CyberPeace Institute

RAPPORT D'ACTIVITÉ

2022

Plus d'impact, ensemble

CONTENU

01.

4 Convictions,
4 objectifs stratégiques
3 populations prioritaires
1 ambition: l'impact

02.

Qui nous sommes

03.

Le CyberPeace Institute sur une carte

04.

Le CyberPeace Institute en 2022

05.

Nos programmes

06.

Nos partenaires

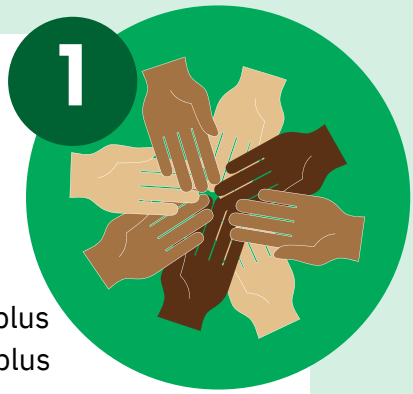
INTRODUCTION

L'histoire du CyberPeace Institute a commencé en décembre 2019, quand une poignée d'acteurs issus de la Tech, de la philanthropie, prend l'audacieuse initiative de tracer un chemin vers la « paix numérique ». Une initiative nécessaire, dans un contexte marqué par la généralisation de la transformation digitale de nos sociétés, et la prolifération continue des menaces qu'elle suscite malgré elle.

Une initiative qui avait aussi, sans doute, besoin de souplesse, d'agilité pour voir le jour, pour anticiper les cadres multinationaux dans lesquels la mission du CyberPeace Institute s'inscrit aujourd'hui, en 2022.

Notre mission s'appuie sur **quatre convictions**, qui guident chacun de nos trois métiers, que sont **l'assistance, l'analyse, la contribution aux politiques publiques, l'anticipation** au profit des trois populations prioritaires : le monde humanitaire, le secteur de la santé et les victimes de conflits armés.

L’assistance



Nous devons être unis pour mieux affronter cette cybermenace, qui frappe indifféremment mais ne cause pas les mêmes dommages, selon les cibles qu’elle se donne et dont le niveau de vulnérabilité varie.

De nombreuses ONG fournissent un soutien de dernier recours, aidant plus d'un milliard de personnes par an à répondre à leurs besoins les plus fondamentaux. Ce que ces ONG font pour ces populations, nous le faisons pour ces ONG, pour les protéger contre les cyberattaques et leur permettre d’assurer la continuité de leur mission.

L’analyse

Pour mieux affronter les cybermenaces, nous devons mieux les connaitre et les faire connaitre.

Les identifier, les tracer, les analyser, en suivant un angle singulier: l’impact humain. Ce travail de recherche, d’analyse, conduit par une expertise unique au monde et renforcé par les liens académiques que nous avons construits, partout dans le monde, vise à décrire le mode opératoire, identifier le mobile mais également leurs impacts humains.

La contribution aux politiques publiques

Tous ces efforts doivent conduire à une plus grande responsabilisation de tous les acteurs concernés : les entreprises, mais aussi les États.

Nous plaçons la responsabilité au cœur de notre plaidoyer pour un cyberespace où les droits et libertés fondamentaux des individus sont respectés, tout en faisant avancer l'État de droit à travers une approche centrée sur l'humain. Nous documentons ainsi les violations dans le but de favoriser la responsabilisation des acteurs concernés et de promouvoir le dialogue, à travers nos recommandations et notre participation à des initiatives internationales.

L'anticipation

Il est impératif d'analyser et de sensibiliser aux menaces de sécurité associées aux technologies émergentes et disruptives à leur impact et à leur préjudice sur les humains.

Nous agissons comme une plateforme pour comprendre les perturbations technologiques et politiques, développer des solutions collaboratives innovantes et renforcer les capacités pour renforcer la société cyber-résiliente de demain.

L’histoire du CyberPeace Institute, nous voulons la raconter à travers le regard des femmes et des hommes qui composent nos équipes, notre Conseil d’administration et notre Comité consultatif. Nous voulons aussi la raconter à travers le témoignage de ceux qui nous ont fait confiance : nos partenaires et les bénéficiaires de nos missions.

Cette histoire, nous voulons aussi et surtout l’écrire avec vous, entreprises, administrations, fondations, qui avez le pouvoir de renforcer notre capacité d’agir, grâce à vos dons et à toutes les formes que pourra prendre votre soutien.

Ensemble, mobilisons-nous.

Ensemble, continuons d'écrire l'histoire du CyberPeace Institute, au service de la paix numérique.

Préparons-nous aussi aux défis qui nous attendent en 2023, où les enjeux lies au déploiement de l'intelligence artificielle et l'omnipresence des operations de désinformation feront l'objet d'un traitement particulier, pour les équipes du CyberPeace Institute.

Stéphane DUGUIN
CEO

CONSEIL D'ADMINISTRATION

Le CyberPeace Institute a été fondé sur la base d'un objectif clair: protéger les populations vulnérables contre la prolifération des cyberattaques et instaurer la confiance dans l'écosystème numérique.

Cela signifie que nous **AIDONS** les ONG à se préparer aux cyberattaques et à s'en remettre, que nous **ANALYSONS** les failles qui touchent les communautés vulnérables afin de comprendre leur paysage de menaces, de fournir une alerte avancée et de réduire les dommages, et que nous **PLAIDONS** pour un comportement responsable dans le cyberespace afin de garantir le respect des libertés et des droits fondamentaux des personnes, tout en faisant progresser l'État de droit à travers une perspective centrée sur l'humain.

Les compétences, les capacités et les programmes que nous avons mis en place pour ces missions, grâce au soutien de nos donateurs, nous ont permis de répondre à des besoins émergents, en nous concentrant sur la prolifération des cyberattaques ciblant le monde humanitaire, le secteur de la santé et la dimension cybernétique du conflit entre la Russie et l'Ukraine.

C'est un honneur pour moi d'être membre fondateur du conseil d'administration du **CyberPeace Institute** et de présider désormais le conseil exécutif. Le conseil d'administration a une composition internationale et ses membres, nommés par cooptation par les membres en exercice, sont des personnes qui ont une expertise dans le domaine du numérique et de la cybernétique. En tant que conseil d'administration, nous avons à cœur de soutenir chaque fois que possible les experts de l'Institut dans leurs projets, au service de ceux qui en ont le plus besoin.

Le CyberPeace Institute est efficace parce qu'il ne se contente pas d'imaginer un cyberespace plus sûr, mais parce qu'il fournit des outils et des ressources concrets pour atteindre cet objectif.

Alexander Niejelow
Président du conseil d'administration

Le Conseil d'Administration est l'organe directeur du CyberPeace Institute. Sa composition est internationale et ses membres sont des individus qui ont une expertise dans le domaine du digital et de la cybersécurité. Les membres du Conseil sont nommés par cooptation par les membres en exercice. Chaque membre du Conseil a un mandat de trois ans et peut être réélu pour deux autres mandats. Le Conseil se réunit tous les trimestres et prend ses décisions par consensus.

Alejandro BECERRA GONZALEZ

Directeur mondial de la sécurité de l'information, Telefonica

Andrew MCCRAKEN

Directeur Mondial, WaterAid International

Maya BUNDT

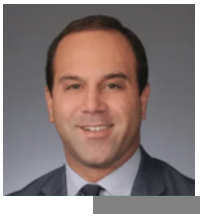
Directrice du Cyber Resilience Chapter de la Swiss Risk Association

Hoo MING NG

Conseiller en Affaires et Opérations Stratégiques, Ancien Directeur Exécutif Adjoint de l'Agence de Cybersécurité de Singapour

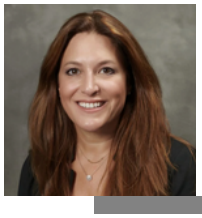
Amy HOGAN-BURNEY

Directrice Générale et Conseillère Générale Associée pour la Politique et la Protection en matière de Cybersécurité, Microsoft



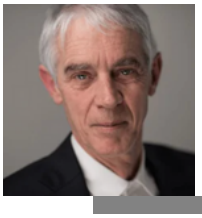
Alexander NIEJELOW

Expert en Technologie et Cybersecurité



Bonnie LEFF

Vice-présidente senior en Gestion de Programme en Sécurité de l'Entreprise, Mastercard



Martin VETTERLI

Président, EPFL

CONSEIL CONSULTATIF

La technologie peut accélérer, améliorer nos vies dans des proportions inimaginables, grâce à l'innovation numérique. Mais la même technologie est aussi utilisée pour nuire, dans des proportions inimaginables, et personne n'est épargné.

La sécurité humaine ne peut plus être assurée sans cybersécurité. Les Droits de l'Homme ne peuvent plus être garantis sans les droits numériques. La dignité humaine n'est rien sans la dignité numérique.

Garantir les droits des personnes à la sécurité, à la dignité et à l'équité dans le cyberespace : c'est précisément la mission du CyberPeace Institute. J'ai accepté, à la fin de l'année 2022, de rejoindre son **Conseil Consultatif**, qui rassemble des personnalités du monde entier, engagées dans les domaines de la sécurité, en général, de la cybersécurité en particulier, des Droits de l'homme ou du dialogue pour la Paix.

D'un point de vue personnel, je souhaite que nous parvenions à trouver le meilleur équilibre possible entre innovation et abus d'innovation, à nous diriger vers une meilleure régulation du cyberespace et un meilleur contrôle de la conformité aux normes cyber, enfin vers une meilleure répartition et un élargissement des responsabilités de tous les acteurs concernés.

J'attends du CyberPeace Institute qu'il fasse preuve de leadership, qu'il poursuive sans relâche ses missions de recherche et d'analyse, qu'il produise des preuves et qu'il défende activement les intérêts de tous. Je pense que sa méthode de travail ouverte et inclusive, dans un cadre multipartite, est et restera la clef de sa réussite.

J'espère pouvoir y contribuer, à ma petite échelle. Car plus que jamais, la construction de la paix est nécessaire et la cyberpaix est essentielle à la paix.

Nnenna Nwakanma

ICT4D Stratège, Experte en EParticipation et Engagement Citoyen

Le Conseil Consultatif est nommé par le Conseil d'Administration, sur la base de l'avis du Directeur Général. Il a une composition internationale et présente une diversité d'expertises et de points de vue sur la cybersécurité, les Droits de l'Homme, la paix et la sécurité. Le Conseil Consultatif se réunit deux fois par an avec le Directeur Général et l'équipe dirigeante de l'Institut.

Sunil ABRAHAM

Ancien Directeur Exécutif,
Centre Internet et Société

Eric MEERKAMPER

Fellow,
Institut montréalais d'Études sur le Génocide et les Droits de l'Homme

Khoo BOON HUI

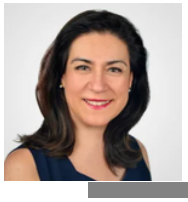
Ancien Président,
Interpol

Nnenna NAWAKANMA

ICT4D Stratège, Experte en Participation et Engagement Citoyen

Frédérick DOUZET

Directrice,
Géopolitique de la Datasphère (GEODE)



Luisa PARRAGUEZ KOBEK

Professeure d'Affaires et de Sécurité Internationale,
Tecnológico de Monterrey

Jen ELLIS

Porte-parole en Cybersecurité

Alejandro ROMERO

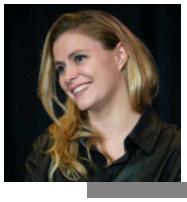
Directeur des Opérations,
Constella Intelligence

Melanio ESCOBAR

Activiste, Journaliste, Auteur

Marietje SCHAAKE

Directrice de la Politique Internationale,
Centre de Politique Cybernétique de l'Université de Stanford



Camille FRANÇOIS

Directrice Mondial de la Confiance et de la Sécurité, Niantic, INC.

Vincent SUBILIA

Directeur Général,
Chambre de commerce, d'industrie et des services de Genève (CCIG)

Vasu GOUNDEN

Fondateur & Directeur Exécutif,
Centre Africain pour la Résolution Constructive des Conflits

Eli SUGARMAN

Directeur de contenu chez Oversightboard ; Ancien Directeur,
Cyber Initiative à la Fondation William et Flora Hewlett

NOS ÉQUIPES

Pour mener à bien ces missions, le CyberPeace Institute s'est entouré, au fil des ans, de nombreux experts, venus d'EUROPOL, de l'ENISA, de l'ANSSI, du monde de l'entreprise, du secteur humanitaire ou de la diplomatie. Ils ont rejoint l'organisation avec une ambition claire : faire la différence, avoir de l'impact, sur un sujet majeur qui conditionne l'avenir de la sphère numérique.

La première force des équipes de l'Institut est la faculté d'adaptation. Né pendant la crise Covid, il a d'abord fonctionné à distance, avant de se réunir à Genève, tout en s'appuyant sur les atouts offerts par la diversité de ses membres, issus de **19 pays différents**, et autant de relais locaux potentiels pour le déploiement de ses activités. La diversité est ainsi au cœur des valeurs de l'Institut, qui observe par ailleurs une parfaite parité (**52 %** de femmes et **48 %** d'hommes fin 2022) et accueille une personne en situation de handicap.

Nous avons commencé à accueillir des stagiaires et des jeunes professionnels en 2022, avec des contrats d'une durée de **3 mois** minimum, et qui peuvent être effectués soit dans nos bureaux à Genève, soit en télétravail. Une convention de stage tripartite est établie entre les trois parties (Université, étudiant et Institut). **88 %** de nos stagiaires étaient/sont des étudiants de niveau Master dans différents domaines (droit, relations internationales, géopolitique, technologies de l'information, etc.).

Les jeunes professionnels sont de jeunes diplômés de troisième cycle à la recherche d'une première expérience professionnelle. Ils sont engagés pour contribuer à des projets spécifiques initiés par l'Institut.

En 2022, l'Institut a également mis en place un *Fellowship Program* pour donner à des personnes d'expérience l'occasion de s'immerger dans la communauté de la cybersécurité humanitaire.

Ce programme s'adresse à des experts passionnés qui souhaitent développer leur talent et mettre à profit leurs compétences dans des projets qui ont un impact direct sur les populations fragiles.

À LA FIN DE 2022, L'INSTITUT COMPTAIT SIX ÉQUIPES, COMPOSÉES DE :

28

ETP*

4

“JEUNES PROFESSIONELS”

8

STAGIAIRES

*Employés à Temps Plein

MANAGEMENT TEAM

Le Cyberespace ne connaît pas de frontières. Nous non plus. Nous sommes des professionnels issus de différents milieux et disposant d'un large éventail de compétences à l'intérieur et à l'extérieur de l'industrie cyber. La diversité (**11 nationalités**), l'égalité (**52 % de femmes et 48 % d'hommes**) et l'inclusion (modèle de travail flexible) font partie intégrante de notre vision collective de la cyberpaix.

Stéphane DUGUIN

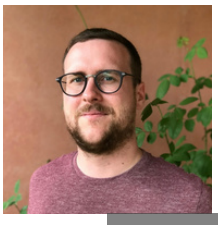
Directeur Exécutif

Charlotte LINDSEY

Directrice des Politiques Publiques

Khristine BENEDICTO

Directriice des Ressources Humaines

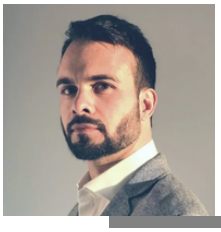


Fabien LEIMGRUBER

Gestionnaire de Programme

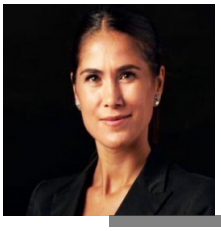
Florent BITSCHY

Directeur de la Sécurité des systèmes d'information



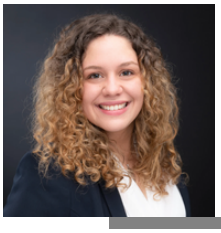
Adrien OGÉE

Directeur des Opérations



Francesca BOSCO

Conseillère Stratégie et Partenariats

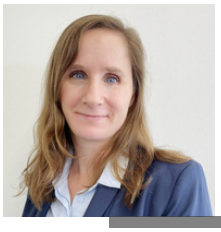


Coralie PÉGAT-TOQUET

Directrice de la Gouvernance

Vincent de CRAYENCOUR

Directeur du Développement et des Partenariats Stratégiques

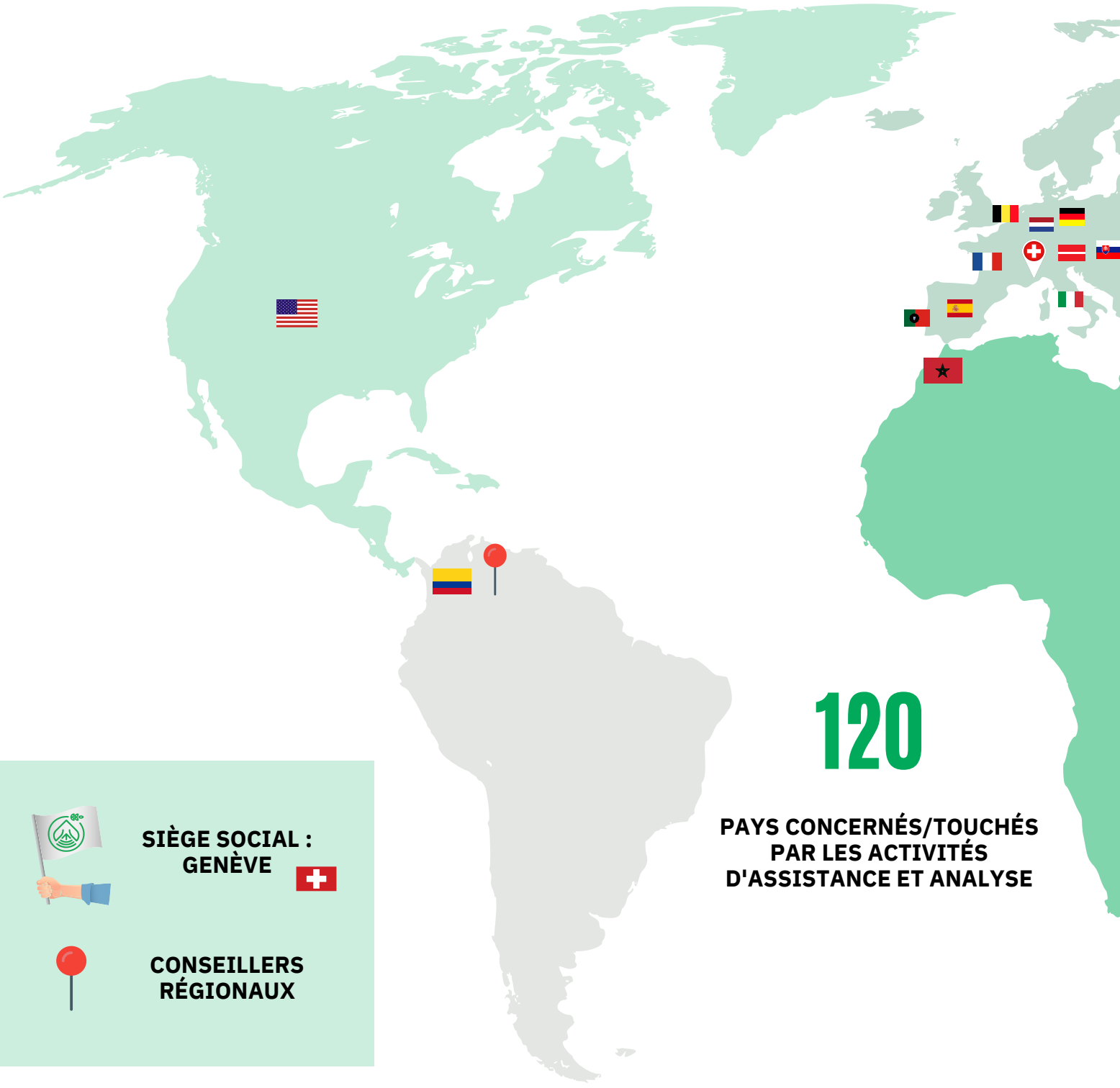


Emma RAFFRAY

Directrice de la Recherche et de l'Analyse

Issus de **19 pays différents**, et autant de relais locaux potentiels pour le déploiement de ses activités.
La **diversité** est ainsi au cœur des valeurs de l'Institut, qui observe par ailleurs une **parfaite parité** (52 % de femmes et 48 % d'hommes fin 2022) et accueille une personne en situation de handicap.

LE CYBERPEACE INSTITUTE



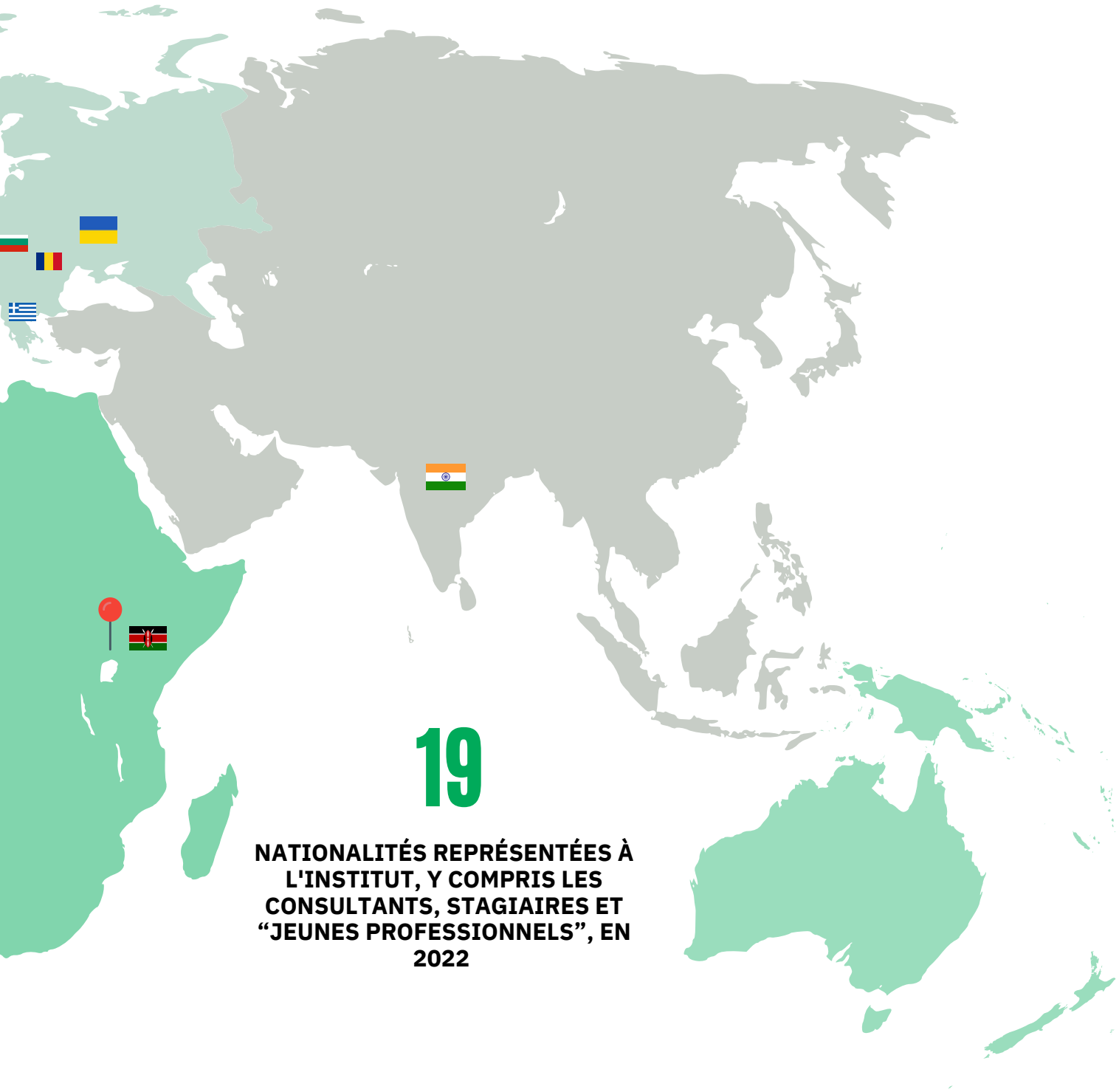
120

PAYS CONCERNÉS/TOUCHÉS PAR LES ACTIVITÉS D'ASSISTANCE ET ANALYSE

SIÈGE SOCIAL : GENÈVE

CONSEILLERS RÉGIONAUX

SUR UNE CARTE



19

NATIONALITÉS REPRÉSENTÉES À L'INSTITUT, Y COMPRIS LES CONSULTANTS, STAGIAIRES ET "JEUNES PROFESSIONNELS", EN 2022

2022

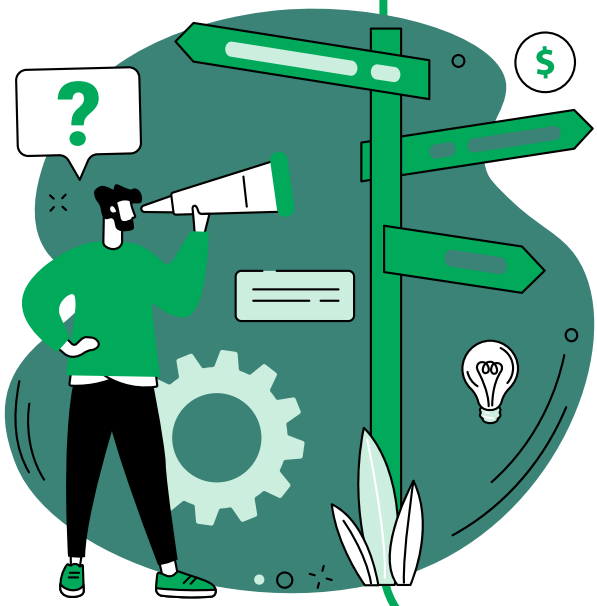
Est la 3ème année « pleine » dans la vie de l'Institut. Année charnière à plusieurs titres.

01

NOUVEAUX PARTENAIRES

2022 aura aussi été une année d'ouverture vers de nouveaux partenaires. C'est l'année où le CyberPeace Institute prend la décision d'entrer dans une nouvelle forme de coopération avec les Etats.

Au-delà de notre travail de sensibilisation, au-delà de la mise à disposition de nos travaux, et des témoignages que nous sommes amenés à faire dans les cadres multilatéraux, nous invitons désormais les Etats à contribuer à nos travaux, sur le plan à la fois technique et financier. Dans le même esprit, nous nous sommes tournés, avec succès, vers les appels à projets proposés par l'Union européenne.



PASSERELLES VERS LE MONDE

2022 est enfin l'année où l'Institut a commencé à tendre des passerelles vers d'autres grandes villes du monde.

02

Nous avons désormais également une présence au sein du Campus Cyber à Paris, écoystème unique réunissant l'ensemble des acteurs de la cybersécurité.

03

CONFIRMATION

2022 est d'abord l'année de la confirmation, pour plusieurs de nos initiatives. Dans le domaine de la santé, avec notamment le développement du ***Cyber Incidence Tracer*** ou le lancement du *Compendium of multistakeholder* perspectives en septembre 2022, aux côtés des Nations unies, dans le sillage du programme ***Cyber 4 Healthcare*** que nous avions créé pour aider les professionnels de santé, analyser les cyberattaques qu'ils ont subi et faire avancer les politiques visant à protéger le secteur.

Dans le secteur humanitaire, le programme **CyberPeace Builders**, première plateforme de cyberassistance aux ONG dans le monde, est devenu la locomotive d'un ambitieux projet, annoncé en décembre 2022, le **Centre de Cybersécurité Humanitaire**, qui vise à offrir aux ONG une gamme complète de services de cyber-protection.

04

ENGAGEMENT

2022, c'est une année d'engagement, pour le CyberPeace Institute pour la promotion d'un comportement responsable. Ce message, nous l'avons porté auprès de 80 pays et au sein de forums diplomatiques majeurs, des Nations Unies à l'OCDE en passant par le G77 ou le Forum de Paris pour la Paix, contribuant à lutter contre l'utilisation des technologies de l'information et de la communication à des fins criminelles ou à renforcer les capacités numériques des pays en développement.

05

NOUVELLES INTITIATIES

2022 a été enfin l'année de la création de la Plateforme sur les cyberattaques en temps de conflit #Ukraine, initiative unique qui trace l'ensemble des cyberattaques survenues dans le cadre du conflit russo-ukrainien et propose une étude d'impact sectorielle pour mieux évaluer les dommages subis par les populations civiles. Aussi 2022 est l'année où nous avons lancé de nouveaux champs de réflexion, sur le Spyware, notamment, aux côtés du Forum Économique Mondial.

NOS PROGRAMMES EN 2022, RACONTÉS PAR CEUX QUI EN BÉNÉFICIENT...

"Les CyberPeace Builders ont convaincu notre organisation par leur expérience et leur professionnalisme, sur l'importance de la cybersécurité. Nous nous sentons soutenus et convaincus que nous prenons les bonnes mesures pour renforcer la résilience et la protection numériques."

Nonviolent Peaceforce

"En tant qu'acteurs de terrain, d'assistance et d'urgence, nous sommes particulièrement sensibles à l'approche développée par le CyberPeace Institute, qui met l'accent sur les populations vulnérables et s'efforce de mieux anticiper les situations de crise."

Alliance Urgences

["Le CyberPeace Institute] contribue à renforcer les capacités du personnel, tant au niveau local qu'en Suisse, ce qui permet de prévenir les crises majeures."

Centre écologique Albert Schweizer

"Pour moi, la création du CyberPeace Institute a été l'une des meilleures mesures prises au cours des 18 derniers mois."

Brad Smith, Microsoft

"Je dois féliciter le CyberPeace Institute d'avoir produit le premier rapport technologique sur ce sujet très important. Pour résoudre ce problème, les gouvernements, les entreprises, les experts en technologie, la société civile, les médias et les universités devront coopérer pour lutter contre ces menaces."

Latha REDDY, coprésidente de la Commission mondiale sur la stabilité du cyberespace

"Nous avons reçu des conseils précis et détaillés sur ce qu'il fallait faire, de la part d'un professionnel accompli de la sécurité informatique, et ce dans un délai très court. Avec une évaluation générale de base de la sécurité, la FSD est maintenant consciente des domaines qui nécessitent le plus d'attention, de toute urgence."

Fondation Suisse de Déminage (FSD)

"Ensemble, engageons-nous auprès du CyberPeace Institute et de ses partenaires pour permettre aux professionnels de santé de continuer à travailler dans les meilleures conditions cybernétiques possibles."

Association des responsables de l'information de l'ANASE (ACIOA)

"[grâce au CyberPeace Institute] nous avons appris à être constamment attentifs aux cybermenaces."

Association médicale mondiale

"Une expérience qui nous a ouvert les yeux. Nous sommes impatients de mettre en place les mesures proposées dans l'évaluation de la sécurité."

Union internationale de lutte contre le cancer

"Au MDNi, nous apprécions la relation de confiance avec le CyberPeace Institute et son engagement à nous aider à trouver des solutions adéquates à nos défis en matière de cybersécurité, en particulier pour protéger les données de nos bénéficiaires. Le nouveau programme CyberPeace Builders apportera une grande valeur ajoutée aux ONG basées à Genève, mais aussi dans le monde entier, pour les aider à faire face aux défis numériques d'aujourd'hui."

Pascal Carpentier, responsable des systèmes d'information et des technologies à la Drugs for Neglected Diseases initiative (DNDi)

"Le CyberPeace Institute, organisation basée à Genève qui aide les organisations à but non lucratif, les organisations humanitaires et les organismes de santé à faire face à la cybersécurité, a mis en place un programme visant à recruter des professionnels du monde de l'entreprise pour expliquer des sujets tels que l'hameçonnage par courriel aux organisations à but non lucratif qui n'ont peut-être pas le budget nécessaire pour embaucher leurs propres experts."

Catherine Stupp,
The Wall Street Journal

"Le CyberPeace Institute a pu aider à évaluer les tentatives de piratage."

CNN

"Je suis extrêmement fier que Logitech contribue au programme CyberPeace Builders. Tous ceux qui, chez Logitech, ont participé à ce fantastique programme ont adoré l'expérience."

Tana Dubel, CISO,
Logitech

NOS PRIORITÉS

Nous développons des programmes pour soutenir les communautés vulnérables aux menaces du cyberespace. En surveillant, en évaluant et en communicant sur les cyber menaces à ces communautés, nous pouvons travailler ensemble avec des partenaires pour les mieux protéger.

Nous supportons les **ONG** et autres secteurs clés

Nous nous engageons à soutenir et protéger les **communautés vulnérables**

HUMANITAIRE

Plus d'un milliard de personnes dépendent des organisations non gouvernementales (ONG) pour manger, boire, dormir ou se soigner. Les tensions économiques, géopolitiques et sociales actuelles les impactent directement.

Parce qu'elles détiennent des données clefs, les ONG subissent un nombre croissant de cyberattaques. Le monde humanitaire est le deuxième secteur le plus ciblé après les acteurs de la Tech. Mais les ONG ont du mal à mettre en place les solutions de cybersécurité les plus élémentaires, pour de multiples raisons : leur transformation numérique récente et souvent précipitée, les restrictions budgétaires inhérentes au secteur et l'impossibilité de rivaliser avec le secteur privé pour recruter des experts cyber.

Nous sommes une ONG qui a pour mission de protéger les autres ONG en ligne. Notre solution ? Mettre en relation les ONG et les volontaires en cybersécurité des entreprises. Plus d'impact, ensemble.

LE PROGRAMME CYBERPEACE BUILDERS : UN BÉNÉFICIAIRE TÉMOIGNE

TÉMOIGNAGE DE HANSJÖRG EBERLE | FSD

Hansjörg Eberle, directeur et cofondateur de la FSD (**Fondation suisse de déminage**), nous parle de l'impact de la cybersécurité sur les activités quotidiennes de son organisation, qui s'occupe de mines et engins explosifs résiduels, de déminage de sites pollués par des déchets toxiques, enfin de soutien à la paix et au développement dans les pays touchés par des conflits armés.

"En tant qu'organisation de déminage, nous éliminons les mines terrestres et les munitions explosives non explosées (UXO). Nous employons environ 400 personnes, dont la plupart utilisent régulièrement des ordinateurs. Pour nous, la cybersécurité est essentielle et prend de plus en plus d'importance. Malheureusement, nous avons déjà été la cible de cyberattaques. Nous avons remarqué une augmentation spectaculaire du nombre de courriels d'hameçonnage et de toutes sortes de messages frauduleux envoyés à notre personnel en peu de temps.

Nous avons contacté le CyberPeace Institute en 2021. À l'époque, je leur ai dit que nous n'avions pas de département informatique véritable, mais que nous voulions améliorer la situation. Il était difficile de trouver une source fiable pour nous conseiller sur les moyens d'améliorer notre cybersécurité et sur la manière de mettre en œuvre ces changements de manière efficace.

Le CyberPeace Institute nous a aidés à approcher des professionnels de la sécurité informatique de très haut niveau qui ont commencé à nous aider dans des domaines spécifiques par le biais du programme **CyberPeace Builders**. Nous avons pu avoir accès à un réseau d'experts mettant gratuitement leurs compétences à notre disposition et améliorer notre réponse aux problèmes de sécurité.

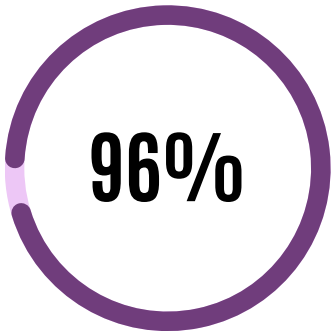
Depuis, nous avons fait beaucoup de progrès. Le fait de disposer d'évaluations de sécurité actualisées de nos systèmes est non seulement rassurant, mais prouve que nos compétences en matière de cybersécurité se développent à long terme. Nous prenons, par exemple, des mesures pour renforcer nos systèmes Microsoft Office 365 et mieux gérer nos mots de passe. Nous nous assurons que toutes les stations disposent d'un antivirus, que certaines fonctions importantes commencent à utiliser des accès VPN et, bien sûr, nous avons également commencé à améliorer la sécurité de notre service en veillant à ce que les données soient cryptées".

POURQUOI AVOIR CRÉÉ LE PROGRAMME CYBERPEACE BUILDERS?

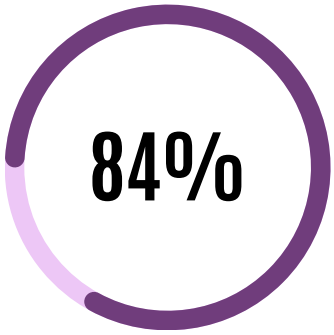
Builders est la première plateforme de cyber assistance en ligne aux ONG, qui permet de mettre en relation les entités les plus vulnérables avec des centaines de volontaires, experts en cybersécurité, pour résoudre les problèmes qu'ils rencontrent et les protéger contre les risques de cyberattaque. Fin 2022, ce sont 100 ONG qui profitent de cet outil gratuit grâce aux 30 premières entreprises partenaires de l'Institut, avec l'objectif d'accompagner 1000 ONG d'ici à fin 2024.

55 **Cyberattaques ou incidents documentés contre des organisations non gouvernementales ou à but non lucratif, dans 12 pays.** Les types d'incidents comprennent la prise de contrôle de comptes, les ransomwares, les dénis de service, etc.

- **311 volontaires en cybersécurité inscrits sur 13 sujets différents**
- **108 ONG embarquées**
- **641 heures d'assistance en cybersécurité**
- **311 missions d'assistance délivrées**



Des ONG sont satisfaites de nos services



Des volontaires sont satisfaits du programme

EN 2022

Le programme Builders a éte intégré à une initiative plus globale, au service du monde humanitaire : le **Centre de Cybersécurité Humanitaire**.

POURQUOI AVOIR CRÉÉ LE CENTRE DE CYBERSÉCURITÉ HUMANITAIRE ?

Après 3 ans d'existence, nous avons décidé en 2022 de rassembler toutes nos activités dédiées aux acteurs humanitaires en une initiative phare dont l'impact se veut global : le Centre de Cybersécurité Humanitaire (CCH).

Cette initiative de l'Institut vise à protéger les acteurs humanitaires dans le cyberespace, partout dans le monde...

...À TRAVERS 4 MISSIONS PRINCIPALES

INFORMER	SUR LES CYBERMENACES, LES VULNÉRABILITÉS ET LES INCIDENTS AUXQUELS SONT CONFRONTÉS LES ACTEURS HUMANITAIRES
AIDER	LES ACTEURS HUMANITAIRES À DÉTECTER LES CYBER-INCIDENTS ET À LES EMPÊCHER DE NUIRE
RÉPONDRE	AUX CYBER-INCIDENTS AUXQUELS SONT CONFRONTÉS LES ACTEURS HUMANITAIRES POUR QU'ILS SE RÉTABLISSENT PLUS RAPIDEMENT
RENFORCER	UN ÉCOSYSTÈME NUMÉRIQUE RÉSILIENT POUR LES ACTEURS HUMANITAIRES

La création du CCH a été annoncée le 8 décembre 2022 à l'issue d'une phase de conception au cours de laquelle nous avons identifié toutes les compétences que nous étions déjà en mesure de mettre à la disposition des acteurs humanitaires et du développement, mais aussi celles qui nous manquaient, pour mieux compléter notre catalogue de services en développant de nouveaux partenariats. C'est pourquoi l'annonce du 8 décembre a pris la forme d'un Appel à soutien, qui a permis à l'Institut d'enregistrer plus de 70 nouveaux partenaires, et avec eux les nouveaux outils, services et expertises destinés à l'ensemble de nos bénéficiaires. **Ensemble, nous sommes plus forts!**

SANTÉ

Guidés par la mission de l'Institut CyberPeace de soutenir les plus vulnérables dans le cyberespace, nous avons lancé en 2021 le programme *Cyber 4 Healthcare* pour aider les professionnels de la santé, analyser les cyberattaques et faire avancer les politiques de protection du secteur. Après notre appel aux Gouvernements pour la protection des établissements médicaux et de santé, et notre rapport "Nos Vies en Péril : les cyberattaques contre les soins de santé sont des attaques contre les personnes" (mars 2021) et son addendum (novembre 2021), deux autres initiatives importantes ont vu le jour en 2022 :

Le Cyber Incident Tracer (CIT) #Health

Le Compendium des perspectives multipartites

TÉMOIGNAGE DU PARIS PEACE FORUM

Dans un rapport récent, le CyberPeace Institute a identifié un manque important de connaissances sur les cyberincidents mondiaux et leur impact. Compte tenu de la nécessité de centraliser ces informations, le CyberPeace Institute développe une plateforme publique qui offre une vue d'ensemble de l'impact des cyberincidents sur les personnes et propose des instruments pour les protéger et les autonomiser. La plateforme vise à susciter un changement positif en faveur de la cyberpaix, à savoir la sécurité, la dignité et l'équité humaines dans le cyberespace. Cyber Incident Tracer (CIT) #HEALTH est développé en coopération avec des partenaires internationaux de différents secteurs afin de garantir une approche multidisciplinaire de la collecte de données à l'échelle mondiale.

COMPEDIUM : TÉMOIGNAGE

"J'ai eu l'honneur d'animer une discussion sur le lancement du ***Compendium*** *en marge de la réunion de l'OEWG en décembre 2021. J'ai été heureux de constater l'intérêt porté à cette question, qui confirme que la protection du secteur de la santé contre les cyberattaques est extrêmement importante et qu'un grand nombre de personnes sont impliquées dans la réflexion sur la façon de protéger le secteur de la santé.*

Je suis convaincu que le Compendium peut apporter une contribution substantielle à la recherche de solutions à des dilemmes spécifiques. Pour moi, le Compendium est aussi la preuve évidente qu'une approche multipartite peut fonctionner sans problème dans la pratique."

POURQUOI AVOIR PARTICIPÉ AU LANCEMENT DU COMPENDIUM ?

En 2022, le gouvernement de la République tchèque, Microsoft et l'Institut CyberPeace ont réuni les communautés de la santé et de la cybersécurité en organisant des ateliers multipartites, chacun traitant d'un sujet essentiel lié à la protection du secteur de la santé contre les cyberattaques. Au cours de ces ateliers, un groupe diversifié d'experts, de praticiens et de parties prenantes a formulé des recommandations clés, des enseignements et des bonnes pratiques.

Sur la base de ce qui a été appris, le **Compendium of Multistakeholder Perspectives on Protecting the Healthcare Sector from Cyber Harm** a été élaboré puis lancé à New York, en marge de la réunion du groupe de travail à composition non limitée de l'Assemblée générale des Nations unies sur la sécurité et l'utilisation des TIC, en juillet 2022.

Le rapport final offre aux établissements de soins de santé, aux gouvernements, aux organisations internationales et aux autres parties prenantes une ressource utile pour soutenir leurs efforts visant à protéger le secteur des soins de santé contre les cybermenaces.

En 2022, il ne s'est pas passé un mois sans qu'une cyberattaque ne touche un établissement de santé quelque part dans le monde. Le signalement et la documentation de ces incidents sont nécessaires, aujourd'hui, pour permettre à l'Institut de :

Comprendre l'ampleur et la portée réelles du problème

Mesurer le préjudice que ces attaques causent aux individus, aux communautés et à la société

Elaborer des réponses appropriées pour réduire la menace

Conçu en 2021 pour documenter les cyberattaques, sensibiliser le public, soutenir l'élaboration de politiques fondées sur des données probantes et offrir des réparations aux victimes, le **Cyber Incident Tracer (CIT) #Health**, plateforme de données centrée sur l'humain, a été mis au point en 2022.

POURQUOI AVOIR CRÉÉ LE CYBER INCIDENT TRACER ?

En pleine pandémie mondiale, le secteur de la santé a été fortement menacé, non seulement par les pressions croissantes exercées sur son personnel et ses organisations, pour maintenir des services essentiels à un moment où la demande augmente de manière exponentielle, mais aussi par des acteurs malveillants qui ciblent le secteur pour en tirer un profit financier et/ou informationnel.

Alors que le CyberPeace Institute cherchait à saisir et à mettre en évidence les conséquences de ces attaques sur le secteur, les personnes et la société dans son ensemble, il a constaté une lacune dans la collecte systématique des cyber-incidents à travers le monde.

Sans ces données, nous ne pouvions nous appuyer que sur des observations anecdotiques et des rapports d'incidents isolés pour déterminer qui, quoi, quand, pourquoi, où et comment le paysage de la menace est constitué. Sur la base de cette première phase de recherche et de la publication de **"Nos vies en péril: pirater la santé, c'est attaquer les personnes"**, l'idée est née de proposer une représentation visuelle des cyberincidents dans ce secteur et de l'impact qu'ils ont sur les personnes et les organisations, en créant **un traceur d'incidents cybernétiques, ou Cyber Incident Tracer (CIT).**

EN 2022, LE CIT A PERMIS DE RELEVER LES INFURRATIONS SUIVANTES :

141

ATTAQUES ONT ÉTÉ RECENSÉES CONTRE DES ÉTABLISSEMENTS DE SANTÉ :

34

HÔPITAUX TOUCHÉS

12

SOCIÉTÉS PHARMACEUTIQUES

7

ÉTABLISSEMENTS DE SANTÉ MENTALE ET D'ABUS DE SUBSTANCES

3,8

MILLIONS DE DOSSIERS ONT ÉTÉ VIOLÉS

3,7

MOYENNE D'ATTAQUES PAR SEMAINE

33

PAYS

250

JOURS D'INTERRUPTION DES ACTIVITÉS ONT ÉTÉ ENREGISTRÉS

LOCKBIT, VICE SOCIETY ET HIVE SONT LES OPÉRATEURS DE RANSOMWARE LES PLUS ACTIFS DANS LE SECTEUR.

CONFLITS

CONFLITS

Dès les premières heures du conflit russo-ukrainien, en février 2022, des civils et des infrastructures civiles ont été la cible de cyberattaques, dont plusieurs ont été manifestement coordonnées avec des opérations militaires cinétiques. Comment le CyberPeace Institute pouvait-il mobiliser ses experts dans cette situation, tout en préservant son indépendance et sa neutralité ?

Comment mettre à profit nos analystes et nos experts en politique publique pour mettre en avant l'impact humain de ces cyberattaques, conduit dans le cadre exceptionnel du plus important conflit du XXIème siècle ?

TÉMOIGNAGE DANS LA PRESSE

> *Les piratages, le sabotage de réseaux et d'autres campagnes de cyberguerre sont intensément déployés par les deux parties à mesure que l'invasion de l'Ukraine par la Russie progresse, bien que les opérations secrètes ne se soient pas révélées décisives sur le champ de bataille - du moins jusqu'à présent. Les alliés occidentaux ont d'abord craint un tsunami de cyberattaques contre le commandement militaire et les infrastructures critiques de l'Ukraine, ce qui aurait entravé sa capacité à résister aux forces russes qui se déversent à travers ses frontières. À la mi-septembre, le Cyber Peace Institute, une ONG basée en Suisse, a recensé près de 450 attaques - environ 12 par semaine - menées par 57 entités différentes de part et d'autre depuis le lancement de l'invasion en février.*
>
> **AFP, Security Week, 28 septembre 2022**

POURQUOI AVOIR CRÉÉ LA PLATEFORME UKRAINE ?

Le déclenchement des hostilités en Ukraine après l'invasion des forces militaires russes en février 2022 a incité l'Institut à commencer à rassembler et à analyser des données sur les cyberattaques en rapport avec ce conflit armé international, et à mettre en place la **Plateforme Ukraine sur les cyberattaques en temps de guerre**. La documentation des cyberattaques et des opérations menées contre des infrastructures essentielles à la survie de la population civile vise à contribuer à l'analyse de l'utilisation de la cybernétique dans les situations de conflit armé et à éclairer les débats sur les dimensions politiques et juridiques du conflit. Il s'agit également d'une importante source d'informations et de données qui permettra d'établir, le moment venu, la responsabilité de chacune des parties prenantes dans la dimension cyber du conflit.

La sensibilisation aux dommages et à l'impact des cyberattaques sur la population civile est un objectif important, de même que la sensibilisation de l'opinion publique, par l'intermédiaire de la plateforme, sur le droit et les normes applicables à l'utilisation de moyens cyber dans les conflits armés. La plateforme facilite également les appels de l'Institut en faveur du respect des civils et du droit international humanitaire, au cœur de notre engagement.

PLATEFORME SUR LES CYBERATTAQUES EN TEMPS DE CONFLIT #UKRAINE EN 2022

3

RAPPORTS PUBLIÉS

9

ARTICLES ET 2 FICHES PUBLIÉS

77

COUVERTURES MÉDIATIQUES

80

ACTEURS DIFFÉRENTS IDENTIFIÉS

1.1 K

CYBERATTAQUES SIGNALÉES TOUCHANT 22 SECTEURS D'INFRASTRUCTURES CRITIQUES DIFFÉRENTS

40

PAYS DIFFÉRENTS TOUCHÉS PAR CERTAINES MENACES

30K

CONSULTATIONS DE LA PLATEFORME AVEC UNE DURÉE MOYENNE DE 3 MINUTES SUR LA PAGE

NOS RAPPORTS TRIMESTRIELS

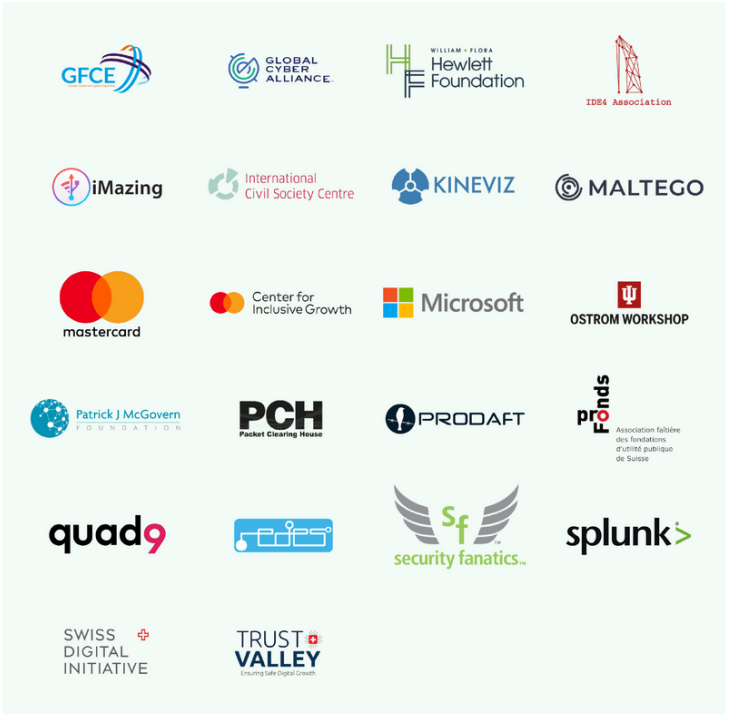
En 2022, nous avons signé 3 rapports d'analyse trimestriels, qui donnent un aperçu des dimensions cybernétiques du conflit armé en Ukraine. Les rapports combinent l'analyse des données collectées par la Plateforme et des informations recueillies par le biais de la recherche OSINT. Le CyberPeace Institute invite les lecteurs de ces rapports à prendre connaissance des tendances et des questions émergentes relatives aux cyber-incidents qui ont lieu en Ukraine, dans la Fédération de Russie et dans d'autres pays touchés par des cyberattaques initiées dans le contexte du conflit. En examinant les secteurs économiques touchés, les types de cybermenaces auxquels ils sont confrontés, en évaluant l'impact et les dommages des cyberattaques sur les civils et les populations, et en identifiant les acteurs les plus actifs, nous avons essayé de contribuer à une meilleure compréhension du paysage des cybermenaces tout au long de l'année 2022.

CyberPeace Institute

Quarterly Analysis Report
Q4 October to December 2022

Cyber Dimensions
of the Armed Conflict in Ukraine

NOS PARTENAIRES



REMERCIEMENTS

"Merci à ceux qui soutiennent le CyberPeace Institute depuis sa création, merci à ceux qui nous ont permis de mener à bien tous nos projets en 2022, merci à ceux qui nous lisent, nous écoutent, suivent nos travaux, participent à nos programmes, merci enfin à tous ceux qui feront le choix de nous rejoindre dans les années à venir..."

CONTACT

Avenue de Sécheron 15
1202 Genève
Suisse

www.cyberpeaceinstitute.org
media@cyberpeaceinstitute.org

@cyberpeaceinst
CyberPeace Institute

@cyberpeaceinst
CyberPeace Institute