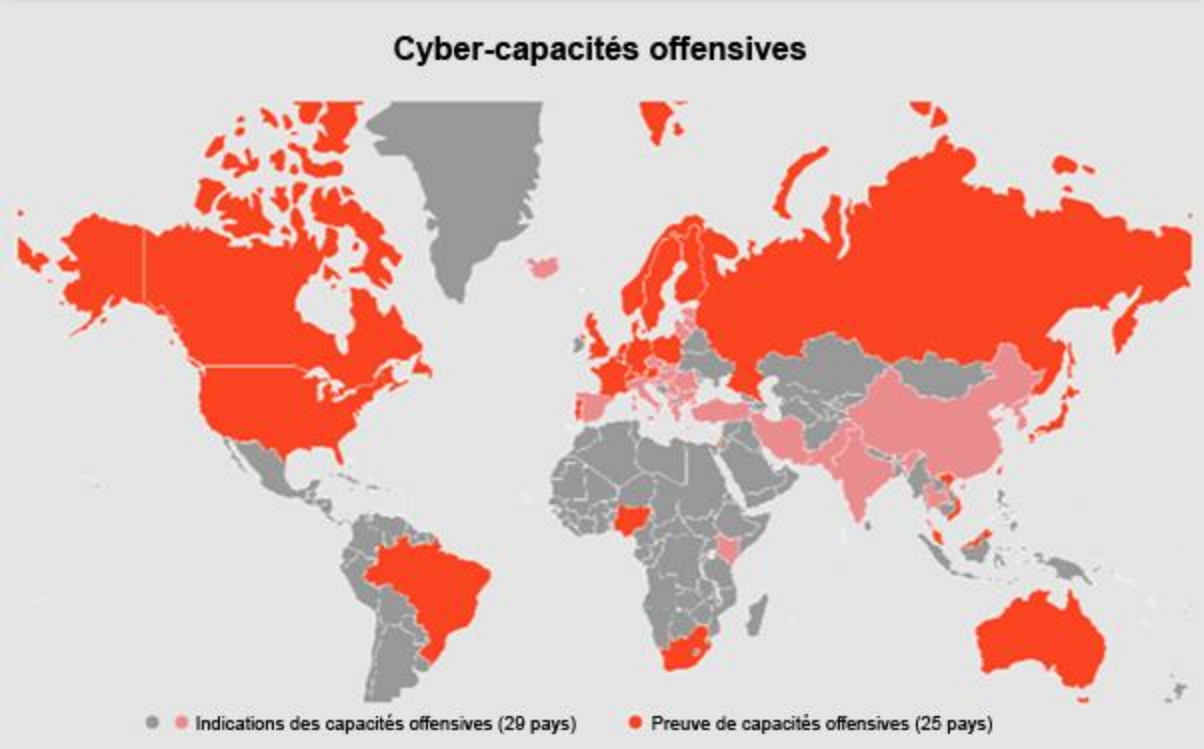

Illustration 3. Carte interactive des États dotés de cybercapacités offensives (DiploFoundation, 2021)

Point de réflexion

Votre pays élabore-t-il des cybercapacités offensives ? Dans quelle mesure les plans de développement et de déploiement des OCC sont-ils clairs ?

Laissez votre commentaire ci-dessous.

2 Vers un accord international

Le fait que de futures cyberattaques potentielles, tout en provoquant des destructions massives, pourraient également déclencher une guerre conventionnelle, a alimenté des initiatives visant à codifier la réponse diplomatique, ainsi qu'à discerner les défis de l'application du droit international au cyberespace et à formuler un cadre pour un comportement responsable des États.

Les négociations dans ce contexte relèvent de trois domaines principaux :

- Critères pour entrer en guerre ou invoquer le *jus ad bellum* (« droit à faire la guerre », c'est-à-dire l'ensemble du droit international régissant le droit des États à recourir à la guerre), et en particulier, comment les principes et certains articles de la Charte des Nations Unies s'appliquent à cyberespace.
- Droit international humanitaire ou *jus in bello* (« droit dans la guerre », c'est-à-dire les lois qui régissent la conduite des conflits), en particulier, comment appliquer les Conventions de La Haye et les Conventions de Genève dans le cyberespace.
- Armes et désarmement, et des questions comme comment (et si) introduire des cyberarmes dans le processus de désarmement.

Même si, pour de nombreux pays, ce sont de nouvelles questions à l'ordre du jour des affaires étrangères, elles sont examinées dans le cadre de l'ONU depuis 1998. Un bref historique des cyber-processus de l'ONU est illustré dans la vidéo 1, tandis que plus de détails sont abordés plus loin dans le module.

[Intégrer la vidéo : https://www.youtube.com/watch?v=JbMn_9uzxfk]

Vidéo 1. Une histoire animée des cyber-processus des Nations Unies. (UNIDIR, 2021)

Outre la clarification de la manière dont le droit international s'applique au cyberespace, les délibérations de l'ONU ont également indiqué comment traiter les incidents en temps de paix, par exemple les cyberattaques qui relèvent des attaques armées. Dans cette optique, un ensemble de normes volontaires, de mesures de confiance (MDC) et de principes de renforcement des capacités ont été élaborés par l'ONU et les organisations régionales.

2.1 Bases pour un comportement responsable des États dans le cyberespace

- *Quelles sont les « règles de conduite » actuelles pour les États dans le cyberespace ?*

Les négociations de l'ONU ont donné naissance à un cadre de comportement responsable des États dans le cyberespace (ci-après appelé le Cadre), composé de quatre piliers : le droit international, les normes, les MDC et le renforcement des capacités (vidéo 2).

[Intégrer la vidéo : https://ad-aspi.s3-ap-southeast-2.amazonaws.com/2020-09/UN-framework_ENGLISH.mp4]

Vidéo 2. Cadre des Nations Unies sur le comportement responsable des États dans le cyberespace (ASPI, 2020)

Le cadre est défini par l'ensemble des accords internationaux existants sous l'égide de l'ONU (appelé officieusement « *l'acquis* », rappelant le terme utilisé comme référence à l'ensemble des lois de l'UE), en particulier les rapports du groupe d'experts gouvernementaux de l'ONU (GGE) et le Groupe de travail à composition non limitée des Nations Unies (GTCNL).

La proposition de résolution A/C.1/76/L.13 de l'Assemblée générale des Nations Unies (AGNU), déposée conjointement par les États-Unis et la Russie à l'automne 2021, précise que les deux instruments de base qui devraient guider les États dans leur utilisation des technologies de l'information et de la communication (TIC) sont :

- Le rapport de 2021 du Groupe de travail à composition non limitée des Nations Unies (GTCNL) (AGNU Res. A/75/816)
- Le rapport de 2021 du groupe d'experts gouvernementaux (GGE) (ANGU Res. A/76/135)

En outre, la résolution réitère l'importance des trois précédents rapports de consensus du GGE : de 2010 (A/65/201), 2013 (A/68/98* et A/RES/68/243) et 2015 (A/ 70/174 et A/RES/70/237).

Ressources

L'Ambassadeur Jürg Lauber, Représentant permanent de la Suisse auprès des Nations Unies et d'autres organisations à Genève, a donné une interview « masterclass » pour le podcast « Inside Cyber Diplomacy ». Dans sa discussion avec Jim Lewis et Chris Painter, il a partagé des expériences dans son travail en tant que président du GTCNL, ainsi que comment son expérience antérieure à l'ONU l'a aidé à accroître son engagement dans le processus et quelle direction prendre à partir de là.

Parallèlement, l'ambassadeur Guilherme Patriota, consul général du Brésil à Mumbai et président du GGE des Nations Unies sur la promotion d'un comportement responsable des États dans le cyberespace dans le contexte de la sécurité internationale, a accordé une interview pour le podcast « Inside Cyber Diplomacy ». Il a discuté dans cet entretien de l'influence de son expérience de négociation passée sur la façon dont il a présidé le groupe, comment ils ont dû s'adapter à la négociation pendant la Covid pour parvenir à un rapport de consensus et si ses plans futurs impliqueront les TIC.

2.2 Application du droit international

- *(Comment) le droit international s'applique-t-il au cyberespace ?*

Selon le Cadre, les États conviennent que le droit international existant et la Charte des Nations Unies s'appliquent au cyberespace. Le droit international établi réglemente la conduite des conflits armés et cherche à en limiter les effets.

Il est cependant moins clair de savoir comment il s'applique dans la pratique et dans des circonstances particulières. La Charte des Nations Unies, en tant que fondement de l'ensemble du droit international qui fournit des motifs pour justifier l'entrée dans un conflit, accorde (Article 51) le droit de légitime défense individuelle ou collective en cas d'attaque armée contre un État membre. Pourtant, qu'est-ce qu'une attaque armée et un recours à la force dans le cyberespace, et quelle est sa limite ? Est-ce limité aux attaques qui causent des dommages physiques et des blessures, ou d'autres effets (par exemple, financiers, environnementaux, économiques ou politiques) d'une cyberattaque en font-ils partie également ? Quand une cyberattaque porte-t-elle atteinte à la souveraineté d'un autre État, le cas échéant ? L'État attaqué devrait-il être autorisé à répondre par n'importe quel moyen, y compris toutes les options militaires avec les méthodes de guerre traditionnelles ?

Il est également difficile de comprendre comment le droit international humanitaire (DIH) régissant l'usage de la force dans les conflits armés, comme la protection des populations civiles et des infrastructures, s'appliquera. Pendant des années, les États n'ont pas réussi à s'entendre sur la question de savoir si le DIH s'appliquerait ou si son application militariserait en fait le cyberespace. Ce n'est qu'en 2021 que le GGE a confirmé que le DIH ne s'applique qu'en situation de conflit armé, donc pas en temps de paix. Le GGE indique également que l'application des principes fondamentaux du DIH à l'utilisation des TIC doit faire l'objet d'études plus approfondies.

L'un des principaux défis est de savoir comment tenir les États responsables de leurs opérations, de pouvoir attribuer de manière sûre l'attaque à la réponse sans risquer l'escalade des tensions politiques. Invoquer les dispositions du droit international et utiliser des éléments du Cadre présentent un intérêt lorsqu'il s'agit d'engager la responsabilité de certains États pour une cyberattaque et de tenir les États responsables de leurs cyberopérations. Le rapport GGE 2021 offre notamment une marge de progression puisqu'il impose des éléments d'attribution des cyberattaques, à savoir « les attributs techniques de l'incident ; sa portée, son échelle et son impact ; le contexte général, y compris la portée de

l'incident sur la paix et la sécurité internationales ; et les résultats des consultations entre les États concernés » (UN GGE, 2021, par. 24).

La recherche la plus approfondie et faisant autorité sur l'applicabilité du droit international au cyberespace et les défis qui y sont liés est le Manuel de Tallinn sur le droit international applicable à la cyberguerre, élaboré en 2013 par un groupe international indépendant d'experts invités par le CCDCOE de l'OTAN. Il a été mis à jour en 2017 ; et s'intitule le Manuel de Tallinn 2.0.

Contribuer et s'engager

Le CCDCOE invite les experts à contribuer au développement du Manuel de Tallinn 3.0. Les experts de votre pays peuvent rechercher des options pour s'engager et contribuer.

Les résolutions de l'AG de l'ONU de 2021 relatives aux rapports du GGE et du GTCNL invitent les États à partager leurs propres positions sur la manière dont le droit international s'applique au cyberespace. En effet, un nombre croissant d'États élaborent et publient les positions de leur pays. Un bon aperçu des questions ouvertes et des positions générales des États sur l'applicabilité du droit international est disponible au Digital Watch Observatory.

Ressources

Le Cyber Law Toolkit est une ressource Web interactive dynamique pour les professionnels du droit qui travaillent sur des questions à l'intersection du droit international et des cyberopérations. La boîte à outils peut être explorée et utilisée de différentes manières. En son centre, elle se compose actuellement de 25 scénarios hypothétiques. Chaque scénario contient une description des cyberincidents inspirée d'exemples concrets, accompagnée d'une analyse juridique détaillée. L'objectif de l'analyse est d'examiner l'applicabilité du droit international aux scénarios et aux problèmes qu'ils soulèvent.

Point de réflexion

Y a-t-il une prise de conscience du cadre existant et des processus connexes au sein de votre ministère des Affaires étrangères et, plus généralement, dans votre gouvernement ? Y a-t-il déjà des discussions en ce qui concerne une position nationale liée à l'applicabilité du droit international au cyberespace, comme invité par l'AG des Nations Unies ?

Laissez votre commentaire ci-dessous.

2.3 Normes, mesures de confiance et renforcement des capacités

2.3.1 Normes volontaires

- *Quelles sont les normes ?*

- *Comment interagissent-elles avec le droit international ?*
- *Comment les mettre en œuvre dans tous les États africains ?*

Les normes offrent des standards de comportement, façonnés par des termes de droits et d'obligations. Bien que non contraignantes, elles reflètent les attentes, augmentent la prévisibilité, réduisent les risques de perceptions erronées et contribuent à la prévention des conflits.

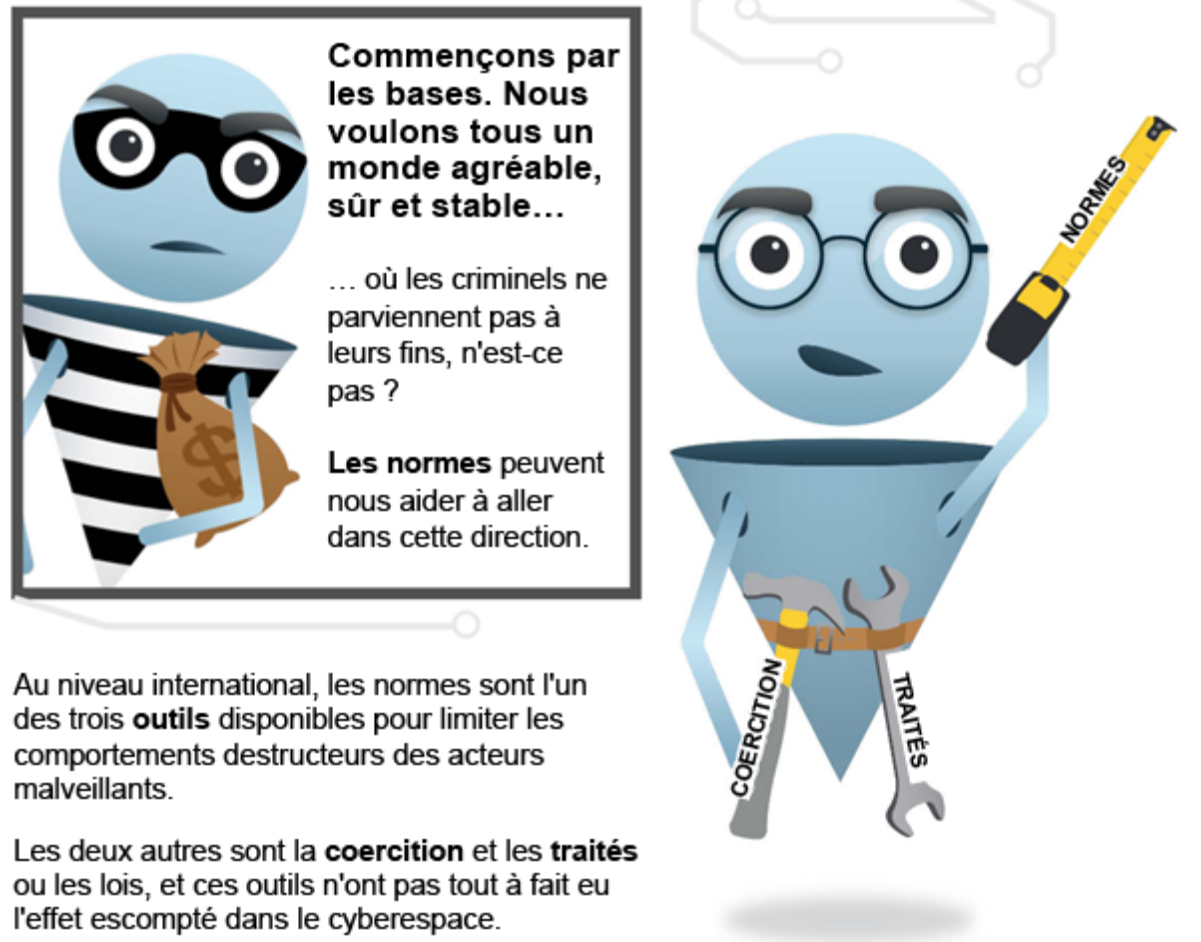

Illustration 4 : Guide graphique du professeur Cy Burr sur : LES CYBERNORMES INTERNATIONALES (Nouvelle Amérique, 2016)

Bien qu'ils ne remplacent pas les obligations contraignantes des États en vertu du droit international, les normes et principes convenus par l'AGNU se voient conférer la plus haute autorité. Dans le contexte du cyberespace, les normes sont particulièrement importantes pour les opérations en temps de paix afin de traiter des aspects qui ne sont pas suffisamment ou clairement couverts par le droit international existant.

Le Cadre décrit et élabore 11 normes pour un comportement responsable des États dans le cyberespace (illustration 5).

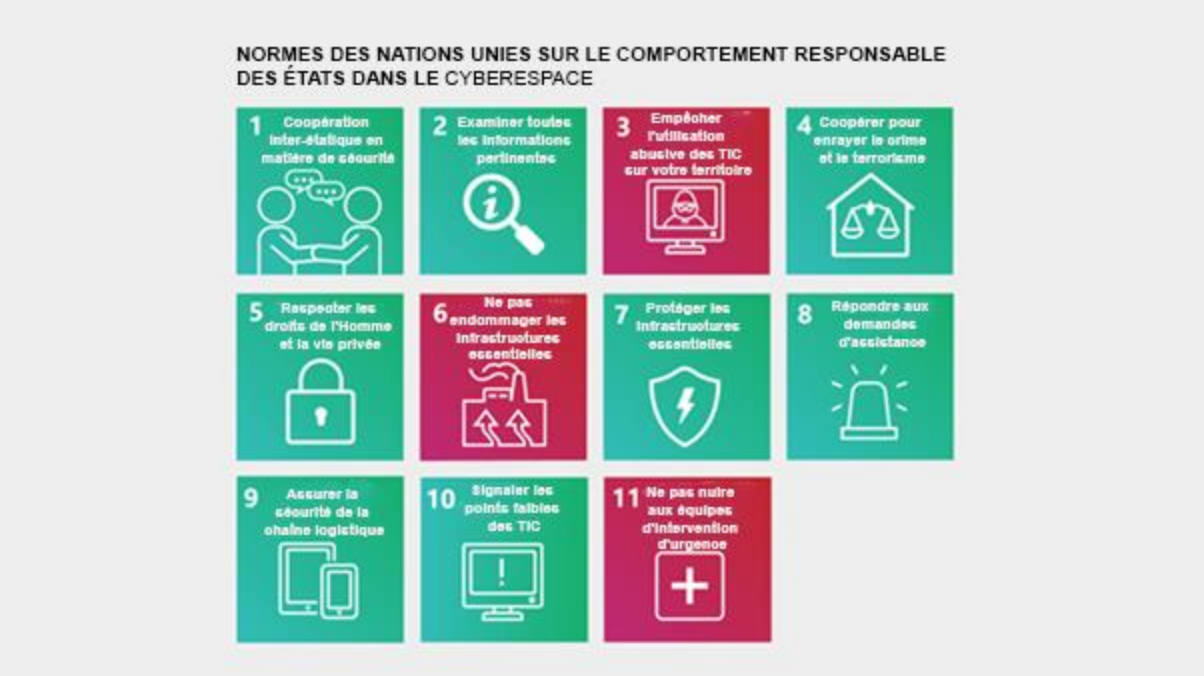

Illustration 5. Onze normes des Nations Unies pour un comportement responsable des États dans le cyberespace adoptées par le GGE des Nations Unies en 2015 (ASPI, 2020)

Contexte africain

« Putting Cyber Norms in Practice: Implementing the UN GGE 2015 recommendations through national strategies and Policies », un rapport rédigé par Mika Kerttunen et Eneken Tikk, commandé par le GFCE avec le soutien du FCDO britannique dans le cadre du processus Global CCB Research Agenda 2021, fournit nombre d'études de cas pour présenter les approches qui peuvent être, et ont été, adoptées pour mettre en œuvre les normes de comportement responsable de l'État qui font partie du Cadre. Le guide comprend également des exemples notables de pays africains.

L'Ile Maurice, par exemple, a pris un certain nombre de mesures pour mettre fin à la criminalité et au terrorisme, qui ont directement contribué à la mise en œuvre de la norme ONU GGE sur la coopération pour mettre fin à la criminalité et au terrorisme (13(d)). Les principales étapes comprennent : la loi sur la prévention du terrorisme (2002) a intégré des systèmes d'information dans la description des actes de terrorisme ; la loi sur l'utilisation abusive de l'informatique et la cybercriminalité a défini les cybercrimes (2003) ; la loi sur l'entraide judiciaire dans les affaires pénales et connexes (2003) qui jette les bases de la coopération internationale ; la stratégie nationale de cybersécurité (2014) a donné la priorité à la défense contre la cybercriminalité ; la stratégie de lutte contre la cybercriminalité (2017) appelle à une réponse plus efficace en matière d'application de la loi et de justice pénale, met l'accent sur l'harmonisation des cadres juridiques dans son approche de lutte contre la cybercriminalité et définit la collaboration avec des homologues internationaux comme l'un des sept objectifs ; le système mauricien de signalement en ligne de la cybercriminalité (MAUCORS) a été conçu pour faciliter le signalement sécurisé de la cybercriminalité en ligne et développer une meilleure compréhension de la cybercriminalité qui touche les

citoyens. Le Kenya est un autre bon exemple de contribution à cette norme, car il est membre du Commonwealth, du Harare Scheme et du London Scheme concernant l'entraide judiciaire en matière pénale au sein du Commonwealth.

Des exemples notables de contributions à la mise en œuvre de la norme relative à la coopération interétatique en matière de cybersécurité (13(a)) sont la Stratégie régionale de cybersécurité et de cybercriminalité de la Communauté économique des États de l'Afrique de l'Ouest (CEDEAO) (2021) et le Cadre stratégique national sud-africain sur la cybersécurité (2015). La norme relative au respect des droits de l'homme et de la vie privée (13(e)) est avancée par le parlement ivoirien, qui a reconnu et affirmé que l'accès à Internet et aux réseaux de communication électronique est un droit humain fondamental et un bien universel. Parallèlement, la loi sur la cybersécurité du Ghana, qui facilite la coopération entre la CERT nationale et les CERT d'autres pays, contribue à la norme relative à la non-atteinte aux équipes d'intervention d'urgence (13(k)).

2.3.2 Mesures de confiance

- *Que sont les mesures de confiance (MDC) ?*
- *Quelle est l'importance des MDC régionales ?*

Les mesures de confiance visent à prévenir l'hostilité, à réduire les tensions, à éviter l'escalade du conflit et à renforcer la confiance mutuelle entre les États. Le cadre des Nations Unies décrit un certain nombre de mesures de confiance volontaires pour accroître la coopération et la prévisibilité, et réduire les malentendus. Les MDC demandent, entre autres :

- *L'échange d'informations sur les* stratégies et politiques nationales, les processus décisionnels, les organisations nationales pertinentes et la terminologie nationale ; sur les menaces nationales et transnationales, les cyberincidents identifiés, les vulnérabilités des produits et les fonctions cachées, les meilleures pratiques en matière de traitement des cyberincidents et les classifications nationales des incidents ;
- La désignation de *points de contact nationaux* aux niveaux politique et technique, ainsi que la création d'un répertoire de personnes ressources ;
- La création et la coopération entre les *CERT/CSIRT nationales*, y compris pour les infrastructures essentielles ;
- La protection des *infrastructures que les États considèrent comme essentielles*, y compris les systèmes industriels, par l'échange d'informations et un recueil de lois et de politiques relatives aux infrastructures essentielles (IE), et le développement de mécanismes techniques, diplomatiques et juridiques pour protéger les IE, ainsi que le partenariat public-privé et la coopération multipartite pour cela ;
- La coopération dans les *enquêtes sur la cybercriminalité et le terrorisme*, grâce à la coopération des autorités chargées de l'application des lois, et désignation de points de contact pour l'échange d'informations sur les incidents et l'assistance aux enquêtes ;

- D'élaborer des mécanismes et des processus de consultation bilatérale, régionale, sous-régionale et multilatérale *pour éviter les perceptions erronées et le risque d'escalade* ;
- De développer des *ateliers, des séminaires et des exercices* pour prévenir et gérer les cyberincidents.

Étant donné que des organisations régionales telles que l'OSCE, l'ASEAN et l'OEA ont élaboré leurs propres mesures de confiance et principes, dont certains ont alimenté le Cadre des Nations Unies, cela encourage le partage d'informations sur les mesures de confiance élaborées dans les forums régionaux et multilatéraux. Nous aborderons le travail des organisations régionales plus tard dans ce module.

Ressources

Le document GFCE « Overview Of Existing Confidence Building Measures As Applied To Cyberspace » donne un aperçu des MDC élaborées par l'ONU et les organisations régionales d'ici 2020.

Point de réflexion

L'un des principaux éléments du renforcement de la confiance est l'amélioration du partage d'informations entre les États et les autres acteurs, et l'établissement de relations de confiance. Dans cette optique, quels sont les bons exemples à travers l'Afrique qui suivent les MDC de l'ONU ?

Quelles sont les autres MDC qui pourraient être particulièrement pertinentes pour la coopération africaine ?

Laissez votre commentaire ci-dessous.

Exercice (pour le format in situ et webinaire ; session en petits groupes)

À développer davantage

1) Discuter de la pertinence et de la mise en œuvre des mesures de confiance de l'ONU et régionales (telles que celles de l'OSCE, de l'OEA ou de l'ASEAN) dans des contextes nationaux.

2) Créer une liste de ces MDC qui s'appliquent au contexte africain, ainsi que celles qui ne sont peut-être pas pertinentes.

3) Discuter de ce que chaque pays africain a fait (ou pourrait facilement faire) pour les mettre en œuvre (par exemple, désigner un point de contact, partager des informations sur les lois nationales, connecter les CERT, etc.)

4) Discuter des MDC supplémentaires qui pourraient être développées pour répondre au contexte spécifique de l'Afrique qui ne sont pas « visées » par les MDC existantes de l'ONU et régionales.

5) Examiner si le fait de demander aux ministres africains de s'engager publiquement envers les MDC existantes (même s'il s'agit uniquement de celles de l'ONU) pourrait accroître leur engagement dans la mise en œuvre, ainsi que leur sensibilisation.

2.3.3 Renforcement des capacités

- *Quels sont les principes fondamentaux de renforcement des cybercapacités fixés par l'ONU ?*

Le renforcement des capacités est le troisième pilier du cadre international de cyberstabilité. Il existe un accord général sur l'importance du renforcement des capacités, et les processus des Nations Unies et diverses organisations régionales élaborent des mesures et des principes spécifiques.

Le rapport du GTCNL des Nations Unies de 2021 recommande que le renforcement des capacités soit un processus durable, comprenant des activités spécifiques par et pour différents acteurs, axé sur les résultats et avec un objectif clair, fondé sur des preuves, politiquement neutre, transparent, responsable et sans conditions, et entrepris en respectant pleinement le principe de la souveraineté de l'État. En outre, il doit être fondé sur la confiance mutuelle, avec une participation volontaire, axée sur la demande et adaptée aux besoins spécifiques, correspondre aux besoins et priorités identifiés au niveau national, entrepris en pleine reconnaissance de l'appropriation nationale et protéger la confidentialité des politiques et plans nationaux. Enfin, le renforcement des capacités doit respecter les droits de l'homme et les libertés fondamentales, être sensible et inclusif à la question du genre, universel et non discriminatoire.

Le rapport de l'ONU GGE de 2021 appelle en outre à ce que le renforcement des capacités soit volontaire, politiquement neutre, mutuellement bénéfique et réciproque, et suggère qu'il devrait aider les États à : élaborer et mettre en œuvre des politiques et stratégies nationales, renforcer les CERT, améliorer la résilience des infrastructures essentielles, renforcer les compétences et les capacités pour répondre aux incidents, approfondir la compréhension commune de la manière dont le droit international s'applique au cyberespace et mettre en œuvre des normes volontaires.

Ressources

Dans la vidéo de Diplo, plusieurs cyber ambassadeurs discutent du renforcement des cyber capacités, en particulier des besoins nécessaires pour développer les capacités de cyber diplomatie.

Contribuer et s'engager

Pour en savoir davantage sur le renforcement des cyber capacités, l'apprentissage et le développement des compétences, reportez-vous au module de connaissances 4.

2.4 Contexte général

- *Quel est le lien entre les droits de l'homme et les cybernormes ?*
- *Quel est l'impact de la cybersécurité sur le développement économique et les ODD ?*

Les délibérations concernant la cybersécurité et les normes connexes ne se font pas à la légère. Afin d'observer un contexte plus général, la cybersécurité devrait être synonyme de discussions politiques en lien avec les aspects numériques des droits de l'homme et le développement économique.

Le lien entre les cybernormes et les droits de l'homme n'est peut-être pas évident à première vue. Le rapport de l'APC et de Global Public Digital, Déballer le Cadre du GGE sur le comportement responsable des États : Cyber normes, précise que l'objectif des cybernormes de promouvoir un comportement responsable de l'État dans le cyberespace contribue aux conditions sous-jacentes nécessaires à l'exercice des droits de l'homme aujourd'hui. Le rapport explique en outre comment chacune des normes se rapporte aux droits de l'homme.

En outre, la relation entre le programme Les femmes, la paix et la sécurité (FPS) et les cybermenaces et la cybersécurité est explorée dans le rapport « Mise à jour système : Vers un programme Femmes, paix et cybersécurité » de l'Institut des Nations Unies pour la recherche sur le désarmement (UNIDIR). Le document analyse les liens entre les thèmes prioritaires FPS (égalité des sexes, participation des femmes à la sécurité internationale, prévention et protection de la violence à l'égard des femmes, besoins différenciés selon le sexe) et la cybersécurité internationale. Il identifie les domaines prioritaires qui doivent être abordés pour garantir un cyberespace non sexiste qui protège les droits des femmes et des filles.

D'autre part, le développement durable s'appuie fortement sur la numérisation et les technologies numériques, en tant que lien entre la transformation numérique et la vitrine des objectifs de développement durable. « Le rapport sur les risques mondiaux 2022 » du Forum économique mondial met l'accent sur le lien entre les deux préoccupations numériques particulières, « l'inégalité numérique » et « l'échec de la cybersécurité ». Un rapport du GFCE intitulé « Intégrer la cybercapacité dans le programme de développement numérique » souligne que la numérisation et la résilience sont indissociables, et identifie des voies pour relier les sujets et les communautés communément détachés ; les communautés du développement et de la cybersécurité, en particulier dans le domaine du renforcement des capacités.

Contexte africain

Dans son interview pour le podcast « Inside Cyber Diplomacy », co-animé par M. Jim Lewis et M. Chris Painter, M. Moctar Yedaly, directeur du programme Afrique pour le GFCE et ancien chef du département de la société de l'information au sein de la Commission de l'Union africaine, aborde le contexte africain et les négociations sur la cybersécurité. M. Yedaly établit également un lien entre la sécurité et le développement, discute de la nécessité d'un intérêt et d'une attention politique de haut niveau pour les questions des TIC, et de la valeur d'inclure davantage d'acteurs dans les négociations multilatérales.

Contribuer et s'engager

Pour en savoir plus sur le contexte plus général de la cybersécurité, reportez-vous au module de connaissances d'introduction.

3 Coopération internationale

3.1 Les Nations Unies

- *Quels sont les antécédents de négociations et de dialogue sous l'ONU ?*
- *Quels sont les éléments actuels et éventualités futures du dialogue institutionnel ?*

3.1.1 Dialogue institutionnel

Les questions liées à la cybersécurité ne sont pas récentes pour l'ONU. En 1998, la Fédération de Russie a présenté le projet de résolution *Développements dans le domaine de l'information et des télécommunications dans le contexte de la sécurité internationale*, de la Première Commission de l'AGNU, qui a été adopté sans vote.

Le cyberarmement croissant des États a conduit à la création en 2004 du GGE de l'ONU, composé d'experts de plusieurs États. Le groupe a terminé ses travaux sans élaborer de rapport final, mais le mandat du GGE a été renouvelé pour 2009/10, 2012/13, 2014/15, 2016/17 et 2019-2021 (ensemble appelés les GGE).

Une avancée importante s'est produite en 2013 lorsque le rapport final (adopté par consensus des 15 pays du GGE de l'époque, y compris tous les membres permanents du Conseil de sécurité - P5) a clairement décrit les tendances croissantes de la cybermilitarisation et a confirmé que le droit international s'appliquait au cyberespace. Le rapport du GGE de 2015 représente une autre avancée et a abouti à un document décisif ; 20 pays, y compris le P5, ont spécifié le cadre normatif volontaire et non contraignant concernant le comportement des États et se sont mis d'accord sur un ensemble de normes volontaires, de MDC et de dispositions de renforcement des capacités.

Le GGE 2016/17, qui a été étendu à 25 pays, n'a pas pu parvenir à un consensus sur son rapport final, notamment en raison d'un désaccord sur les options dont disposent les États pour répondre aux cyberattaques. En 2021, cependant, le GGE est de nouveau parvenu à un consensus sur un rapport final qui est devenu un pilier du cadre de comportement responsable. Il a confirmé l'applicabilité du DIH pendant les conflits armés, suggéré ce qui devrait être considéré comme infrastructures essentielles, élaboré plus en profondeur les normes volontaires et les MDC précédemment convenues, et défini des principes de renforcement des capacités.

En 2018, outre une résolution parrainée par les États-Unis qui a renouvelé le GGE pour 2018-2020, l'AGNU a adopté une autre résolution (A/RES/73/27) parrainée par la Russie qui a mis en place un processus parallèle, le Groupe de travail à composition non limitée (GTCNL), qui a impliqué tous les États intéressés et a permis les contributions d'autres acteurs. Alors que les deux groupes travaillaient en parallèle dans des contextes quelque peu différents, une coopération considérable s'est établie entre les présidents des deux groupes (Brésil et Suisse), et la plupart des pays ont exprimé leur intérêt à faire en sorte que les deux réussissent.

En effet, en mars 2021, le GTCNL est parvenu à un consensus, le premier accord des Nations unies sur la cybersécurité en près de six ans, depuis le rapport du GGE de 2015. Le rapport final du GTCNL a confirmé les questions convenues en 2015, a suggéré ce qu'il faut comprendre comme clusters IE, a invité à un accord pour garantir l'intégrité d'Internet et de la chaîne d'approvisionnement des TIC, a demandé la prévention de la prolifération d'outils malveillants et l'utilisation de fonctionnalités malveillantes cachées (c'est-à-dire les backdoors), défini des MDC spécifiques supplémentaires (telles que la désignation de points de contact nationaux) et défini des principes de renforcement des capacités. Le rapport recommandait également que le dialogue institutionnel régulier se poursuive sous les auspices de l'ONU, y compris le GTCNL 2021-2025, avec une participation égale des États, tout en ouvrant également la porte à d'autres types et formats de processus.

Le GGE n'a pas été renouvelé en 2021 et le GTCNL 2021-2025 reste le seul format actif de dialogue institutionnel au sein de l'ONU.

Point de réflexion

Selon M. Abdul-Hakeem Ajijola (président du groupe d'experts de l'Union africaine sur la cybersécurité (AUCSEG) et commissaire de la Commission mondiale pour la sécurité du cyberespace), la communauté internationale élabore des normes et celles-ci auront des conséquences pour l'Afrique. Par conséquent, il est déterminant que l'Afrique participe aux discussions, s'engageant avec ses partenaires en tant que pair habilité. La cybernétique est aussi solide que le maillon le plus faible, il est donc impératif que l'Afrique ne soit pas ce maillon faible. (Extrait du panel 'Cyber diplomatie en Afrique et transformation numérique', IGF 2021)

Comment mieux inciter les pays africains à participer significativement au dialogue institutionnel et aux autres cybernégociations connexes ?

Laissez votre commentaire ci-dessous.

Contribuer et s'engager

Inscrivez-vous au cours en ligne de Diplo sur la diplomatie de la cybersécurité (apprentissage personnalisé et facilité en petits groupes), avec quatre modules : impact stratégique de la cyber(in)sécurité, questions à l'ordre du jour diplomatique (droit international, normes, mesures de confiance et renforcement des capacités, infrastructures essentielles, chaîne d'approvisionnement, questions d'attribution, liens avec les droits de l'homme et le développement), rôles des différents acteurs, cartographie des processus multilatéraux et multipartites et préparation d'un État pour la cyberdiplomatie.

Inscrivez-vous à la formation en ligne de l'UNODA sur la cyberdiplomatie (cours à votre rythme), comprenant cinq piliers : menaces existantes et émergentes ; droit international ; normes, règles et principes ; mesures de confiance ; coopération internationale et assistance au renforcement des capacités.

Mobilisez votre ministère des Affaires étrangères à participer activement au dialogue institutionnel et aux autres processus liés à la cybersécurité.

3.1.2 Processus à venir

Il existe cependant des points de vue et des positions différents sur la façon dont le dialogue institutionnel devrait se présenter à l'avenir. Par exemple, certains appellent à un processus à long terme plutôt qu'à un mandat limité à quelques années, comme c'est actuellement le cas pour le GTCNL. Une autre question ouverte est le mandat du futur dialogue : doit-il se concentrer sur la mise en œuvre des normes, des mesures de confiance et des mesures de renforcement des capacités déjà convenues, ou doit-il (également) développer de nouvelles normes et mesures ? Et doit-il élargir la liste des sujets à l'ordre du jour, ou rester concentré sur les questions de paix et de sécurité puisque le dialogue se déroule sous la Première Commission de l'ONU ?

Une proposition concrète pour répondre à certaines de ces questions est déjà présentée par la France et l'Égypte, avec le soutien de 40 autres États ; une proposition de programme d'action (PA) en tant que processus à long terme et inclusif. Le PA devrait créer un cadre et un engagement politique basé sur le Cadre, avec des réunions annuelles régulières au niveau du travail axées sur la mise en œuvre du cadre existant et des conférences d'examen périodiques pour déterminer si des normes supplémentaires doivent être élaborées. Le rapport final du GTCNL 2021 désigne les PA comme une possibilité de dialogue institutionnel futur.

Il est particulièrement important de savoir s'il est nécessaire d'établir un quelconque traité sur le cyberespace. Six pays de l'Organisation de coopération de Shanghai (OCS) ont proposé un code de conduite international pour la sécurité de l'information à l'ONU en 2011 et à nouveau en 2015. La proposition prévoyait que le code de conduite couvrirait plus que le simple cyberconflit, y compris des dispositions sur la guerre de l'information dans le

cyberespace et d'autres questions de gouvernance de l'internet, la surveillance, la politique de contenu et la souveraineté. Les États-Unis, l'UE et leurs partenaires ont fermement résisté à de telles initiatives, soutenant qu'elles introduiraient une plus grande censure et un contrôle du contenu Internet dans les pays du monde entier. Étant donné que le GTCNL des Nations Unies est ouvert à tous les États, la question d'un traité ou d'une convention contraignants est abordée dans le cadre de la discussion sur le futur dialogue institutionnel.

Il est important de mentionner, cependant, un autre processus important qui se distingue du dialogue relatif à la paix et à la sécurité, mais qui peut l'influencer indirectement. La résolution de l'ONU sur la lutte contre l'utilisation des TIC à des fins criminelles, adoptée en 2019, a créé la commission internationale ad hoc à composition non limitée d'experts (connu sous le nom de commission ad hoc) dans le cadre de la Troisième Commission de l'ONU, chargée d'élaborer un nouveau traité sur la cybercriminalité. La commission ad hoc devrait fournir un projet de convention à l'Assemblée générale des Nations unies en août 2023. L'une des principales questions de ces négociations porte sur la cohérence de l'éventuelle convention mondiale avec la Convention sur la cybercriminalité du Conseil de l'Europe (dite Convention de Budapest) de 2001. Une autre question est de savoir comment préserver les droits de l'homme tout en répondant aux exigences d'une plus grande souveraineté des États dans le cyberespace.

Contribuer et s'engager

Pour en savoir plus sur la cybercriminalité ainsi que les problèmes et processus connexes, ainsi que sur les opportunités de renforcement des capacités, reportez-vous au module de connaissances 3.

3.2 Autres instances multilatérales

- *Quels autres principaux processus diplomatiques et politiques ont des composants de cybersécurité à l'ordre du jour ?*

Les processus diplomatiques et politiques qui ne sont pas axés sur la cybersécurité prennent également de plus en plus en compte les aspects de la cybersécurité.

Le cyberespionnage est apparu à l'ordre du jour du G20, un groupe de 20 grandes puissances économiques, en 2015, lorsqu'il a convenu « qu'aucun pays ne devrait mener ou soutenir le vol de propriété intellectuelle, y compris les secrets d'affaires ou d'autres informations commerciales confidentielles, avec l'intention de fournir des avantages compétitifs aux entreprises ou aux secteurs commerciaux » (G20, 2015, art. 26). Le groupe de travail du dialogue sur la cybersécurité du G20, dans le cadre du groupe de réflexion sur l'économie numérique du G20, est un lieu de discussion multipartite et intersectorielle sur la sécurité dans le contexte de l'économie numérique, comme l'échange de bonnes pratiques nationales. En outre, le G20 Osaka Track, lancé en 2019, a intensifié les efforts internationaux d'élaboration de règles dans l'économie numérique, en particulier sur les flux de données et le commerce électronique, tout en promouvant des protections renforcées pour la propriété intellectuelle, les informations personnelles et la cybersécurité.

De même, par le passé, le Groupe des Sept (G7) a réfléchi à la nécessité d'un comportement responsable des États dans le cyberespace et, en particulier, à sa pertinence pour le vol de propriété intellectuelle et le cyberespionnage économique.

L'Organisation mondiale du commerce (OMC), dans le cadre de ses négociations plurilatérales sur le commerce électronique menées dans le cadre de l'Initiative conjointe (JSI), promeut la cybersécurité comme l'une des questions à son ordre du jour. En conséquence, les discussions sur la cybersécurité se sont concentrées sur le renforcement des capacités nationales de réponse aux incidents, l'encouragement de la coopération et la promotion du partage d'informations (JSI Focus Group D), mais ont également pris en compte les flux de données transfrontaliers (Focus Group B) et l'authentification électronique (Focus Group A).

Le Forum mondial sur la sécurité numérique pour la prospérité de l'Organisation de coopération et de développement économiques (OCDE) offre un cadre multilatéral et multidisciplinaire qui, depuis 2018, rassemble des experts et des décideurs pour partager des expériences et de bonnes pratiques en ce qui concerne la sécurité numérique et discuter des enjeux économiques et aspects sociaux de la cybersécurité. En outre, le groupe de travail de l'OCDE sur la sécurité et la vie privée dans l'économie numérique (SPDE) rassemble les acteurs pour élaborer des recommandations politiques de haut niveau, telles que celles liées à la sécurité des technologies et des produits numériques.

3.3 Initiatives régionales

- *Quels sont les principaux instruments développés au niveau régional ?*
- *Comment ces outils peuvent-ils aider les développements africains ?*

3.3.1 L'OSCE

Des initiatives diplomatiques au sein de plusieurs organisations régionales visent à formuler des mesures de confiance pour le cyberespace afin de renforcer la coopération et de prévenir les malentendus et les conflits éventuels. L'ensemble de mesures de confiance visant à réduire le risque de conflit découlant de l'utilisation des TIC, adopté en 2013 (décision n° 1106) et prorogé en 2016 (décision n° 1202), par l'Organisation pour la sécurité et la coopération en Europe (OSCE), est particulièrement important. La décision décrit les mesures que les États participants sont invités à suivre volontairement, notamment : partager les points de vue nationaux sur les menaces et les meilleures pratiques ; coopérer avec les organismes nationaux compétents ; consulter pour réduire les risques de perception erronée et les éventuels tensions ou conflits ; renforcer la législation nationale pour permettre le partage d'informations ; partager et discuter de la terminologie nationale liée à la cybersécurité ; coopérer à la protection des infrastructures essentielles ; divulguer les vulnérabilités ; promouvoir les partenariats public-privé ; et impliquer le secteur privé, les universités, les centres d'excellence et la société civile dans les mesures de cybersécurité.

Contribuer et s'engager

Inscrivez-vous au cours en ligne de l'OSCE sur les mesures de confiance en matière de cyber/sécurité des TIC (apprentissage à votre rythme), avec trois modules : un bref aperçu des quatre piliers du cadre international pour la stabilité dans le cyberespace et les rôles des organisations régionales, le développement du cyber/de la sécurité des TIC dans l'OSCE et les 16 MDC, et un examen plus approfondi de chacunes des 16 cyber MDC individuellement, avec un accent particulier sur la mise en œuvre pratique.

3.3.2 ASEAN et ARF

Le Forum régional de l'ASEAN (FRA) a suivi l'exemple de l'OSCE avec son programme de travail de 2015 sur la sécurité et l'utilisation des technologies de l'information et des communications, qui fait suite à la déclaration de 2012 des ministres des Affaires étrangères de l'ASEAN. En 2018, les pays de l'ASEAN ont convenu qu'un mécanisme officiel de cybersécurité de l'ASEAN pour la cyberdiplomatie et les questions politiques et opérationnelles devrait être établi. Les pays de l'ASEAN ont également décidé de souscrire aux 11 normes volontaires et non contraignantes recommandées en 2015 par le GGE de l'ONU, ainsi que de se concentrer sur le renforcement des capacités régionales dans la mise en œuvre de ces normes. Le Cyber Programme ONU-Singapour (UNSCP) a été lancé, axé sur les cybernormes, la sensibilisation et la planification de scénarios cyberpolitiques. En 2020, les ministres de l'ASEAN ont en outre convenu d'élaborer un plan d'action régional de cybersécurité à long terme pour mettre en œuvre les normes. S'appuyant sur l'organigramme des normes que les pays de l'ASEAN ont élaboré en 2019, Singapour et le Bureau des affaires de désarmement des Nations Unies (UNODA) ont convenu d'établir une liste de contrôle pour la mise en œuvre des normes, la rendant applicable à un plus large éventail d'États membres de l'ONU.

En Asie, le Forum régional (FRA) de l'Association des nations de l'Asie du Sud-Est (ASEAN) aborde également les mesures de confiance en matière de cybersécurité et de lutte contre la cybercriminalité. En 2012, le FRA a présenté une déclaration ministérielle intensifiant la coopération régionale sur la sécurité des TIC (FRA, 2012). En 2017, l'ASEAN a adopté une stratégie de coopération en matière de cybersécurité, qui guide l'organisation et ses États membres dans une approche coordonnée pour renforcer leurs capacités en matière de cybersécurité. En outre, le Centre d'excellence en cybersécurité ASEAN-Singapour et le Centre de renforcement des capacités en matière de cybersécurité ASEAN-Japon ont été créés pour augmenter le niveau d'expertise en matière de cybersécurité.

3.3.3 L'OEA

En 2018, l'OEA a adopté une résolution soulignant la nécessité de préparer et de convenir d'un ensemble de mesures de confiance pour le cyberespace, et commençant par les deux mesures volontaires : partager des informations sur les politiques de cybersécurité et identifier un point de contact national au niveau politique. En 2019, quatre mesures de confiance supplémentaires ont été recommandées, notamment la désignation de points de contact dans les ministères des Affaires étrangères et le renforcement des capacités en matière de cyberdiplomatie.

L'Organisation des États américains (OEA) a établi la *Stratégie interaméricaine de cybersécurité* en 2003. Cette stratégie regroupe les initiatives de trois groupements connexes de l'organisation : le Comité interaméricain contre le terrorisme (CICTE), les ministres de la Justice ou d'autres ministres ou procureurs généraux des Amériques (REMJA) et la Commission interaméricaine des télécommunications (CITEL). Ces groupes travaillent avec les États membres pour mettre en œuvre des programmes qui préviennent la cybercriminalité et protègent les IE par des mesures législatives et d'autres mesures procédurales. La REMJA encourage la coopération dans la lutte contre la cybercriminalité par le biais de son Groupe de travail sur la cybercriminalité et du Portail interaméricain de coopération sur la cybercriminalité. D'autres déclarations de l'OEA – Renforcer la cybersécurité dans les Amériques en 2012 et la Déclaration sur la protection des infrastructures essentielles contre les menaces émergentes en 2015 – et la Déclaration du CICTE sur le renforcement de la coopération et du développement continental en matière de cybersécurité et de lutte contre le terrorisme dans les Amériques, ont renouvelé l'engagement de l'OEA envers la cybersécurité régionale.

3.3.4 Afrique

La Convention de l'Union africaine sur la cybersécurité et la protection des données à caractère personnel (connue sous le nom de Convention de Malabo), adoptée en 2014, fournit un cadre juridique pour la promotion de la cybersécurité, la lutte contre la cybercriminalité, la conduite du commerce électronique et la protection des données personnelles. Cependant, son influence sur les cadres juridiques nationaux reste limitée à ce jour, puisque seuls 19 des 55 États membres l'avaient signée ou ratifiée à la mi-2020.

Bien qu'il n'y ait pas de MDC régionales, de nombreuses initiatives de cybersécurité et de cyberdiplomatie sont déployées aux niveaux régional et sous-régional : le Groupe d'experts en cybersécurité (AUCSEG), le fleuron de l'Agenda 2063 de l'UA, l'Initiative politique et réglementaire pour l'Afrique numérique (PRIDA), le Programme de développement des infrastructures pour l'Afrique (PIDA), la Stratégie de transformation numérique pour l'Afrique, l'Alliance Smart Africa, la stratégie de cybersécurité de la CEDEAO et le plan d'action de la SADC sur la cybersécurité. « Africa as a Cyber Player », une recherche menée par l'ISS de l'UE ans le cadre de l'initiative Cyber Direct de l'UE, donne un bon aperçu des principaux acteurs et instruments du continent, dans les domaines de la cybersécurité et de la cyberdiplomatie.

Point de réflexion

Dans son mémoire de Master « Négociations diplomatiques internationales sur la cybersécurité : le rôle de l'Afrique dans la coopération interrégionale pour une approche mondiale de la sécurité et de la stabilité du cyberespace », Mme Souhila Amazouz suggère que, pour accélérer le processus de ratification de la Convention de Malabo au sein des pays membres de l'UA, la CUA doit faire remonter la question au niveau du Comité ministériel sur les défis de la ratification/adhésion et de la mise en œuvre des traités de l'UA, et engager des réflexions pour trouver le moyen approprié de transposer les dispositions de la convention de Malabo dans les lois nationales afin d'harmoniser les cadres de cybersécurité au niveau continental. Elle suggère également que les pays africains devraient

se soucier d'intégrer la cybersécurité dans leurs politiques étrangères et de sécurité, ainsi que dans le développement de leur stratégie numérique.

Quelles mesures pourraient amener à une meilleure adoption de la cybersécurité en tant que problème parmi les ministères africains des Affaires étrangères, et par conséquent leur rôle dans l'élaboration des instruments africains et mondiaux ?

Laissez votre commentaire ci-dessous.

Ressources

Le Forum mondial sur la cyber expertise (GFCE) fournit un « Aperçu des mesures de renforcement de la confiance existantes appliquées au cyberespace ». Le document « Vers un cyberespace sécurisé via la coopération régionale » de la Geneva Internet Platform propose une analyse comparative des domaines thématiques couverts par les normes cyber, les MDC et les mesures de renforcement des capacités par les organisations régionales.

3.4 Initiatives multipartites

- *Quelle est l'utilité des discussions multipartites pour les initiatives de cyberdiplomatie ?*
- *Quelles sont les instances multipartites les plus pertinentes avec lesquelles les États africains devraient dialoguer ?*

3.4.1 Forum sur la gouvernance de l'Internet

Le Forum des Nations Unies sur la gouvernance de l'Internet (IGF) est un forum non décisionnel qui implique une variété d'acteurs pour discuter ouvertement des questions de gouvernance de l'Internet, y compris la sécurité et la confidentialité. Bien que l'IGF ne prenne pas de décisions ou ne formule de recommandations, il offre la possibilité d'un dialogue et d'un partenariat ouverts, d'échanges d'informations et d'orientations politiques volontaires utiles par le biais du Forum des meilleures pratiques (BPF) sur la cybersécurité, de la Coalition dynamique (CD) sur les normes Internet, la sécurité et Sécurité (CD-ISSS), et les rapports des sessions thématiques tenues chaque année. En outre, la feuille de route du secrétaire général pour la coopération numérique envisage un rôle renforcé pour l'IGF (appelé IGF+) dans la coopération numérique mondiale et la création d'un organe multipartite de haut niveau au sein de l'IGF, qui travaillera à concrétiser les discussions en résultats, renforçant l'importance de l'IGF pour des discussions coordonnées sur la cybersécurité.

Ressources

Les BPF offrent à la communauté IGF des moyens substantiels de produire des résultats plus concrets. Grâce à un dialogue et des échanges ouverts, BPF Cybersecurity a élaboré un certain nombre de rapports pertinents :
- Exploration des meilleures pratiques en relation avec les initiatives internationales de cybersécurité (2020)
- BPF Cybersecurity sur les accords internationaux de cybersécurité (2019)
- Culture, normes et valeurs de la cybersécurité (2018)
En 2021, le BPF s'est tourné vers le test des normes existantes par rapport aux événements historiques de cybersécurité.

Contexte africain

Le Forum africain sur la gouvernance de l'Internet (AfIGF) a été officiellement reconnu par les ministres des TIC comme une plate-forme continentale nécessaire, le Secrétariat étant hébergé par la CUA. Il organise des événements annuels pour discuter d'un large éventail de questions de gouvernance de l'Internet, y compris la cybersécurité, avec de multiples intervenants. En outre, toutes les cinq régions d'Afrique ont mis en place des IGF sous-régionaux, afin de rassembler les IGF nationaux et de promouvoir les dialogues politiques locaux. Selon l'IGF des Nations Unies, 30 pays africains ont établi leur IGF national.

3.4.2 Le GFCE

Le Forum mondial sur la cyber expertise (GFCE) est une plateforme rejointe par 60 pays et de nombreuses organisations internationales et régionales, entreprises et organisations de la société civile pour collaborer au renforcement des capacités en matière de cybersécurité. Le communiqué de Delhi sur un programme mondial du GFCE pour le renforcement des cybercapacités, adopté en 2017, a défini plusieurs domaines prioritaires pour le renforcement des capacités mondiales et a permis au GFCE de créer des groupes de travail thématiques correspondants pour la coopération de ses membres et partenaires. Ces domaines prioritaires comprennent l'élaboration de cadres nationaux, l'intervention en cas d'incident et la protection des IE, la lutte contre la cybercriminalité et le développement d'une culture et de compétences en matière de cybersécurité. En outre, le GFCE vise à établir un « mécanisme d'échange d'informations » pour permettre à ses membres d'obtenir tout soutien nécessaire de la part d'autres membres. Pour schématiser son travail et les connaissances mondiales disponibles, les ressources et les activités de renforcement des capacités dans le domaine de la cybersécurité, le GFCE a lancé son portail de connaissances CyBil.

3.4.3 Appel de Paris

En collaboration avec le gouvernement français, Microsoft a lancé l'Appel de Paris pour la confiance et la sécurité dans le cyberespace, une déclaration de haut niveau sur le développement de principes communs pour la sécurisation du cyberespace. L'Appel de Paris a été signé par plus de 80 pays et plus de 1 000 entreprises et organisations dans le

monde. L'Appel a affirmé l'importance des normes volontaires de comportement responsable des États pour la cybersécurité, en s'appuyant sur les normes GGE 2015 et les normes GCSC.

3.4.4 La GCSC

La Commission mondiale sur la stabilité du cyberespace (GCSC), un groupe de réflexion multipartite créé en 2015, a proposé un ensemble de nouvelles normes à examiner par divers forums, tels que le GGE. Les propositions comprennent l'Appel à protéger le noyau public d'Internet, un Appel à la défense des processus électoraux et l'ensemble de six normes de Singapour qui demandent aux États d'éviter d'altérer les produits, de créer des processus d'actions de vulnérabilité et d'atténuer les faiblesses importantes, d'améliorer la cyberhygiène, et de s'abstenir d'utiliser des botnets ou de mener des opérations offensives par l'intermédiaire d'acteurs non étatiques. Ces normes sont destinées à compléter les normes élaborées dans le cadre de l'ONU.

3.4.5 Le FOC

La Coalition pour la liberté en ligne (FOC) s'emploie à rehausser le profil des droits de l'homme en tant que considération intégrale dans l'élaboration des politiques de cybersécurité. Le FOC a publié une déclaration conjointe concernant une approche de l'élaboration des politiques de cybersécurité fondée sur les droits de l'homme et a fourni une définition de la cybersécurité « la préservation ; par la politique, la technologie et l'éducation ; de la disponibilité, de la confidentialité et de l'intégrité des informations et de leur infrastructure sous-jacente afin d'améliorer la sécurité des personnes en ligne et hors ligne ».

4 Cyber diplomatie

La numérisation et les sujets connexes ont touché presque tous les aspects de la politique étrangère. Ce n'est pas une prise de conscience récente, mais les ministères des Affaires étrangères n'ont que récemment commencé à aborder ce problème de manière plus globale. Ainsi, nous assistons aujourd'hui à l'émergence d'une « politique étrangère numérique », en particulier de *stratégies* de politique étrangère numérique qui offrent un aperçu complet des approches des pays sur les sujets, les acteurs et les processus numériques, et à la création de cyber départements et portefeuilles au sein des ministères des Affaires étrangères.

Ressources

« Améliorer la pratique de la cyberdiplomatie : formation, outils et autres ressources », une recherche développée par le GFCE et Diplo, explique qui sont les spécialistes de la cyberdiplomatie, où la cyberdiplomatie est exécutée et quels sont les pays les plus actifs et les plus inactifs. L'étude schématise également les formations, outils et autres ressources disponibles, ainsi que la manière dont ils aident les diplomates à s'intéresser à la cyberdiplomatie. Il est important de noter que l'étude présente également les résultats d'une

enquête et analyse l'importante utilisation de ces outils et ressources par les diplomates du monde entier, en mettant l'accent sur les pays et les régions qui ne sont pas aussi actifs dans la cyberdiplomatie.

À travers plusieurs entretiens vidéo thématiques, les cyber-représentants examinent la portée de la cyber-diplomatie, l'inclusivité et les rôles des acteurs, ainsi que les compétences à développer pour la cyber-diplomatie. Font partie des entretiens :

- Amb. Nathalie Jaarsma (Ambassadrice itinérante pour la politique de sécurité et la cybersécurité, Pays-Bas)
- M. Chris Painter (Président, Fondation du Forum mondial sur la cyber expertise (GFCE))
- Amb. Tobias Feakin (Ambassadeur pour les cyberaffaires et les technologies essentielles, Australie)
- M. David Koh (Commissaire à la cybersécurité et directeur général de la Cyber Security Agency de Singapour)
- Amb. Asoke Mukerji (ancien Ambassadeur d'Inde)

4.1 Objectifs

- *La cyberdiplomatie concerne-t-elle uniquement la cybersécurité ?*

Expériences partagées par M. Painter, Mme Jaarsma et M. Feakin :
La cyberdiplomatie derrière la sécurité (vidéo)

4.2 Inclusivité et rôles des acteurs

- *Quel rôle jouent les acteurs non étatiques dans la cyberdiplomatie, notamment au niveau régional ?*
- *Pourquoi l'inclusion des acteurs est-elle importante pour parvenir à des accords significatifs ?*

Expériences partagées par M. Koh :
Processus régionaux et rôle des acteurs (M. Koh) (vidéo)

Expériences partagées par Amb. Mukerji :
Inclusivité et éventuels accords (Amb Mukerji) (vidéo)

4.3 Ensembles de compétences

- *Quelles sont les compétences requises par les cyberdiplomates ?*
- *De quelles compétences les autres acteurs ont-ils besoin pour contribuer aux cyberprocessus ?*
- *(Pourquoi et comment) les diplomates et les non-diplomates devraient-ils travailler ensemble ? Quel est le rôle des autres acteurs ?*

Expériences partagées par Amb. Jaarsma et Amb. Feakin :
Ensemble de compétences pour les cyberdiplomates (vidéo)

Expériences partagées par M. Painter, Amb. Mukerji, et M. Koh :
Ensemble de compétences pour les non-cyberdiplomates (vidéo)

Expériences partagées par M. Koh Amb. Mukerji :
Diplomates et non-diplomates qui travaillent ensemble (vidéo)

Contribuer et s'engager

Collaborez avec le groupe de travail A du GFCE, en particulier son groupe de travail 2 sur la cyberdiplomatie, pour partager vos points de vue sur la question et aider à façonner d'autres ressources, guides pratiques et activités de renforcement des capacités.

Contribuez au portail CyBil en soumettant des informations sur les ressources, les guides pratiques et les activités disponibles en Afrique.