COMITÉ : UIT - Cybersécurité
PROBLÉMATIQUE : Dans quelle mesure les États peuvent-ils développer des stratégies nationales de cyberdéfense efficaces contre les attaques visant les infrastructures critiques, sans pour autant freiner la coopération internationale ?
PRÉSIDENTS : Anouchka WEISROCK, Indri SELIMI et Hicham FOFANA

PRÉSENTATION DU PRÉSIDENT

Bonjour à toutes et à tous !
Je m'appelle Indri SELIMI, j'ai 16 ans et je suis en classe de première. C'est un immense honneur pour moi de vous accueillir en tant que délégués au sein de notre comité sur la cybersécurité pour ce FerMUN 2027.
Passionné et engagé dans le sport, et plus particulièrement dans le journalisme footballistique, j'ai appris l'importance du collectif, de la stratégie et du respect. Ce sont ces mêmes valeurs, combinées à mon intérêt pour les droits humains et la diplomatie, qui me passionnent aujourd'hui dans les questions de sécurité internationale. L'année dernière, j'ai eu la chance de vivre l'aventure FerMUN, à votre place, en tant que délégué. C'est un rôle exigeant, mais gratifiant, et je suis convaincu que vous saurez le porter à la perfection tout en y prenant un plaisir immense.
Lors de cette conférence, notre comité se penchera sur un sujet d'une importance majeure et d'une grande actualité : la stratégie nationale de cyberdéfense. Nous avons tendance à l'oublier, mais derrière les écrans et les lignes de code, la cybersécurité est avant tout une question de droits humains et de protection des vies. Chaque année, les attaques contre nos hôpitaux, nos réseaux électriques ou nos services publics se multiplient, touchant directement le quotidien de millions de citoyens.
Le défi qui vous attend est magnifique : comment s'unir et coopérer à l'échelle internationale pour protéger nos peuples, sans que les États n'aient l'impression de sacrifier leur souveraineté ? Avant tout, je vous conseille de visionner cette vidéo d'une minute pour comprendre concrètement les enjeux d'une cyberattaque. Je suis impatient de découvrir vos idées, de voir votre talent et de vous guider dans ce débat passionnant. Bonne préparation à tous, et à très vite !

MOTS-CLÉS

Stratégie nationale : Une stratégie nationale désigne l'ensemble des plans d'action, des lois et des ressources qu'un gouvernement coordonne à l'échelle de son territoire pour atteindre un objectif de sécurité majeur. *(Source : Union internationale des télécommunications)*

Cyberdéfense : La cyberdéfense consiste à déployer l'ensemble des moyens techniques, organisationnels et militaires nécessaires pour protéger les systèmes d'information d'un pays et repousser les attaques dans l'espace virtuel. (Source : Union internationale des télécommunications - UIT)

Cyberattaques : Une cyberattaque désigne une action malveillante menée via les technologies de l'information pour pirater, saturer, voler des données ou détruire des systèmes numériques ciblés. (Source : Groupe d'experts gouvernementaux des Nations Unies - GGE)

Infrastructures critiques : Une infrastructure critique désigne l'ensemble des installations indispensables au bon fonctionnement d'un pays, dont la perturbation grave impacterait la santé, l'économie ou la sécurité des citoyens (ex: centrales électriques, hôpitaux, réseaux d'eau). (Source : Assemblée générale des Nations Unies)

Coopération internationale : La coopération internationale désigne
une collaboration entre des gouvernements, des entreprises ou des individus qui ont convenu de travailler ensemble sur des points similaires dans certains sujets. (Source : GEMET/ODE)

Souveraineté numérique : Concept selon lequel un État affirme son autorité et son contrôle absolu sur les infrastructures physiques, les données, les réseaux et les technologies d'information situés sur son territoire national. (Source : Assemblée générale des Nations Unies)

Interpol : Organisation internationale de police criminelle qui facilite la coopération policière transfrontalière et l'échange de données criminelles sécurisées en temps réel (notamment via le réseau I-24/7) pour traquer la cybercriminalité mondiale. (Source : OIPC-Interpol)

Attribution : Processus juridique et technique extrêmement complexe visant à désigner avec précision et preuves le responsable direct (individu, groupe non étatique ou État tiers) à l'origine d'une cyberattaque. (Source : UN Digital Watch)

Cybercriminalité : Activités criminelles réalisées au moyen d'ordinateurs ou de réseaux informatiques, englobant les infractions contre la confidentialité, l'intégrité et la disponibilité des données, ainsi que l'utilisation de serveurs étrangers pour blanchir des fonds ou lancer des attaques. (Source : Conseil de l'Europe, Convention de Budapest)

Résilience (numérique) : Capacité d'un système informatique ou d'une infrastructure d'importance vitale à résister à une cyberattaque, à absorber le choc tout en maintenant ses fonctions essentielles, et à restaurer rapidement son activité normale. (Source : Global Forum on Cyber Expertise - GFCE)

Cyberespace : Environnement virtuel complexe résultant de l'interconnexion mondiale de systèmes informatiques, d'infrastructures de télécommunication et d'utilisateurs, reconnu aujourd'hui comme un domaine opérationnel à part entière au même titre que la terre, la mer et l'air. (Source : UIT)

Dispositifs d'alerte (CIRT/CERT/CSIRT) : Centres d'alerte et de réponse aux incidents informatiques chargés de surveiller continuellement les réseaux, de diffuser en temps réel des correctifs de sécurité et de coordonner l'intervention technique d'urgence lors d'une cyberattaque majeure. (Source : UIT)

Données : Toute représentation d'informations, de faits ou de concepts sous une forme propre à être traitée par des moyens informatiques. Leur intégrité, leur protection et leur confidentialité constituent l'enjeu majeur de la cyberdéfense civile et étatique. *(Source : Agence des Nations Unies pour les TIC)*

APERÇU GLOBAL

Une nouvelle stratégie de cyberdéfense

Les infrastructures numériques sont devenues essentielles au fonctionnement de notre société moderne, aujourd'hui profondément dépendante des technologies. En effet, près de 75% de la population mondiale dispose aujourd'hui d'un accès à internet.[1] Cette augmentation massive et continue souligne la nécessité absolue de protéger les citoyens et les États face à la multiplication des cyberattaques. En France, en 2023, l'ANSSI a traité plus de 3 800 incidents de sécurité et plus de 1 000 cyberattaques majeures en une seule année, ciblant des hôpitaux, des collectivités locales et des entreprises stratégiques[2].[2]

Dès lors, renforcer la cyberdéfense et sécuriser les infrastructures critiques, comme les réseaux électriques ou les systèmes de santé est crucial pour la sécurité nationale et la stabilité économique de chaque nation. Tout l'enjeu de notre comité sera donc de répondre à la question suivante : dans quelle mesure les États peuvent-ils développer des stratégies nationales de cyberdéfense efficaces contre les attaques visant les infrastructures critiques, sans pour autant freiner la coopération internationale ?

I - Failles et évolution des menaces

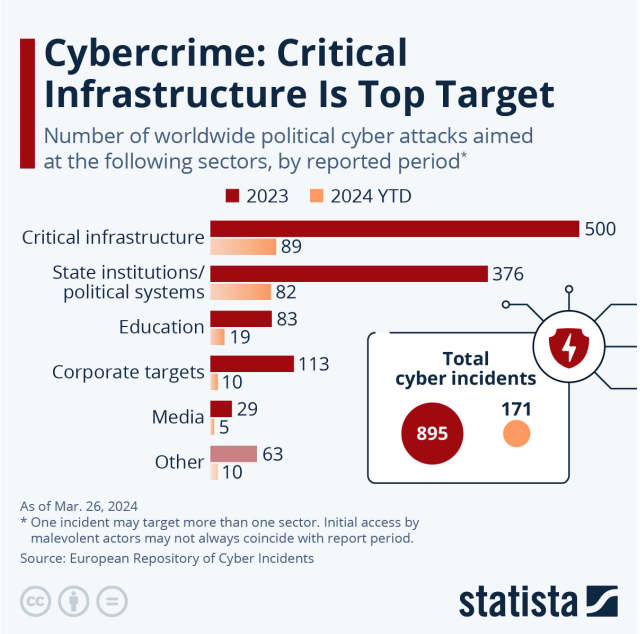
A - La dépendance critique des services vitaux

Aujourd'hui, le fonctionnement d'une grande partie de nos activités socio-économiques repose de manière croissante sur l'utilisation des TIC (Technologies de l'Information et de la Communication). Dans ce contexte, le renforcement des capacités nationales en matière de cybersécurité constitue un levier clé pour accroitre la résilience des infrastructures et favoriser la confiance des utilisateurs, contribuant ainsi à réduire les vulnérabilités au sein de l'espace numérique.

En effet, cette dépendance pose des défis majeurs : elle rend nos infrastructures vitales extrêmement vulnérables, les hôpitaux ou les réseaux d'énergie se retrouvant en première ligne. Une cyberattaque dépasse largement la simple coupure d'Internet : elle peut paralyser des services vitaux. L'attaque par rançongiciel WannaCry, qui a bloqué plus de 80 établissements de santé du NHS au Royaume-Uni en annulant des milliers de soins et d'interventions, ou les cyberattaques contre le réseau électrique ukrainien (*BlackEnergy*),

[1] Selon l'Union Internationale des Télécommunications (UIT), *Faits et chiffres sur le développement des télécommunications / TIC*.
[2] Selon le rapport Panorama de la cybermenace de l'Agence nationale de la sécurité des systèmes d'information (ANSSI).

ayant privé des centaines de milliers de citoyens d'électricité, en sont des illustrations claires. La sécurisation de ces systèmes ne relève donc plus d'un arbitrage technique secondaire, mais constitue un pilier fondamental de la sécurité nationale que chaque État doit inscrire au cœur de sa stratégie de cyberdéfense.



Comme le démontre le graphique de Statista ci-dessus, les infrastructures critiques sont devenues les cibles privilégiées des cyberattaques. Ce phénomène montre la fragilité de nos services essentiels qui manquent de sécurité et de modernité face à la numérisation croissante. En ciblant massivement les secteurs de la santé, des transports ou de l'énergie plutôt que de simples entreprises privées, les cyberattaquants peuvent avoir comme objectifs d'engendrer une paralysie de ces services vitaux, d'extorquer des fonds ou d'extraire des données stratégiques.

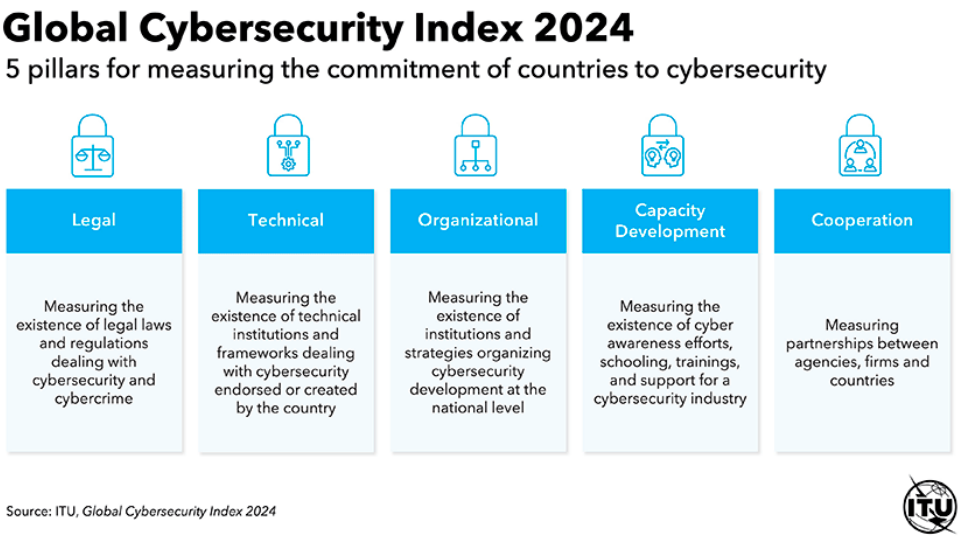
À l'heure actuelle, la dépendance aux technologies anciennes crée une réaction en chaine où un incident virtuel peut engendrer de lourdes conséquences au sein de la population. Face à cela, la concentration des attaques sur ces réseaux stratégiques prouve que la sécurité des services vitaux n'est plus un problème sectoriel, mais un des problèmes majeurs de la sécurité collective. Ce constat statistique force le comité à repenser d'urgence la protection des piliers de notre vie quotidienne pour garantir la continuité des États.

B - Des outils anciens face à des technologies de pointe

Actuellement, une part majeure des infrastructures d'importance vitale (réseaux d'eau, de distribution d'énergie ou transports) repose sur des systèmes hérités (*legacy systems*), notamment des systèmes de contrôle industriel (SCADA) et des automates conçus il y a plusieurs décennies. Ces équipements n'ont pas été développés pour être raccordés à Internet ni pour faire face à des cyberattaques. Leur mise à jour ou remplacement génère des coûts considérables et des interruptions de service critiques, retardant ainsi leur sécurisation. Dès lors, les capacités défensives évoluent nettement moins vite que celles des attaquants. Par

exemple, alors que les groupes malveillants automatisent désormais la recherche de failles grâce à l'intelligence artificielle générative[3] et exploitent massivement des vulnérabilités non corrigées (*Zero-Day*[4]), les opérateurs d'infrastructures mettent parfois des mois à déployer un simple correctif. Plutôt que d'envisager un alignement technologique parfait entre tous les États, irréaliste au vu des fractures économiques actuelles, notre comité doit cibler des mécanismes de coopération pragmatiques et de transfert de compétences pour renforcer la résilience minimale de ces systèmes vitaux.

L'infographie ci-dessous, issue de l'UIT, modélise les cinq piliers fondamentaux permettant de mesurer l'engagement d'un État en matière de cybersécurité : juridique, technique, organisationnel, développement des capacités et coopération. Le document présente ainsi les piliers constitutifs d'une cyberdéfense nationale. En pratique, l'adoption d'un cadre législatif solide constitue souvent la première étape pour un État, mais l'analyse montre qu'elle reste insuffisante si le pilier technique fait défaut. Sans institutions et cadres techniques



opérationnels, notamment des équipes d'intervention d'urgence de chaque pays et des outils de détection face à des menaces sophistiquées comme les rançongiciels ciblés, l'exploitation de vulnérabilités *Zero-Day* ou l'usage malveillant de l'intelligence artificielle, la protection réelle des infrastructures critiques et des services vitaux ne peut être garantie.

Le rapport de l'Indice mondial de cybersécurité (GCI) de l'UIT confirme ce décalage technologique. Bien que la majorité des États (177 pays) disposent de lois, l'UIT souligne que le niveau mondial reste faible dans le pilier technique. Actuellement, seuls 110 pays ont un cadre pour adopter des normes de cybersécurité et à peine 139 pays possèdent un système

[3] Microsoft Threat Intelligence & OpenAI, « *Staying ahead of threat actors in the age of AI* »
[4] Google Threat Analysis Group (TAG) & Mandiant, « *Zero-Day Exploitation Report* »

d'alerte technique actif (CIRT). L'UIT rappelle ainsi que s'engager juridiquement ne suffit plus : il faut garantir l'efficacité des efforts par des actions concrètes, ce qui illustre le manque de mise en œuvre sur le terrain par rapport aux mesures adoptées.

De plus, ce déficit de protection a un impact financier majeur : selon le rapport d'IBM Security (*Cost of a Data Breach Report 2024*), le coût moyen mondial d'une violation de données a atteint 4,88 millions de dollars. Pour les petites et moyennes structures, ce coût s'élève en moyenne à plus de 3 millions de dollars, un montant susceptible d'asphyxier durablement leur économie. Ce retard s'explique notamment par des contraintes budgétaires et les vulnérabilités liées aux chaînes d'approvisionnement technologiques, les organisations devant souvent acquérir des outils externes sans pouvoir en vérifier pleinement la sécurité. Il devient alors impératif pour notre comité d'établir des mécanismes de coopération renforcés.

C - L'explosion des tensions internationales et des cyberattaques

Ces dernières années, une explosion des conflits et des tensions internationales s'est fait ressentir à travers le monde. C'est notamment le cas avec la guerre russo-ukrainienne, où le cyberespace est devenu un véritable champ de bataille : des hackeurs parviennent à perturber le fonctionnement des États et à paralyser des infrastructures critiques à l'échelle mondiale. Plus récemment, les tensions au sein du conflit américano-iranien ont confirmé cette dynamique. Selon le CSIS, des groupes de cyberattaquants ont mené des attaques destructrices de type « Wiper » (visant l'effacement total des données) contre des firmes de technologies médicales américaines, ralentissant ainsi les chaînes d'approvisionnement d'équipements médicaux vitaux. En réponse, des piratages ciblant des applications populaires en Iran ont été effectués afin de diffuser des messages de guerre psychologique directement sur les téléphones des citoyens. Ce glissement des hostilités vers le domaine virtuel prouve que la guerre informatique ne se limite plus à l'espionnage, mais impacte directement et concrètement la sécurité des populations civiles.

Ce basculement géopolitique est pris au sérieux par l'ONU et la communauté internationale. Dans le rapport final du Groupe de travail à composition non limitée (OEWG) de l'ONU (2021-2025), l'Assemblée générale rappelle l'urgence de définir des normes et des principes de comportement responsable des États dans le cyberespace. L'objectif est de prévenir l'utilisation des technologies d'information à des fins malveillantes, qu'elles soient menées directement par des acteurs indépendants ou tolérées depuis leur territoire. L'ONU insiste également sur la poursuite de l'examen des risques émergents, notamment pour la protection des infrastructures critiques et des données. Cela témoigne d'une menace en

constante évolution qui exige une coopération renforcée et le respect des engagements internationaux.

II - Les obstacles à une gouvernance et une coopération mondiale

A - Des conflits d'intérêts qui bloquent une coopération mondiale

Ces rivalités géopolitiques s'expriment à travers des approches contrastées de la gouvernance du réseau. D'un côté, les démocraties libérales, notamment les États-Unis et les États membres de l'Union européenne, défendent un modèle multiacteur associant le secteur privé et la société civile. Ce groupe présente toutefois des nuances internes importantes : alors que les États-Unis privilégient une approche très libérale, l'Union européenne impose un cadre réglementaire strict pour garantir sa souveraineté numérique. D'un autre côté, des États comme la Chine et la Russie prônent une souveraineté numérique stricte, axée sur le contrôle gouvernemental des données et des infrastructures. Entre ces orientations, de nombreuses nations émergentes cherchent à équilibrer sécurité nationale et ouverture numérique.

Au-delà de la gouvernance, l'application du droit international dans le cyberespace fait l'objet de désaccords fondamentaux entre les États. Si un consensus existe sur le principe même de son applicabilité, les modalités concrètes divisent la communauté internationale. Les pays occidentaux plaident pour une clarification précise de l'application du droit international humanitaire (DIH) aux cyberconflits. À l'inverse, d'autres nations proposent qu'une telle démarche ne revienne à légitimer la militarisation du cyberespace ou à justifier des ripostes armées au titre de la légitime défense. Leur objectif est de définir le seuil précis à partir duquel un piratage informatique de grande ampleur justifie légitimement une riposte militaire. À l'inverse, la Russie et la Chine freinent activement ces discussions, redoutant que la formalisation de ces règles ne légitime des contrattaques occidentales face aux opérations cyber qui leur sont régulièrement attribuées.

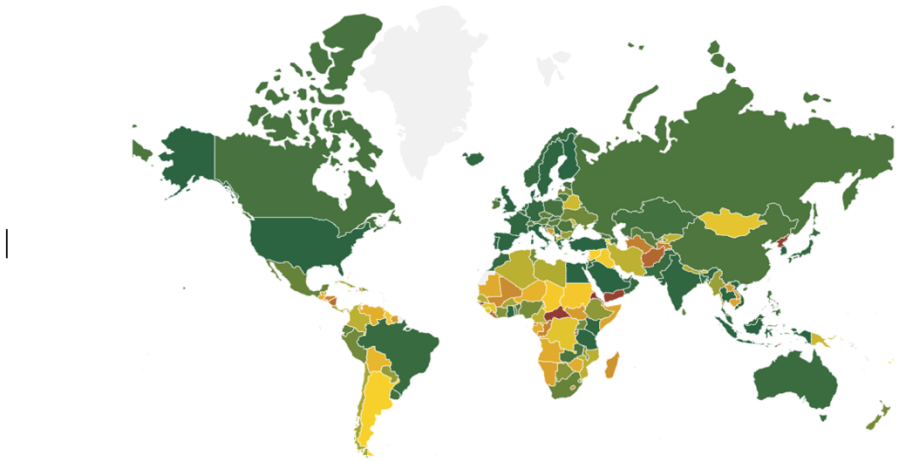
Enfin, le Digital Watch souligne qu'aucune définition commune de la notion de cyberarme n'existe à ce jour. Les grandes puissances refusent catégoriquement de signer des traités de non-prolifération cyber, pour la simple et bonne raison qu'il est techniquement impossible pour des inspecteurs internationaux de vérifier si un pays développé, modifie ou stocke secrètement des codes informatiques malveillants.

B - Le manque de moyens financiers et humains

Au-delà des divergences politiques, la capacité financière et technique constitue un facteur d'inégalité majeur face à la menace cyber. Comme le soulignent les rapports de l'Union internationale des télécommunications (UIT), de nombreux pays, en particulier au sein des

pays les moins avancés (PMA) comme la Centrafrique, ainsi que certains petits États en développement, se heurtent à des contraintes structurelles sévères. Ces nations font face à un déficit simultané de budget, d'expertise spécialisée et d'équipements technologiques de pointe pour répondre à des cyberattaques sophistiquées. Une solution inclusive doit impérativement être trouvée au sein de notre comité afin d'éviter que ce manque de ressources ne freine le développement sécuritaire de ces nations et ne fragilise l'écosystème numérique mondial.

C'est précisément pour répondre à cette fracture que le Global Forum on Cyber Expertise (GFCE) encourage un développement de chaque thème aux niveaux national, régional et mondial, ce qui peut en retour soutenir la cyber-résilience globale du cyberespace, bien au-delà des frontières d'une seule nation. Cela implique un engagement politique au niveau national en faveur de la cybersécurité afin de guider la planification stratégique, l'allocation des ressources et la mise en œuvre, ce qui comprend en général l'élaboration et le déploiement d'une Stratégie nationale de cybersécurité (NCSS). Parallèlement à cet encouragement du développement national, le GFCE soutient le déploiement de systèmes de réponse aux incidents pour prévenir, détecter, dissuader, réagir et se rétablir après des cyber-incidents ; un système qui repose sur des équipes d'intervention d'urgence en sécurité informatique (CERT/CSIRT) dotées de responsabilités nationales.



Carte - Cartographie de l'indice mondial de cybersécurité selon l'UIT (2024)

- **Vert foncé - Niveau 1 (T1 — Modèle) :** Pays ayant obtenu un score global d'au moins 95/100.
- **Vert clair - Niveau 2 (T2 — En progression) :** Pays ayant obtenu un score global d'au moins 85/100.
- **Jaune - Niveau 3 (T3 — En établissement) :** Pays ayant obtenu un score global d'au moins 55/100.
- **Orange - Niveau 4 (T4 — En évolution) :** Pays ayant obtenu un score global d'au moins 20/100.
- **Rouge - Niveau 5 (T5 — En construction) :** Pays ayant obtenu un score global inférieur à 20/100.
- **Gris** - Données non disponibles.[5]

La carte ci-dessus, issue des données du *Global Cybersecurity Index 2024* (GCI) publié par l'Union internationale des télécommunications (UIT), illustre les disparités mondiales dans l'adoption de cadres institutionnels de cybersécurité. Cet indice évalue l'action des États à travers cinq piliers fondamentaux : les législations, les mesures techniques (dont les CSIRT), les cadres organisationnels, la formation et la coopération internationale.

Sur le plan géographique, on constate que la majorité des pays affichant un faible niveau d'engagement réglementaire (Niveaux 4 et 5) se trouvent parmi les pays les moins avancés. Cependant, la carte démontre qu'il ne s'agit pas d'une corrélation économique stricte : des

[5] Union Internationale des Télécommunications (UIT), *Global Cybersecurity Index 2024* / Agence Maurice de Promotion Numérique.

économies émergentes comme l'Égypte, le Maroc ou le Brésil atteignent les niveaux de maturité les plus élevés (Niveaux 1 et 2), au même titre que la France ou l'Arabie saoudite. L'indicateur traduit ainsi avant tout des choix de gouvernance et de structuration juridique, indépendamment de la seule richesse d'un État.

C - L'Impunité numérique et l'absence de sanctions

De nos jours, l'identification des auteurs d'une cyberattaque demeure extrêmement complexe, contrairement aux conflits cinétiques où l'agresseur peut être formellement identifié et sanctionné. Dans le cyberespace, la majorité des offensives souffrent d'un problème d'attribution technique qui rend l'identification certaine difficile, voire impossible. Face à cette opacité et au manque de preuves irréfutables, les procédures judiciaires sont souvent inopérantes et aucune sanction internationale contraignante n'est réellement applicable à ce jour. Cette impunité numérique favorise la persistance des menaces. Il est donc impératif, au sein de notre comité, d'aboutir à une solution commune qui faciliterait l'identification des auteurs et permettrait enfin l'application de sanctions internationales coordonnées.

Le Conseil de l'Europe précise que la cybercriminalité est un crime transnational. Les attaquants ainsi que les preuves se trouvent très souvent dans plusieurs pays différents, ce qui nécessite une coopération internationale. Une coopération qui demeure difficile à l'heure actuelle. Dès lors, un outil juridique existe déjà, c'est le cadre de la Convention de Budapest (Chapitre III). Ce cadre impose aux États de coopérer au maximum en utilisant une assistance mutuelle afin d'obtenir des informations. Le COE insiste également sur l'urgence d'intervenir rapidement pour que les preuves numériques soient encore disponibles et demande la sauvegarde immédiate de ces données dans les pays tiers pour identifier un coupable.

Pour contourner la lenteur juridique, un réseau d'alerte a été mis en place avec un système de communication sécurisée I-24/7 d'Interpol et un réseau d'enquêteurs dans plus de 120 pays. Il est nécessaire pour notre comité de s'inspirer du système européen tout en relevant les défis internationaux et l'amélioration des technologies d'attaques pour se doter d'une solution davantage efficace.



La carte ci-dessus présente l'implantation d'INTERPOL et 194 de ses pays membres. Elle montre l'interconnexion entre le Secrétariat général basé à Lyon (France) et ses bureaux régionaux (Abidjan, Nairobi, Singapour, San Salvador), illustrant le réseau de présence globale de l'organisation.

Ce visuel démontre qu'une structure technique de coopération policière internationale existe déjà pour échanger des renseignements sur la criminalité de droit commun. Cependant, il convient de souligner qu'INTERPOL est un organe de facilitation technique et policière : l'organisation n'a pas vocation à devenir une autorité internationale de sanction. Pour notre comité, l'objectif n'est donc pas de créer un système technique concurrent, mais de renforcer la coopération internationale tout en distinguant impérativement la cybercriminalité (relevant du travail d'INTERPOL) des cyberopérations étatiques (qui relèvent de la souveraineté des États et du cadre normatif des Nations Unies).

TRAITÉS DE L'UIT ET GRANDS ÉVÉNEMENTS

1988 - Création de la Journée internationale de la sécurité informatique : Cette date marque le début de la prise de conscience mondiale des vulnérabilités informatiques, la même année où le tout premier virus d'envergure (le ver Morris) paralysait une partie du réseau Internet. Elle reste aujourd'hui le point de repère annuel pour la cyber-hygiène.

2003 - Sommet mondial sur la société de l'information – Phase de Genève : Ce sommet majeur de l'ONU confie à l'UIT le rôle de chef de file pour la “Ligne d'action C5", entièrement dédiée à la sécurité et à la confiance dans l'utilisation des technologies de l'information. C'est le moment où la cybersécurité entre officiellement dans les missions politiques de l'UIT.

2007 - Lancement du Programme mondial cybersécurité : Sous l'impulsion de son Secrétaire général, l'UIT lance ce projet, qui devient le cadre de coopération mondiale de référence. Il établit les 5 piliers stratégiques que tous les États doivent développer : mesures juridiques, techniques, organisationnelles, renforcement des capacités et coopération internationale.

2010 - Adoption de la Résolution 130 : C'est le premier grand texte politique contraignant au sein de l'UIT. La Résolution 130 donne un mandat permanent à l'organisation pour aider concrètement les pays en développement à créer leurs lois sur la cybercriminalité et à se doter d'équipes d'urgence (les CERT/CSIRT).

2014 - Adoption de la Résolution 174 : Cette nouvelle résolution se focalise spécifiquement sur le rôle de l'UIT concernant les questions de politiques publiques internationales relatives à la sécurité de l'Internet. Elle encadre la protection des données et la vie privée des utilisateurs au niveau des infrastructures mondiales.

2015 - Rapport du GGE de l'ONU : C'est le premier accord mondial où les grandes puissances ont validé ensemble 11 normes de comportement. Ils ont par exemple voté qu'un État ne doit pas attaquer volontairement les infrastructures critiques (hôpitaux, centrales électriques) d'un autre pays en temps de paix.

2018 - Extension de la Résolution 130 : L'UIT adapte ses textes à l'explosion de l'Internet des Objets (IoT) et des premières vagues de cyberattaques massives et mondiales (comme *WannaCry*). Le texte pousse les États à accroître le partage d'alertes techniques en temps réel pour protéger les réseaux de télécommunications nationaux.

2021 - Adoption du rapport final de l'OEWG de l'ONU : C'est l'évènement le plus important de l'histoire récente de l'ONU sur le sujet. Pour la première fois, tous les pays du monde (et pas seulement un petit groupe) ont voté un texte officiel réaffirmant que le droit international classique (la Charte de l'ONU) s'applique pleinement dans le cyberespace.

2022 - Modernisation de la Résolution 130 : L'UIT met à jour son texte fondamental pour intégrer la lutte contre les rançongiciels qui paralysent les infrastructures critiques (hôpitaux, réseaux d'énergie). Elle charge l'UIT de coordonner les exercices de simulation de cyberattaques à l'échelle mondiale pour tester la résilience des États.

2024 - Adoption de la Résolution 50 : Adoptée par l'Assemblée mondiale de normalisation des télécommunications, cette résolution est cruciale : elle ordonne à l'UIT de créer des standards de sécurité obligatoires d'ici la fin de la décennie pour l'intelligence artificielle et les systèmes connectés, afin de bloquer les failles de sécurité directement à la racine.

SOLUTIONS POSSIBLES

Opérationnalisation des recherches d'Interpol : Intégrer un mécanisme juridique permettant d'utiliser les conclusions et les alertes du réseau I-24/7 d'Interpol comme preuves directement recevables devant les tribunaux nationaux, afin de déclencher des mandats d'arrêt internationaux ciblés.

Modernisation de la preuve et des sanctions : Mettre en place un cadre légal international standardisé qui adapte la sévérité des sanctions pénales et financières à la nature des preuves numériques, empêchant les cybercriminels de profiter des vides juridiques entre les frontières.

Fonds global d'équipement cyber : Créer un programme de financement et de transfert technologique, supervisé par l'UIT, pour fournir gratuitement aux pays en développement des outils modernes de détection (logiciels de type EDR/SIEM en open-source) et des formations pour leurs ingénieurs nationaux.

Plateforme d'attribution partagée : Développer une base de données mondiale décentralisée, accessible aux services de cyberdéfense de tous les États membres, pour centraliser, anonymiser et croiser les données sur les modes opératoires des attaquants, facilitant ainsi leur identification technique rapide.

QUESTIONS GUIDÉES

→ Comment contraindre les États souverains à extrader ou à sanctionner les cybercriminels opérant depuis leur territoire lorsque les preuves numériques proviennent d'un réseau tiers comme Interpol ?

→ De quelle manière pouvons-nous assurer un financement pérenne et équitable des infrastructures de cybersécurité dans les pays en développement sans créer une dépendance technologique vis-à-vis des grandes puissances ?

→ Face à la vitesse de propagation d'une cyberattaque, quel mécanisme d'urgence juridique mondial permettrait de geler des serveurs malveillants à l'étranger sans violer la souveraineté numérique de l'État hébergeur ?

→ Quels critères universels devons-nous adopter pour qu'une preuve numérique soit jugée "irréfutable" lors de l'attribution d'une attaque devant une instance internationale ?

BIBLIOGRAPHIE :

I. Rapports internationaux et documents onusiens

- **Union internationale des télécommunications (UIT)** – *Global Cybersecurity Index (GCI) 2024*
  Accéder au rapport GCI 2024
- **Organisation des Nations Unies (ONU)** – *Rapport du Groupe de travail à composition non limitée (OEWG)*
  Accéder au rapport officiel de l'OEWG
- **Global Forum on Cyber Expertise (GFCE)** – *Global Agenda for Cyber Capacity Building*
  Accéder au rapport du GFCE (PDF)
- **Geneva Internet Platform (GIP)** – *UN GGE & OEWG Digital Watch Tracker*
  Accéder au suivi des processus onusiens

II. Traités, résolutions et textes juridiques

- **UIT** – *Résolution 130 : Renforcement du rôle de l'UIT dans la protection des réseaux*
  Texte de la Résolution 130 (Rév. Bucarest, 2022)
- **UIT** – *Résolution 50 : Études relatives à la cybersécurité et normalisation*
  Texte de la Résolution 50 (Rév. New Delhi, 2024)
- **UIT** – *Résolution 174 : Politiques publiques internationales relatives à la sécurité de l'Internet*
  Texte de la Résolution 174 (Busan, 2014)
- **Conseil de l'Europe** – *Portail de la coopération internationale et Convention de Budapest sur la cybercriminalité*
  Accéder aux ressources juridiques du Conseil de l'Europe

III. Données statistiques et bases de données institutionnelles

- **UIT** – *Digital Development Dashboard (Global Connectivity Data)*
  Accéder aux statistiques de connectivité de l'UIT
- **Statista Research** – *Distribution of cyber attacks recorded worldwide by industry sector*
  Accéder aux graphiques sectoriels Statista
- **StatBase** – *Global Cyber Security Dataset and Country Rankings*
  Accéder à l'Index Global de StatBase

IV. Analyses géopolitiques et documents opérationnels

- **Center for Strategic and International Studies (CSIS)** – *Demystifying Cyber Operations in International Conflicts*
  Accéder à l'analyse du CSIS
- **Telefónica Security Room** – *Origins and evolution of the International Computer Security Day*
  Accéder à l'historique du 30 novembre