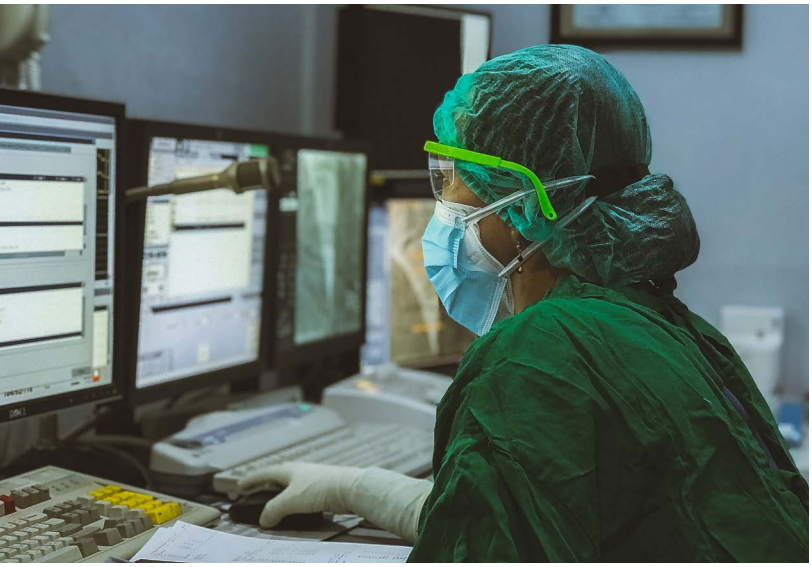
CyberPeace Institute

CYBERPEACE INSTITUTE

RAPPORT D'ACTIVITÉ 2019-2021



SOMMAIRE

MESSAGE DU DIRECTEUR EXÉCUTIF

« La promesse de la technologie, qui pénètre et influence toujours plus nos vies, pourra être réalisée seulement si nous parvenons à contrer les menaces que font peser des acteurs malintentionnés cherchent à tirer profit de la technologie à des fins malveillantes, notamment pour surveiller, attaquer, perturber, désinformer et nuire, en violant les lois et les normes internationales et en compromettant la sécurité à laquelle les sociétés civilisées aspirent. »

Stéphane DUGUIN, Directeur exécutif, CyberPeace Institute

Les années 2020 et 2021 ont été éprouvantes pour chacun et chacune d'entre nous. La pandémie du COVID-19 a entraîné des changements rapides et majeurs dans nos manières de communiquer, de travailler et d'apprendre – une situation qui a donné lieu à un nombre record de cyberattaques et de cybermenaces.

L'Institut est convaincu qu'il est essentiel, parfois même indispensable de se focaliser sur les conséquences sociétales des cyberattaques, et ce tout simplement parce que ces offensives ont un impact direct sur les personnes et sur la société. À ces fins, l'Institut a élaboré, lancé et mis en œuvre des programmes essentiels pour soutenir le secteur de la santé et les ONG.

Les défis systémiques appellent des réponses systémiques ainsi que l'engagement de toutes les parties prenantes à jouer leur rôle. L'Institut s'est associé à des efforts diplomatiques déployés au niveau international dans le cadre d'un appel à une action concertée de tous les gouvernements pour mettre fin aux cyberattaques contre le secteur de la santé. Cette initiative s'est doublée d'un soutien opérationnel sous la forme du Cyber4Healthcare, un programme visant à renforcer l'aide apportée aux victimes de cyberattaques, et de la publication d'un rapport d'analyse stratégique intitulé Nos vies en péril : pirater la santé, c'est attaquer les personnes, qui met en lumière la problématique et présente des recommandations sur les mesures à prendre. De plus, conscient de l'importance de référencer les cyberattaques, l'Institut a mis en place la plateforme Cyber Incident Tracer (CIT) #HEALTH en vue de sensibiliser le public à l'ampleur et à l'impact des attaques dirigées contre le secteur de la santé, de soutenir les décideurs en leur permettant de s'appuyer sur des éléments concrets et d'aider les victimes à se remettre.

Par ailleurs, l'Institut a lancé le CyberPeace Builders, premier réseau mondial de professionnels volontaires voués à soutenir les ONG humanitaires en renforçant leurs capacités en matière de cybersécurité.

Le personnel spécialisé de l'Institut a collaboré avec plusieurs acteurs issus du secteur privé, de la société civile, d'ONG et d'autres organisations internationales pour appeler l'attention sur les cybermenaces et proposer des solutions concrètes pour les contrer. L'Institut se caractérise par son analyse basée sur des éléments concrets pour soutenir les victimes et pour proposer des mesures efficaces en vue de prévenir les cyberattaques. Il s'est doté des capacités nécessaires pour réaliser des analyses scientifiques des cyberattaques et pour informer les victimes des résultats de ces analyses.

L'Institut a également mené des activités diplomatiques ainsi qu'un travail de sensibilisation pour faire connaître les comportements dans le cyberespace et les orienter, pour veiller au respect des lois et normes internationales, pour limiter les comportements considérés comme inacceptables et pour amener ceux qui enfreignent ces règles à répondre de leurs actes. L'Institut a suivi de près les négociations menées à ce sujet aux Nations Unies, et a soumis des recommandations et des éclairages.

Le soutien que l'Institut a reçu de ses donateurs et partenaires a contribué pour beaucoup aux résultats que nous avons atteints en si peu de temps. Ce Rapport d'activité présente les principales réalisations de l'Institut en 2020 et 2021 et témoigne du soutien extraordinaire dont nous avons bénéficié et dont nous sommes profondément reconnaissants.

Stéphane Duguin
Directeur exécutif
CyberPeace Institute

Décembre 2021

MISSION, PRINCIPES FONDAMENTAUX ET OBJECTIFS STRATÉGIQUES

Des milliards de personnes partout dans le monde dépendent d'Internet pour nouer des liens, travailler, faire des affaires, se former et partager des connaissances. Le cyberespace est aussi devenu un facteur de risque croissant dans la vie des gens : lorsqu'une cyberattaque se produit, les êtres humains sont touchés de plein fouet.

Les efforts pour instaurer la paix dans le cyberespace visent avant tout à créer des conditions dans lesquelles chacun peut accéder à l'ensemble des possibilités offertes par la technologie et tirer pleinement profit du cyberespace sans avoir à craindre pour sa sécurité et le respect de sa vie privée.

Afin de remédier à l'escalade des cyberattaques et de contribuer aux conditions nécessaires pour que le cyberespace réalise la promesse de l'ère numérique, l'Institut est une organisation non gouvernementale (ONG) indépendante et neutre dont la mission est de garantir les droits des personnes à la sécurité, à la dignité et à l'équité dans le cyberespace.

En analysant les cyberattaques, l'Institut met en évidence leur impact sociétal ainsi que la manière dont les lois et les normes internationales sont violées, et promeut les comportements responsables pour faire respecter la paix dans le cyberespace.

L'Institut promeut une analyse des cyberattaques fondée sur des éléments concrets et axée sur l'être humain, car il considère une telle approche comme essentielle pour aider les victimes à se remettre et pour leur assurer un droit à réparation.

L'action du CyberPeace Institute et son approche collaborative reposent sur six principes fondamentaux :

INTÉGRITÉ
L'Institut s'attache, dans ses travaux et ses interactions avec les acteurs de la cybersécurité et les victimes de cyberattaques, à se conformer aux normes éthiques et analytiques les plus élevées.

INDÉPENDANCE
L'Institut opère dans la seule poursuite de son objectif et de sa mission, à l'abri de la direction, du contrôle ou de l'ingérence de tout acteur externe, notamment des États, du secteur privé ou d'autres organisations.

INCLUSION
L'Institut agit de manière inclusive et collaborative ; il coopère et recherche des synergies avec des partenaires.

IMPACT
L'Institut réduit la fréquence, les dommages et l'ampleur des cyberattaques en appelant à leur restriction, en faisant progresser la responsabilisation de tous les acteurs concernés et en renforçant les capacités de prévention et de récupération.

NEUTRALITÉ
L'Institut promeut la stabilité et la sécurité dans le cyberespace et non les intérêts des acteurs individuels. À ce titre, il respecte les cadres juridiques applicables pour défendre les victimes de cyberattaques en ne faisant aucune discrimination fondée sur leur situation géographique, leurs convictions philosophiques, politiques ou religieuses, leur nationalité, leur race, leur statut social, leur sexe et leur identité sexuelle, ou leur handicap.

TRANSPARENCE
L'Institut est transparent sur ses propres opérations et sur les méthodologies qu'il applique pour s'acquitter de sa mission.

Afin de mener à bien sa mission et de fournir des produits et des services efficaces, le CyberPeace Institute poursuit quatre objectifs stratégiques :

Objectif stratégique 1 : ASSISTANCE

Accroître et intensifier les efforts d'assistance aux communautés les plus vulnérables dans le monde entier.

Objectif stratégique 2 : ANALYSE

Combler les lacunes en matière de responsabilisation au moyen d'analyses collaboratives des cyberattaques.

Objectif stratégique 3 : SENSIBILISATION

Mettre en avant les lois et les normes internationales afin de promouvoir des comportements responsables dans le cyberespace.

Objectif stratégique 4 : ANTICIPATION

Anticiper et analyser les menaces pour la sécurité créées par les technologies de rupture, proposer des solutions innovantes et renforcer les compétences en vue de relever les défis mondiaux posés par la cybercriminalité.

RÉALISER LA PAIX DANS LE CYBERESPACE

Mai 2020 – décembre 2021

Face aux réalités de la pandémie du COVID-19, l'Institut s'est attaché à délimiter l'impact du virus sur le cyberespace et la cybersécurité. Le COVID-19 a eu des répercussions sur les sociétés à tous les niveaux, y compris sur le monde numérique. En effet, la pandémie a intensifié le recours aux outils numériques dans les sphères économiques et sociales, engendrant une dépendance croissante à ces technologies et, partant, une augmentation des cybermenaces.

Les criminels et les acteurs étatiques savent très bien exploiter l'incertitude qui entoure des situations de crise comme la pandémie pour renforcer leurs activités malveillantes et les profits qu'ils tirent des cyberattaques (en particulier l'envoi de spams malveillants et l'hameçonnage).

L'« infodémie », c'est-à-dire le déferlement d'informations fausses ou trompeuses, couplée à l'intensification des théories du complot induites par la pandémie ont été exploitées par des acteurs malveillants pour éroder la confiance de la société dans le secteur de la santé et dans les vaccins, et même pour remettre en cause l'existence du virus. Les cyberattaques dirigées contre les hôpitaux et d'autres acteurs du monde médical augmentent et entravent la capacité du secteur à fournir des soins de qualité et à allouer efficacement les ressources disponibles.

L'Institute a lancé une série d'initiatives opérationnelles conçues spécifiquement pour ce secteur en vue de fournir une assistance, de promouvoir la responsabilisation de tous les acteurs et de faire prévaloir des comportements responsables dans le cyberespace. Ces initiatives visaient en particulier à renforcer la résilience des infrastructures civiles essentielles et à protéger les communautés les plus vulnérables.

DE LA THÉORIE À L'ACTION : LE PROGRAMME CYBER4HEALTHCARE

La pandémie du COVID-19 a créé une nouvelle réalité pour le secteur de la santé en testant ses limites partout dans le monde. En effet, des acteurs malveillants ont profité des circonstances pour lancer une série de campagnes d'hameçonnage et de rançongiciels contre les établissements de santé. Les hôpitaux ne peuvent tout simplement pas se permettre d'interrompre leurs opérations pour parer à une cyberattaque, c'est pourquoi ils sont généralement plus enclins que d'autres institutions à payer pour protéger leurs patients.

En tant que fournisseur de services essentiels et souvent même vitaux, le secteur de la santé doit être interdit de toute intention ou action malveillante, protégé par et pour tous.

Avec son programme Cyber4Healthcare (C4H), lancé en mai 2020, l'Institut est parvenu à réunir le secteur privé et la société civile autour d'un objectif ambitieux : faire cesser les cyberattaques contre le secteur de la santé et renforcer sa résilience.

> *« Le secteur de la santé fait face à une succession de cyberattaques systémiques qui mettent en danger non seulement ses systèmes, mais aussi la vie des patients. »*
>
> **Stéphane DUGUIN, Directeur exécutif du CyberPeace Institute**

PROGRAMME CYBER4HEALTHCARE (C4H)

Formuler l'enjeu : lancement de l' Appel aux gouvernements, demandant aux États de s'engager résolument à mettre un terme aux attaques contre le secteur de la santé.

Plus de 40 dirigeants internationaux issus de gouvernements, du secteur privé, d'organisations internationales, d'ONG et du monde universitaire ont rallié l'appel aux gouvernements à prendre des mesures fermes et immédiates pour mettre fin aux cyberattaques perpétrées contre le secteur de la santé.

Apporter une aide concrète : mise en place de la plateforme Cyber4Healthcare, avec le concours d'entreprises disposées à offrir un soutien direct aux communautés vulnérables.

Avec son programme Cyber4Healthcare, l'Institut a renforcé le soutien apporté aux communautés vulnérables dans le secteur de la santé ayant été victimes de cyberattaques en les mettant en lien avec des partenaires privés disposés à fournir une assistance gratuite en matière de cybersécurité aux organisations actives dans ce secteur, où qu'elles se trouvent dans le monde. Au total, le programme a servi à 18 organisations actives dans sept pays, à savoir au Cameroun, en France, en Haïti, en Inde, au Kenya, au Nigéria et en Suisse.

> *[Grâce au soutien du CyberPeace Institute,] « ... nous avons évité un piratage de données qui aurait pu engendrer de graves perturbations. [...] Nous remercions le CyberPeace Institute d'aider des start-up actives dans le secteur de la santé, comme OneHealth, à mieux se protéger sur Internet. Nous pouvons dès lors nous concentrer sur notre mission : secourir les gens quand ils en ont besoin et en toute sécurité. »*
>
> **Adeola ALLI, Directrice exécutive, OneHealth, Kenya, février 2021**

Formuler et publier des recommandations et des conseils pratiques : *Nos vies en péril : pirater la santé, c'est attaquer les personnes*. Rapport d'analyse stratégique formulant des recommandations pratiques à l'intention des États, du secteur privé et des ONG.

Le rapport compile pour la première fois des informations sur les cyberattaques perpétrées contre le secteur de la santé et démontre toute la complexité, l'ampleur et la violence des menaces auxquelles les établissements de santé sont soumis, qu'il s'agisse de demandes de rançons, de la désinformation ou du cyberespionnage dans le contexte du COVID-19.

Le Rapport présente des constatations qui mettent en parallèle l'ampleur des cyberattaques perpétrées dans le secteur de la santé et l'impact de ces offensives sur leurs victimes. Il en ressort que, face à la menace croissante à laquelle les professionnels de santé et les patients sont confrontés, une action collective est non seulement possible, mais aussi nécessaire. Les principales constatations du rapport sont les suivantes :

- **Les attaques contre la santé causent des dommages directs aux personnes et constituent une menace à l'échelle mondiale.**
- **Les attaques augmentent et évoluent, les auteurs continuant de profiter de la fragilité des infrastructures numériques de la santé et de ses faiblesses en**

matière de cybersécurité.

- **Les attaques contre la santé sont des crimes peu risqués et très lucratifs.**
- **Les dispositifs juridiques et les initiatives d'aide au secteur médical ne sont pas suffisamment mis à profit.**
- **Les gouvernements doivent montrer la voie pour protéger la santé. Ils doivent faire respecter les normes et les lois nationales et internationales, s'engager à ne pas nuire et déclarer illégaux le cyberespionnage ainsi que la collecte de renseignements ciblant la santé.**
- **La santé a besoin d'investissements afin de se protéger.**
- **Compte tenu de son rôle dans le développement des technologies médicales, le secteur privé détient sa part de responsabilité.**

Passer des recommandations à l'action pour promouvoir la responsabilisation : Cyber Incident Tracer #HEALTH et Additif au Rapport d'analyse stratégique Nos vies en péril : ***pirater la santé, c'est attaquer les personnes***[1]

Pour donner suite à la première recommandation du Rapport d'analyse stratégique, qui propose de détailler les attaques et d'analyser leur impact sur l'homme et la société, l'Institut a développé une plateforme publique visant à renforcer la transparence et l'accès à l'information sur les cyberattaques contre le secteur de la santé. Les données recueillies sur cette plateforme ont été analysées dans l'Additif au Rapport d'analyse stratégique, qui est une source d'information précieuse pour les responsables qui fondent leurs décisions opérationnelles, politiques et juridiques sur des faits.

[1] Addendum to the Strategic Analysis Report *Playing with Lives: Cyberattacks on Healthcare are Attacks on People* (en anglais seulement)

La grande expertise de l'Institut en font un partenaire fiable et renommé. Il collabore ainsi avec des autorités sanitaires actives au niveau mondial, notamment avec l'Organisation mondiale de la Santé (OMS), sur l'interconnexion entre l'infodémie autour du COVID-19 et les cyberattaques. Dans le cadre de son approche multipartite, l'Institut a aussi collaboré avec Microsoft et le Ministère des affaires étrangères de la République tchèque pour promouvoir la protection du secteur de la santé contre les cybermenaces.

PRINCIPALES RÉALISATIONS

Objectif stratégique 1 : ASSISTANCE

L'Institut aide les communautés vulnérables et les ONG à se préparer aux cyberattaques et à s'en remettre. Nous mobilisons à cette fin des sympathisants et des volontaires et nous renforçons l'impact des efforts d'assistance déjà déployés.

◊ Au cours de la période considérée, l'Institut a reçu 114 demandes d'assistance en provenance d'Europe, d'Amérique latine, d'Afrique et d'Asie.

- ***Formations et outils à l'usage des ONG humanitaires :***

◊ L'Institut a élaboré 22 kits d'information en anglais, en français et en swahili afin de présenter aux populations des bonnes pratiques et les aider ainsi à renforcer leur résilience face aux cyberattaques.

◊ L'Institut a aidé plusieurs organisations et réseaux de la société civile, notamment le Fonds mondial et le Centre international de la société civile (International Civil Society Centre), à renforcer leurs capacités en matière de cybersécurité. Au total, 18 séances de formation réunissant plus de 400 participants ont été organisées.

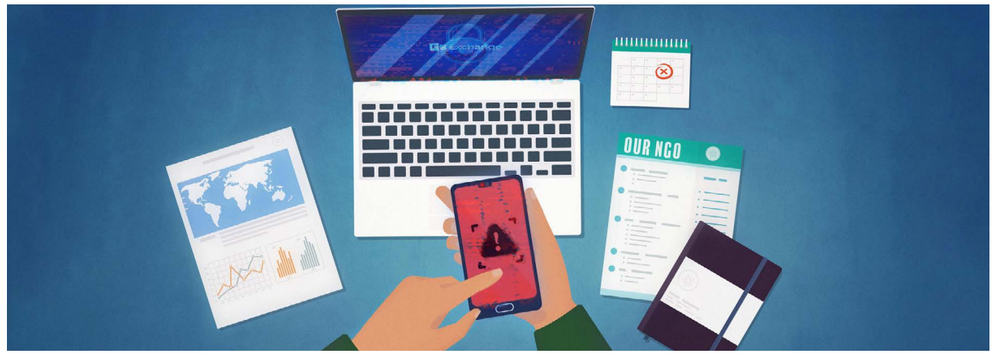
- *CyberPeace Builders*
  - ◊ Les ONG contribuent pour beaucoup au développement de la société, au renforcement des communautés et à la promotion de la participation des citoyens, et soutiennent la réalisation des Objectifs de développement durable (ODD). Elles sont actives dans de nombreux pays en développement pour garantir l'accès des populations à des services essentiels comme les soins et la nourriture, mais aussi à l'information et la protection des droits de l'homme.
  - ◊ Des acteurs malveillants ciblent aujourd'hui déjà des ONG actives dans les secteurs humanitaire et du développement en vue d'obtenir des rançons et d'exfiltrer des données. Ces organisations n'ont souvent pas le budget, le savoir-faire et le temps nécessaires pour sécuriser efficacement leurs infrastructures et pour mettre en place des mécanismes de réponse solides leur permettant de gérer et de surmonter des attaques sophistiquées.
  - ◊ Face à cette situation, l'Institut a lancé en 2021 le CyberPeace Builders, premier réseau de professionnels volontaires voués à fournir une assistance en matière de cybersécurité aux ONG qui soutiennent les populations vulnérables.
  - ◊ Les CyberPeace Builders aide les ONG à se préparer aux cyberattaques et à s'en remettre. Cette initiative apporte aux organisations actives dans des secteurs critiques un soutien d'une ampleur jusque-là inégalée en termes de ressources humaines, d'outils et de capacités.
  - ◊ Vingt organisations à but non lucratif ont bénéficié de ce programme et six entreprises ont mis à disposition des volontaires.
  - ◊ Les capacités ont été renforcées en 2021 dans la perspective de mettre le programme à disposition également en Afrique et en Amérique latine en 2022.

> *« Nous avons apprécié la relation de confiance établie avec le CyberPeace Institute, qui s'est efforcé de trouver des solutions adaptées à nos enjeux en matière de sécurité, notamment pour protéger les données de nos bénéficiaires. Le nouveau programme CyberPeace Builders apporte une importante valeur ajoutée aux ONG ici à Genève, mais aussi ailleurs dans le monde, car ces organisations seront mieux armées pour relever les défis numériques d'aujourd'hui. »*
>
> **Pascal CARPENTIER, Responsable des systèmes d'information et de la technologie, Drugs for Neglected Diseases initiative (DNDi), Genève**

Objectif stratégique 2 : ANALYSE

L'Institut réalise, facilite et coordonne des analyses, des recherches et des enquêtes collectives sur les cyberattaques visant les communautés vulnérables, afin d'amener les auteurs de ces offensives à répondre de leurs actes.

- *Analyses de données et rapports d'analyse scientifique*
  - ◊ L'Institut a produit des analyses sur 5 cyberattaques et a joué le rôle de centre d'échange d'informations en vue d'identifier les cibles et d'avertir les victimes.
  - ◊ Des rapports d'analyse scientifique ont été établis et communiqués de manière confidentielle au réseau de partenaires et bénéficiaires de l'Institut.



- *Impact sociétal des attaques par rançongiciel*
  - ◊ L'Institut a dirigé un groupe de travail ad hoc au sein de l'équipe spéciale de lutte contre les rançongiciels (Ransomware Task Force) de l'Institut pour la sécurité et la technologie. Le groupe de travail s'est employé à formuler une série de recommandations concrètes pour lutter contre les rançongiciels et a évalué l'impact sociétal de ce type d'attaque.
  - ◊ Fort de ces nouvelles connaissances, l'Institut a organisé un atelier sur les rançongiciels. S'adressant aux journalistes, cet atelier visait à mettre en commun les connaissances et expériences en la matière et à renforcer l'élément humain dans la communication sur les rançongiciels. L'atelier a été le fruit d'une collaboration entre le CyberPeace Institute, la Global Cyber Alliance et Swissnex à Boston et à New York.
- *Cybercapacités offensives (Offensive Cyber Capabilities – OCCs) et technologies de surveillance*

◊ L'Institut s'est joint à l'effort déployé au niveau international pour dénoncer et combattre l'utilisation de cybercapacités offensives très intrusives contre des dissidents, des opposants politiques, des journalistes, des avocats, des enquêteurs internationaux et d'autres membres de la société civile. Il a ainsi fourni gratuitement des outils d'investigation et un soutien pour détecter les logiciels espions. Il a également contribué au développement de la « Digital Violence Platform » lancée par le groupe de recherche Forensic Architecture, et s'est joint aux préoccupations d'un groupe d'experts en premier plan demandant un moratoire mondial sur la vente et le transfert de technologies de surveillance jusqu'à ce que des mesures strictes de protection des droits de l'homme soient adoptées.

Objectif stratégique 3 : SENSIBILISATION

L'Institut rappelle aux acteurs étatiques et non étatiques le droit international et les normes régissant des comportements responsables dans le cyberespace, et contribue à faire progresser l'état de droit pour réduire les dommages et garantir le respect des droits des personnes dans le cyberespace.

- *Contribution à des processus majeurs de l'ONU*

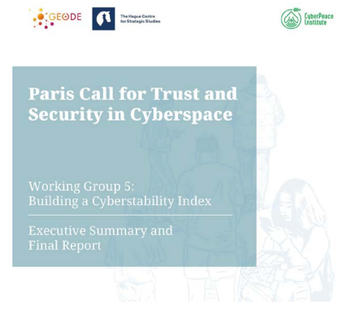
  ◊ L'Institut a contribué et offert son expertise à plusieurs processus de l'ONU, (notamment au Groupe d'experts gouvernementaux chargé d'examiner les moyens de favoriser le comportement responsable des États dans le cyberespace dans le contexte de la sécurité internationale et au Groupe de travail sur l'utilisation de mercenaires comme moyen de violer les droits de l'homme et d'empêcher l'exercice du droit des peuples à disposer d'eux-mêmes).

  ◊ L'Institut suit de près les travaux du Groupe de travail à composition non limitée sur les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale, et milite pour que le secteur de la santé soit envisagé comme une infrastructure essentielle et met en garde contre le manque d'engagement en faveur d'une approche fondée sur des éléments concrets et axée sur l'être humain.

- *Participation à des initiatives internationales de premier plan : les groupes de travail de l'Appel de Paris*

  ◊ L'Institut a co-présidé, aux côtés du centre de recherche Géopolitique de la Datasphère (GEODE – Université Paris 8) et du Hague Center for Strategic Studies, le Groupe 5 de l'Appel de Paris chargé de « construire un index de stabilité du cyberespace ».

  ◊ Le groupe de travail a consigné les résultats de ses travaux dans un rapport final[2] qui a été publié en 2021 à l'occasion de la quatrième édition du Forum de Paris sur la paix. Il a établi une méthodologie afin de montrer comment la mise en œuvre de mesures normatives, juridiques, opérationnelles et techniques contribue à la stabilité et, in fine, à la paix dans le cyberespace.



  ◊ L'Institut a par ailleurs contribué aux travaux du Groupe 3 chargé de « promouvoir une approche multi-acteurs dans le cadre des négociations cyber à l'ONU ». Ce groupe a également fait état de ses travaux dans un rapport final[3].

- *Manifeste multipartite*

  ◊ En vue des défis liés à la négociation de la nouvelle convention des Nations Unies sur la cybercriminalité, intitulée Lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles, le CyberPeace Institute et le Cybersecurity Tech Accord ont réuni plus de 60 parties prenantes pour publier un Manifeste multipartite sur la cybercriminalité. Les signataires du Manifeste ont énoncé un ensemble de principes qui, selon eux, doivent être au cœur de toute législation sur la cybercriminalité et orienter le processus de négociation de la nouvelle convention, en mettant l'accent sur la nécessité de protéger les droits de l'homme.

> *« La participation d'acteurs issus de la société civile, du secteur privé et du monde universitaire aux travaux de ce groupe de travail a mis en évidence la nécessité d'une coopération multipartite pour renforcer la cybersécurité. Les nombreuses contributions écrites de parties prenantes sur le site web du groupe, notamment celles du CyberPeace Institute, montrent ce que peut apporter une telle coopération. »*
>
> **Ambassadeur Jürg LAUBER, Représentant permanent de la Suisse auprès de l'Office des Nations Unies et des autres organisations internationales à Genève, mars 2021**

[2] Appel de Paris pour la confiance et la sécurité dans le cyberespace, Working Group 5: Building a Cyberstability Index – Executive Summary and Final Report (en anglais seulement)
[3] Multistakeholder participation at the UN: The need for greater inclusivity in the UN dialogues on cybersecurity (en anglais seulement)

Objectif stratégique 4 : ANTICIPATION

L'Institut anticipe et étudie les opportunités, les menaces et les risques créés par les technologies de rupture, et il analyse les nouveaux défis mondiaux liés au cyberespace.

- *Technologies de rupture et cyberespace*
  - ◊ L'Institut a élaboré un cadre de référence pour l'anticipation des opportunités, menaces et risques créés par les technologies de rupture. Pour ce faire, il a recueilli des avis d'experts à l'occasion d'un atelier sur les technologies de rupture et le cyberespace et a analysé les enjeux fondamentaux posés par les technologies de rupture et par la convergence des technologies,en particulier leur impact sur la paix dans le cyberespace
- *Intelligence artificielle et communautés vulnérables*
  - ◊ Il a été établi que les médiateurs de paix sont exposés à des risques dans leurs interactions avec les technologies existantes et les technologies émergentes. L'Institut a exploré l'utilisation actuelle et future de l'intelligence artificielle (IA) dans les processus de médiation en analysant en particulier les opportunités et les risques liés aux technologies d'IA, mais aussi leur impact sociétal, qui est souvent négligé.

STRUCTURE ET RESSOURCES HUMAINES

Gouvernance

Conseil d'administration

Le Conseil d'administration est l'organe directeur suprême du CyberPeace Institute. Il détient les pouvoirs les plus élevés et les plus étendus en matière de prise de décision et d'administration. Il est composé d'éminents experts et de personnes à la tête de l'action pour la paix numérique.

Membres en exercice pendant la période considérée :

- Alejandro Becerra Gonzalez, Directeur mondial de la sécurité de l'information, Telefonica
- Kelly Born, Directrice, Cyber Initiative, The Hewlett Foundation
- Merle Maigre, Experte principale sur la cybersécurité, e-Governance Academy (eGA)
- Alexander Niejelow, Premier Vice-Président de la Coordination et promotion de la cybersécurité, Mastercard
- Kate O'Sullivan, Directrice générale de la Diplomatie numérique, Microsoft
- Martin Vetterli, Président, Ecole Polytechnique Fédérale de Lausanne (EPFL)

Membres en exercice avant la période considérée :

- Khoo Boon Hui, Président, INTERPOL (2008-2012)
- Anne Marie Slaughter, Directrice exécutive, New America
- Brad Smith, Président et Vice-Président, Microsoft
- Eli Sugarman, Directeur des contenus (modération), Oversight Board

Direction et personnel

L'Institut est composé de professionnels de haut niveau issus de différents horizons et réunissant un large éventail de compétences en matière de technologie et de cybersécurité, mais aussi dans d'autres domaines.

Membres de l'équipe de direction :

- Marietje Schaake, Présidente (2019-2021)
- Stéphane Duguin, Directeur exécutif
- Francesca Bosco, Directrice de la stratégie
- Bruno Halopeau, Directeur de la technologie
- Klara Jordan, Directrice des affaires publiques et gouvernementales
- Charlotte Lindsey (Curtet), Directrice de la communication
- Adrien Ogée, Directeur des opérations

Effectifs

Au 31 décembre 2021, l'Institut comptait 33 employés, à savoir 20 femmes (60,6 %) et 13 hommes (39,4 %). Treize nationalités sont représentées.

Conseil consultatif

Le Conseil consultatif soutient l'Institut dans ses activités en mettant à sa disposition une expertise et une analyse critique qui contribuent à la réalisation de ses objectifs stratégiques. Le Conseil consultatif est composé de 16 membres dont les parcours et les compétences sont très variés. Les membres sont nommés pour une période de deux ans et siègent à titre personnel.

COLLABORATIONS ET RÉSEAU

L'approche multipartite de l'Institut

L'Institut est convaincu que pour opérer des changements concrets, plusieurs acteurs, secteurs et industries doivent travailler ensemble. Aussi, face aux défis complexes auxquels il est confronté dans son action pour garantir la paix dans le cyberespace, l'Institut collabore avec de nombreux acteurs au niveau mondial, issus aussi bien du secteur privé, de la société civile, du monde universitaire et d'organisations philanthropiques que d'institutions ayant un pouvoir de décision politique. Il contribue aux efforts de paix dans le cyberespace en mettant à disposition des connaissances fondées sur des faits, en faisant valoir la nécessité d'adopter une approche axée sur l'être humain dans les projets et processus techniques et politiques, et en mettant en avant la perspective de la société civile pour soutenir et faire connaître les initiatives existantes.

L'Institut s'est associé à plusieurs initiatives en accord avec sa mission et ses valeurs. Il a mis à disposition son expertise, a amplifié l'action d'autres institutions et a fait entendre la voix de la société civile dans certaines initiatives multipartites. Il est notamment membre du Global Forum on Cyber Expertise (GFCE) (Forum mondial sur la cyber expertise), un réseau regroupant divers acteurs clés chargés de renforcer les capacités dans le cyberespace à l'échelle mondiale.

Face à la menace hybride posée par les groupes criminels et les acteurs étatiques, les partenariats réunissant des acteurs issus des secteurs privé et public sont essentiels et bénéfiques pour la société en général. Aussi, l'Institut s'est associé à la Coalition Against Stalkerware (Coalition contre les logiciels de traque), qui a conduit de nombreuses organisations à se mobiliser contre la surveillance privée en donnant la priorité aux intérêts des victimes.

Le rôle clé de la Suisse et de la Genève internationale[4]

L'Institut s'est établi à Genève, ville hôte de nombreuses institutions internationales. Genève constitue un pôle de compétences reconnu en matière de coopération internationale et accueille notamment des organisations actives dans les secteurs humanitaire et des droits de l'homme. Soucieux de s'intégrer et de participer à l'écosystème de la région, l'Institut est membre de la Chambre de commerce, d'industrie et des services de Genève (CCIG).

L'Institut a collaboré avec plusieurs établissements universitaires pendant la période

[4] Les collaborations dont il est question dans cette section sont mentionnées à titre d'exemples et non de manière exhaustive. L'Institut s'emploie actuellement à élargir son réseau en explorant diverses possibilités de collaboration à Genève et ailleurs en Suisse.

considérée. Il a ainsi participé à des conférences, des ateliers et des cours, notamment au sein de l'EPFL – en particulier du Center for Digital Trust (C4DT) –, de l'Université de Genève et de l'Institut de hautes études internationales et du développement.

En septembre 2020, l'Institut s'est associé à la Trust Valley, un partenariat public-privé et centre d'expertise qui promeut la confiance numérique et la cybersécurité.

L'Institut a entamé des collaborations prometteuses notamment avec Swissnex et la division Numérisation du Département fédéral des affaires étrangères (DFAE).

> *« La présence de l'Institut [à Genève] renforce notre capacité à offrir des solutions innovantes à des défis particulièrement complexes auxquels l'humanité fait face. »*
>
> **Nathalie FONTANET, Conseillère d'État du canton de Genève, décembre 2020**

Awards

L'Institut a été lauréat de plusieurs prix au cours de leurs deux premières années d'activité. Ils ont été récompensés pour leurs efforts innovants et assidus dans la promotion de la paix dans le cyberespace.

2020

- Deuxième Prix de l'innovation en matière de sécurité mondiale décerné par le Centre de politique de sécurité de Genève

2021

- Premier Prix de l'innovation en matière de sécurité mondiale décerné par le Centre de politique de sécurité de Genève

- Prix de l'Économie décerné par la Chambre de commerce, d'industrie et des services de Genève (CCIG)

COMMUNICATION

L'Institut a dès le début axé sa stratégie de communication sur un double objectif : devenir une référence incontournable pour les questions relatives à la paix dans le cyberespace et atteindre un public essentiel et varié de manière à :

- faire connaître ses travaux ainsi que les menaces qui pèsent sur la paix dans le cyberespace ;
- diffuser des messages clés et stimuler l'action sur des thèmes et problèmes majeurs ;
- informer et orienter les responsables politiques, les gouvernements et les professionnels sur les questions relatives à la paix dans le cyberespace ;
- mener, aux côtés d'autres organisations de la société civile, une action de sensibilisation en vue de faire changer les mentalités, les pratiques et les comportements ;
- contribuer à des objectifs de financement.

PRINCIPAUX OUTILS DE COMMUNICATION

L'Institut communique en ligne par le biais de son site web et de sa présence sur les réseaux sociaux, ses principaux publics cibles sachant très bien accéder à des documents et à des informations sur Internet. En 2021, l'Institut a publié un Appel aux gouvernements ainsi que le Rapport d'analyse stratégique Nos vies en péril : pirater la santé, c'est attaquer les personnes et son additif. Il a aussi lancé la plateforme Cyber Incident Tracer #HEALTH, le programme le CyberPeace Builders et un Manifeste multipartite. Des activités de communication ont fait un large écho à la participation de l'Institut à différents événements publics, tels que le Sommet mondial sur les droits humains à l'ère numérique RightsCon et le Forum de Paris sur la paix.

Principales réalisations et chiffres clés pour la période considérée :

- **Site web**
  - ◊ En 2021, quelque 55 articles et blogs ainsi que 10 communiqués de presse ont été publiés sur le site web de l'Institut. Des sujets et problèmes clés ont été abordés, notamment les contributions de l'Institut à divers forums de l'ONU, les cyberattaques dirigées contre les ONG humanitaires et celles visant le secteur de la santé. De nombreuses communications ont également été publiées en français.

- **Réseaux sociaux**
  - ◊ L'Institut est présent sur Twitter, LinkedIn, YouTube, Instagram et Facebook. Le nombre d'abonnés sur ses plateformes Twitter et LinkedIn a ainsi augmenté respectivement de 47.5 % et 86.3 %.

- **Vidéos**
  - ◊ 15 vidéos ont été produites sur des thèmes clés tels que les cyberattaques visant le secteur médical et les ONG humanitaires.

- **Bulletin d'information**
  - ◊ L'Institut a publié son premier bulletin d'information au cours du dernier trimestre de 2021. Cette publication mensuelle présente de manière condensée des histoires percutantes en lien avec le cyberespace.

- **Mobilisation des médias**
  - ◊ L'Institut s'est attaché en 2021 à mobiliser les médias tant généraux que spécialisés. Il a ainsi bénéficié d'une vaste couverture médiatique en anglais et en français, avec notamment un article sur le Cyber Incident Tracer #HEALTH en première page du Financial Times, un article dans la revue Foreign Policy, un film pour la série Defenders of Digital consacré exclusivement à son travail, et des articles dans des journaux comme le quotidien suisse Le Temps.

- **Événements**
  - ◊ Des experts de l'Institut ont participé à un rythme quasi hebdomadaire à des événements en tant qu'intervenants principaux. Les réseaux sociaux se sont fait l'écho de leur contribution en relayant les défis liés à la réalisation de la paix dans le cyberespace, ainsi que des recommandations en la matière.

FINANCEMENT

Conformément à son principe fondamental d'indépendance, l'Institut fonctionne à l'abri de la direction, du contrôle ou de l'ingérence de tout acteur externe, notamment des États, du secteur privé ou d'autres organisations.

Le CyberPeace Institute compte sur les dons volontaires. Il collecte des fonds de manière indépendante pour soutenir ses opérations, en acceptant les dons compatibles avec sa mission, ses principes et ses normes de diligence raisonnable. Le rapport financier analyse les 14 premiers mois d'activité de l'Institut, du 15 novembre 2019 au 31 décembre 2020. Les comptes de l'Institut ont été contrôlés par l'organe de révision Deloitte conformément aux exigences légales.

Financial report

SOUTENIR L'ACTION DU CYBERPEACE INSTITUTE

Au cœur du cyberespace se trouvent des vies humaines. Fort de ce constat, le CyberPeace Institute soutient les entités et les personnes qui fournissent des services essentiels aux groupes les plus vulnérables de la société et qui, par là même, servent l'ensemble de la société, telles que les ONG et les personnels de santé. Les attaques dirigées contre ces organisations et ces professionnels peuvent avoir de graves conséquences sur respectivement leurs bénéficiaires et leurs patients, dont les droits et même la vie sont mis en péril.

Pour mener à bien sa mission, l'Institut dépend des dons et de la générosité de particuliers, de fondations, d'entreprises et d'autres sympathisants. Ce soutien permet à l'Institut d'aider les ONG à protéger leurs ressources et à renforcer leur résilience face aux cyberattaques. Il lui permet aussi de mettre à disposition des connaissances fondées sur des faits, de sensibiliser la société à l'impact qu'ont les cyberattaques sur les personnes, de donner aux victimes les moyens de faire valoir leurs droits légitimes, et de faire entendre la voix de ces personnes, mais aussi de l'ensemble des acteurs qui s'engagent pour que le monde parvienne à garantir un avenir numérique sûr pour tous.

Le CyberPeace Institute est une organisation non gouvernementale indépendante et neutre dont la mission est de garantir les droits des personnes à la sécurité, à la dignité et à l'équité dans le cyberespace. L'Institut travaille en étroite collaboration avec les partenaires concernés pour réduire les dommages causés par les cyberattaques sur la vie des gens dans le monde entier, et leur fournir une assistance. En analysant les cyberattaques, l'Institut met en évidence leur impact sociétal ainsi que la manière dont les lois et les normes internationales sont violées, et promeut les comportements responsables pour faire respecter la paix dans le cyberespace.

CyberPeace Institute
Campus Biotech Innovation Park
Avenue de Sécheron 15,
1202 Genève, Suisse

cyberpeaceinstitute.org
@CyberPeace Institute
@CyberpeaceInst
@CyberpeaceInst