Forum Suisse de Politique Internationale

Interview de Madame Solange Ghernaouti
Professeure, Directrice du Swiss Cybersecurity Advisory & Research Group (SCARG),
Université de Lausanne,
Présidente de la Fondation SGH-Institut de recherche Cybermonde.

9 novembre 2020

FSPI : L'histoire a montré que quand nouveau un champ de savoir prend de l'importance dans la société il se masculinise. Vous êtes un magnifique contre-exemple, car la cybersécurité est un domaine qui peine à s'ouvrir aux femmes et ce alors que la branche fait face à une pénurie d'experts. Comment améliorer la place des femmes dans ce secteur et lutter contre les stéréotypes dans les formations dites techniques ?

Solange Ghernaouti: Promouvoir la diversité et la place des femmes dans les milieux professionnels et les cercles dirigeants est fondamental dans bien des domaines. Divers évènements existent pour mettre en avant des parcours exceptionnels de professionnelles engagées et promouvoir l'importance des femmes en cybersécurité. Ainsi par exemple, le Cercle des femmes de la cybersécurité a le 27 octobre à Paris, réalisé une cérémonie de remise de Trophée de la Femme Cyber 2020. Ce dernier a été créé lors du Forum International de la Cybersécurité de Lille pour avoir lieu en marge du mois européen dédié à la sensibilisation à la cybersécurité.

C'est dans la catégorie Dirigeante & Entrepreneure que j'ai été distinguée pour la reconnaissance de mon expertise et engagement dans les cercles dirigeants aux niveaux national, européen et international ainsi que pour mon rôle de pionnière et de leader en matière d'approche transdisciplinaire de la cybersécurité. Ce trophée vient compléter la dizaine de distinctions qui jalonne mon activité professionnelle et qui contribue à rendre visible le rôle des femmes.

FSPI : Au titre de diverses initiatives internationales souhaitant faire de Genève un hub en matière de régulation du cyberespace (Swiss Digital Initiative), Microsoft s'est placé en acteur incontournable de la cyberdiplomatie. Ne doit-on pas craindre que l'influence des multinationales dans l'établissement des règles de jeu de l'économie du numérique dépassent celles des acteurs étatiques et des milieux issus de la société civile ?

Solange Ghernaouti: Depuis de nombreuses années, partout dans le monde le lobby auprès des acteurs étatiques et non étatiques, des multinationales du numérique est effectif. Leurs actions d'influence sont efficaces pour imposer leurs visions et outils du numérique, dans tous les secteurs d'activités et dans

tous les aspects de la vie. L'emprise de ces organisations sur la société est considérable, comme l'est d'ailleurs leur empire et leur puissance économique qui se sont développés à partir d'une promesse sans engagement d'émancipation et de liberté et d'une illusion du « gratuit ».

Le numérique exerce un pouvoir de fascination auprès des dirigeants et de la population qui masque sa puissance ontologique de domination, de transformation et de déstabilisation de la société. Cette «hypnose» empêche de penser et de développer d'autres modèles économiques et avenirs techniques possibles. Elle phagocyte l'imaginaire et contribue à alimenter l'utopie d'un profit infini d'un capitalisme numérique néo-libéral. Les problèmes écologiques que génère la fabrication, l'exploitation et la consommation du numérique sont ignorés des acteurs hégémoniques, comme le sont d'ailleurs les impacts et les coûts des nouveaux risques cyber qu'ils ont contribués à engendrer et qui sont supportés par la société.

Les entreprises transnationales de l'Internet, organisées en oligopole, se comportent en prédateurs. Le jeu de la concurrence est faussé, le tissu socio-économique des pays dans lesquelles elles sont implantées se délite. Sans réel contre-pouvoir, elles savent tirer parti de l'absence de réglementation contraignante en particulier dans le domaine de la fiscalité. Echappant à un impôt à la hauteur des valeurs captées et des profits engendrés, elles renforcent leur puissance par des dispositifs techniques et des usages conçus pour maximaliser toujours plus leur profitabilité et augmenter la dépendance.

Le difficile contrôle de ces compagnies, qui sont en mesure de racheter ou d'anéantir toutes entreprises concurrentes, leur confère un pouvoir politique et économique d'envergure, auquel se soumettent les acteurs étatiques et non étatiques.

De nombreux partenariats sont établis avec les institutions publiques, y compris dans le domaine de la recherche et de l'enseignement pour entretenir l'illusion d'une coopération au service de la société. Cela participe à faire accréditer par l'académie et la société civile des pratiques numériques, ce qui contribue à les développer et à les rendre incontournables.

Renforcer l'image « sociale » positive de ces compagnies, masquer leur côté prédateur et les impacts directs et indirects du développement du numérique et de la transformation de la société, par des actions qui semblent relever de la philanthropie, fait également partie des stratégies de consolidation de leur puissance.

Devenues intermédiaire-médiateur indispensables, que cela soit au sein des territoires, des villes ou des familles, que cela soit dans les domaines de l'énergie, de la santé, de l'éducation, des moyens de communications, des chaînes d'approvisionnement, de la finance, du travail, du divertissement, ou encore dans des missions régaliennes de l'Etat, ces multinationales établissent des rapports de force asymétrique. En position de force, elles contribuent à affaiblir les entités qui en dépendent.

Ces acteurs ont un réel pouvoir de coercition en imposant de nouvelles normes socioéconomiques. L'adoption massives des pratiques numériques a un effet « trou noir » démultiplicateur et catalyseur de leur puissance. Les multinationales du numérique instaurent un nouvel ordre du monde en imposant de nouveaux modèles de domination, de surveillance et de contrôle. L'administration algorithmique des vies professionnelles et privées est une réalité, la main invisible des algorithmes s'est substituée à celle du marché.

Il est certain que les règles du jeu de l'économie numérique, de l'économie de la donnée et de celle concomitante de la surveillance et de l'intelligence artificielle sont fixées par les acteurs les plus forts. Les multinationales du numériques savent très bien utiliser, l'image de marque de la Suisse et de la Genève internationale, avec une certaine complaisance des acteurs locaux, pour défendre leurs intérêts et conforter leur pouvoir et renommée.

A travers diverses initiatives, Microsoft par exemple, en utilisant notamment le vocabulaire, l'imagerie associés à la Croix-Rouge et aux Nations Unies, se place en acteur non questionnable et se positionne au niveau des Etats pour discuter des questions de (non) régulation du cyberespace. Cela est d'ailleurs également le cas des autres multinationales qui sont toutes actives dans le domaine de la diplomatie Cyber.

Au-delà de l'aspect lié au pouvoir et à la puissance technico-économique et politique de ces entreprises, c'est avant tout une vision du monde (et de l'espace extra atmosphérique) et aussi des modes de vie, qui sont en cause. Ces entreprises, en instaurant de nouvelles pratiques, de nouvelles manière d'être au

monde, de penser, d'agir, de communiquer, de se déplacer, de faire de la politique, de commercer, ou encore « d'augmenter l'humain », ont un réel pouvoir de remaniement du vivant et de transmutation de la société. Le marché est gigantesque et les perspectives économiques illimitées.

FSPI : S'agissant de la gouvernance du cyberespace, deux logiques s'affrontent, l'une cherchant à donner aux États des outils contraignants, l'autre visant à empêcher l'adoption de telles mesures. Par ailleurs, il y a une certaine asymétrie entre les multinationales du numérique dont on ne connaît finalement pas grand-chose et leurs utilisateurs (organisations publiques et privées, individus, y compris les dirigeants politiques et économiques) dont elles connaissent tout. Quelles sont à votre avis, la place de la Suisse et les perspectives d'avenir en matière de cybersécurité ?

Solange Ghernaouti: Aborder l'avenir nécessite de recourir au passé, de faire un rapide détour sur l'évolution des initiatives internationales dans ce domaine. C'est à Genève que la première phase du Sommet mondial sur la société de l'information organisé par l'Union Internationale des Télécommunications (UIT) s'est déroulé en 2003 avec notamment la ligne d'action C5, dédiée à la cybersécurité « Établir la confiance et la sécurité dans l'utilisation des TIC ». La seconde phase a eu lieu à Tunis et a donné naissance en 2006 au Forum sur la Gouvernance de l'Internet (IGF), dont l'objet est de traiter des questions de politique publique de l'Internet.

C'est aussi à Genève sous les auspices de l'UIT, que la concertation internationale «Global Cybersecurity Agenda» a proposé, en 2008 des recommandations stratégiques de cybersécurité. Ces travaux constituèrent une avancée majeure en matière d'approche globale des questions légales, techniques, organisationnelles, de construction des capacités et de coopération. C'est lors de la 5ème édition de l'IGF, en 2009 que nous avons présenté le document « A Global Protocol on Cybersecurity and Cybercrime » qui défend le besoin d'établir un traité international du cyberespace pour lutter contre les cyberattaques.

Diverses instances onusiennes, gouvernementales et intergouvernementales abordent depuis longtemps la problématique de la sécurité dans le cyberespace sous l'angle de la paix, de la stabilité, de la lutte contre la criminalité ou des mesures de confiance.

En 2004, un groupe d'experts gouvernementaux est mis en place lors de l'Assemblée générale des Nations Unies pour examiner les questions de sécurité et de stabilité dans le cyberespace et sur les impacts des développements des TIC sur la sécurité nationale. Un autre groupe est établi en 2019 pour promouvoir un comportement responsable des Etats dans le cyberespace dans le contexte de la sécurité internationale. Des experts gouvernementaux issus de 25 Etats membres travaillent en collaboration avec des organisations régionales (l'Union africaine, l'Union européenne, l'Organisation des États américains, l'Organisation pour la sécurité et la coopération en Europe et le Forum régional de l'association des nations de l'Asie du sud-est).

À Genève, la Suisse a lancé en 2014 l'initiative « Geneva Internet Platform » et en 2019, la Swiss Digital Initiative et la fondation Geneva Science and Diplomacy Anticipator. Toujours à Genève, se situe le Centre pour la cybersécurité du World Economic Forum (WEF), le CyberPeace Institute, fondé par Microsoft, MasteCard et Hewlett Foundation. En 2020 fut inauguré, sous le haut patronage du patron de Microsoft, le concept de Trust Valley en lien avec l'arc lémanique et les acteurs du numérique de la région.

En matière de cybersécurité, toutes ces initiatives ne peuvent faire oublier que le premier instrument à portée internationale de la lutte contre la cybercriminalité est la Convention sur la Cybercriminalité du Conseil de l'Europe de 2001 (CETS No.185, connue sous le nom de Convention de Budapest). L'Europe, y compris avec son approche de la protection des données personnelles (le règlement général sur la protection des données - RGPD) est à considérer comme un acteur important de la régulation du monde Cyber. Par ailleurs, d'autres approches régionales ont vu le jour à travers divers textes relatifs à la cybersécurité et plus de 125 pays ont signé ou ratifié des accords concernant la cybersécurité (Appel de Paris, Commonwealth Cyber Declaration, Déclaration du sommet des pays du BRICS, Déclaration du Sommet du G-20 de Buenos Aires, …).

L'Appel de Paris « Pour la confiance et la sécurité dans le cyberespace » de 2018 a le mérite d'être de portée universelle et non partisane. Il est soutenu par un grand nombre d'acteurs dont les signataires du

Cybersecurity Tech Accord, dont Microsoft qui promeut depuis 2017, l'idée d'une Convention de Genève du cyberespace.

Si la pluralité des débats contribue à augmenter la sensibilisation à ces questions et le nombre d'acteurs concernés, cela engendre une grande confusion des rôles et finalités de ces diverses initiatives. Cela rend incompréhensible l'écosystème « normatif » et difficile l'élaboration de mesures concrètes qui instancient des recommandations de haut niveau en des textes de lois contraignants dont l'applicabilité serait vérifiée.

Le brouhaha induit par ces initiatives et leur marketing par le secteur privé, leur manque d'harmonisation, la forte défense des intérêts du secteur privé, une société civile peut active ou inféodée au privé, font écran à un véritable débat multilatéral et à l'établissement de mesures applicables, dont le non-respect serait punissable.

La maitrise de l'outil mondial de production du numérique, qui se décline en puissance et pouvoir politique, économique et technologique, constitue l'enjeu du siècle. Par certains égards, du fait de la présence des instances internationales et des multinationales du numérique, le destin commun technologique de l'humanité se détermine aussi en Suisse. Espérons qu'elle soit à la hauteur des enjeux et des défis que posent à la planète, la course à l'armement technologique.

FSPI : L'intelligence artificielle aura sans aucun doute une double incidence sur la cyber sécurité dans les années à venir, sur le plan offensif comme défensif. D'une part elle amplifie les menaces cyber d'un point-de-vue quantitatif et qualitatif, augmentant l'envergure des menaces en offrant d'avantage de cibles à exploiter et en donnant un certain élan aux cyberattaques; d'autre part, à l'inverse, en aidant à s'en défendre, en permettant la découverte de nouvelles vulnérabilités, en détectant des activités cyber malveillantes et en mettant en œuvre des contre-mesures. Que devraient faire selon vous les gouvernements sur les plans national et international pour favoriser une gouvernance positive et inclusive de l'IA ?

Solange Ghernaouti: L'intelligence artificielle ne se limite pas aux aspects de cybersécurité ou de cyberdéfense. Force est de constater que le déficit de vision prospective et d'actions collectives allant dans le sens de création de mécanismes internationaux de régulation et de contrôle, favorise des développements sauvages de l'intelligence artificielle, y compris dans le domaine militaire et ouvre la porte à toutes sortes de dérives préjudiciables aux droits humains.

Le cas de la Chine, avec l'évolution des comportements et des pratiques de contrôle des citoyens et des organisations, qui met en œuvre et à grande échelle l'intelligence artificielle via un système dit de «crédit social » pour surveiller, punir et contraindre, est exemplaire. Quelle sera l'évolution dans d'autres pays ? Quelles sont les limites du techno-pouvoir? Peut-on contrôler la recherche et l'innovation ? Qui discute de ces questions et y apporte des réponses convaincantes du point de vue de la société civile ?

Qui est en mesure d'envisager qu'une gouvernance positive et inclusive de l'intelligence artificielle peut passer par une interdiction de certains usages de l'intelligence artificielle ?

Pour ma part, je milite pour que de nouveaux droits fondamentaux soient reconnus : le droit à la déconnexion, le droit de ne pas être sous surveillance informatisée, le droit de la personne à savoir si elle interagit avec une intelligence artificielle (qui simule l'humain), le droit à la transparence des prises de décisions effectuées par une intelligence artificielle, le droit de pouvoir recourir contre une décision prise par une intelligence artificielle.

L'utopie d'une intelligence artificielle parfaite, qui résoudrait tous les problèmes, relève plus du phantasme que de la réalité des faits. Tant que les évolutions technologiques servent une logique de rationalisation économique, de compétitivité et de performance économique pouvant aller jusqu'à la réification de l'humain, que la recherche de profit est au centre de l'informatisation de la société et de l'automatisation des processus et des prises de décisions, le respect des droits humains restera un horizon inatteignable.

L'adoption des technologies issues de l'informatique et des sciences cognitives nécessite un accompagnement politique, économique et juridique. Les ruptures technologiques sont des ruptures stratégiques auxquelles il faut répondre de manière stratégique c'est-à-dire politique … y compris en

matière de cybersécurité. Cela est possible à condition d'être en mesure d'accorder une place importante à la prospective réalisée de manière holistique, à une époque où la réflexion stratégique semble avoir des difficultés à se distancier de celles des acteurs hégémoniques du numérique et qui alimente sans la questionner la fuite en avant technologique. Telle qu'elle est réalisée et imposée, forte de ses pouvoirs incitatifs, prescriptifs et coercitifs, l'intelligence artificielle, contribue à aussi à détruire des métiers à haute compétence cognitive.

La vigilance est de rigueur pour que l'intelligence artificielle ne soit pas l'expression d'une hypocrisie pseudo-humaniste, ni le bras armé du techno-libéralisme, ni celui de systèmes autoritaires ou totalitaires.

FSPI : La crise sanitaire du Covid-19 a de nombreuses conséquences collatérales et notamment une vulnérabilité accrue des entreprises au risque cyber, suite au basculement de pans d'activité entiers en mode digital et au recours généralisé au télétravail. Au demeurant, il apparaît que beaucoup d'acteurs malveillants ont déjà profité de ce moment où l'urgence de la gestion de crise prime souvent sur le respect des mesures de sécurité et que les attaques cyber ont augmenté sensiblement depuis le printemps dernier. Est-ce que le Swiss Cybersecurity Advisory and Research Group que vous dirigez peut confirmer cette situation ? Quelles mesures de cyber sécurité complémentaires recommandent-elles aux institutions publiques et entreprises privées?

Solange Ghernaouti: Effectivement, le télétravail par l'ouverture de leur système d'information, fragilise les organisations. En augmentant le nombre de systèmes connectés, de flux d'informations échangés et le volume de données véhiculées, il y a accroissement du nombre de cibles et d'opportunités de cybermalveillance. D'être victime de cyberattaques n'est pas une fatalité.

Comme toutes démarches de sécurité, la cybersécurité reposent sur la responsabilité des acteurs, une volonté politique, des mesures stratégiques et opérationnelles de prévention, protection, défense et de réaction cohérentes. Les organisations qui ont développé des postures de gestion des risques sont mieux préparées que les autres à anticiper et à se mobiliser pour faire barrière à la propagation de virus, qu'ils soient d'origine biologique ou informatique. Mettre en place des mesures proactives et préventives avant que les problèmes surviennent est impératif, comme l'est d'ailleurs les mesures de réaction, de gestion de crises et de la continuité des activités. Cela demande de comprendre les cyberrisques, une stratégie de sécurité, une organisation, des ressources et un certain savoir-faire. Ainsi il existe des solutions pour maitriser les risques et minimiser leurs effets délétères, pour que l'organisation soit moins vulnérable et ne devienne pas une cible privilégiée de la cybercriminalité.

Les virus biologiques et informatiques soulèvent le défi commun de savoir d'une part, comment rester sain dans un monde de malades et d'autre part, comment assurer sa sécurité et sa sûreté alors que la qualité de celles-ci dépend de celles des autres ?

Aujourd'hui, l'urgence n'est pas uniquement liée aux cryptovirus (rançongiciels), qui depuis Wanacry en 2017, sont devenus des préoccupations des responsables de la sécurité informatique, de manière pragmatique, l'urgence est humaine. Que devient la sécurité informatique en cas de pandémie, qui est disponible pour l'assurer ? Comment protéger le système d'information quand l'humain est défaillant ? Même si des mécanismes d'intelligence artificielle peuvent être des éléments de solutions, ils ne pourront en aucun cas résoudre tous les problèmes liés à la disponibilité, l'intégrité, des infrastructures numériques et aux exigences d'authenticité et de confidentialité. Sommes-nous prêts à faire face à un tsunami combiné de virus informatique et biologique ? La crise « Covid-19 » est un révélateur de notre capacité à gérer les risques complexes, à déterminer les risques acceptables et à savoir qui les assume.

La cybersécurité n'est pas une fin en soi mais sans cybersécurité il est désormais impossible de vivre !

FSPI : Le déploiement de la 5G va marquer une véritable révolution technologique, puisqu'elle permettra de connecter plusieurs centaines de milliards d'objet dans les domaines les plus divers comme la mobilité, l'approvisionnement énergétique, la production industrielle, la santé, la sécurité, etc. A ce titre, la 5G est devenue un enjeu stratégique et géopolitique majeur tout en bouleversant les rapports de force économiques et politiques. Est-ce que selon vous l'utilisation des infrastructures disponibles actuellement sur le marché (Huawei, Ericsson, Nokia, Samsung, ZTE) aurait un impact sur la cybersécurité, en élargissant possiblement l'éventail des risques cyber et en accentuant leur ampleur ?

Solange Ghernaouti: Un peu de concurrence sur le marché des équipements et des infrastructures de télécommunication ne saurait nuire. En théorie tout au moins avec une certaine diversité des équipementiers, la concurrence devrait éviter les risques liés aux situations de monopole et la dépendance envers un fournisseur unique, qu'il soit d'origine nord-américaine ou chinoise.

Pour faciliter leur gestion opérationnelle et leur mise à jour régulière, les équipements constitutifs d'un réseau de transmission restent connectés à leur fournisseur. Ce lien légitime est susceptible d'être doublé par des dispositifs qui le sont moins, et notamment des systèmes d'écoute parfois intégrés par les constructeurs dès la conception de leurs appareils. Quand de telles portes dérobées (backdoors) existent, l'accès aux données qui les traversent et la fuite de données à des fins d'espionnage, de surveillance, ou encore d'intelligence économique, est toujours possible.

Dès lors, pour une entité (ou un pays) qui possède une infrastructure de télécommunication reposant sur des équipements étrangers dont la fabrication n'est pas maitrisée, il est nécessaire d'être au moins en capacité de maitriser tous les flux de gestion des systèmes et d'être en mesure de décider quelles données doivent être autorisées à transiter au travers des équipements (vers et en provenance de quels équipements). Cela est du ressort des entités en charge de l'administration des systèmes et de la gestion de réseaux.

Puisqu'il n'y a pas de maitrise absolue de la neutralité des équipements constitutifs d'un réseau de transmission, il est tout aussi impératif de maitriser le chiffrement des données qui y transitent. Pour le propriétaire de l'infrastructure de télécommunication, il est fondamental de maitriser le chiffrement «de bout en bout » par la mise en œuvre de mécanismes de cryptographie offrant des fonctions de confidentialité, de contrôle d'intégrité et d'authentification. Pour renforcer la sécurité des données, il est possible de chiffrer un échange de données à plusieurs niveaux de l'architecture de communication, via plusieurs et différents protocoles cryptographiques. Ce type d'approche permet de reprendre le contrôle des échanges de données réalisés au travers d'une infrastructure dont le niveau de confiance est faible et de reprendre le contrôle au niveau logique puisqu'il n'est pas garanti au niveau physique, c'est-à-dire matériel, par les équipements du fournisseur.

L'enjeu majeur de la bataille US / Chine (Huawey) est celui de la maitrise de l'infrastructure et de la surveillance de l'Internet des objets (IoT & Internet of every things) – de la surveillance des flux, des personnes, des organisations privées et publiques, de l'économie toute entière.

Dans un monde hyperconnecté et dans un contexte de dépendance numérique, les enjeux des équipementiers des infrastructures de la téléphonie mobile de cinquième génération (5G) dépassent largement les questions technologiques. Ils sont d'ordre politique, géostratégique et au final souvent économique. Les diverses autorisations - interdictions liés à des composants électroniques, logiciels et services (Huawei, TikTok,...) relèvent d'approches géopolitiques et de stratégie de guerre commerciale.

Le rouleau compresseur de la 5G, du big data, de l'intelligence artificielle et des objets connectés ignore les préoccupations et résistances d'un pan important de la société civile qui s'interroge sur leurs finalités, capacités de surveillance et sur leurs impacts sur l'environnement et le vivant.

On assiste parfois à une certaine inféodation du monde académique et de certains scientifiques au techno-pouvoir et à la doxa techno-libérale. Toutefois des voix s'élèvent, le refus de la 5G ou de certaines pratiques numériques, par la population est un révélateur qui devrait renforcer et soutenir l'action politique qui ne devrait pas considérer le solutionnisme technologique comme une finalité et succomber aux discours des évangélistes du « tout numérique ».