Cyberespionnage et sécurité des données : l'Occident dans la ligne de mire ?

Rapport de synthèse | 15e FFS Security Talk du 22 novembre 2023, Hôtel Schweizerhof, Berne

Avec le triomphe d'Internet et la numérisation croissante qui en découle, un cyberespace extrêmement complexe a vu le jour au cours des deux dernières décennies, grâce auquel le monde entier a été mis en réseau. Cet espace numérique ouvre d'une part une multitude de nouvelles possibilités, mais il est d'autre part extrêmement dangereux. Les attaques de pirates informatiques contre les institutions étatiques et les entreprises occidentales ont massivement augmenté ces dernières années. En Suisse aussi, cette tendance est clairement perceptible, comme le montrent les nombreux exemples de l'année dernière. Les acteurs du secteur privé ne sont pas non plus épargnés et sont de plus en plus souvent la cible de telles attaques.

Quels sont les secteurs et les institutions ciblés par de telles attaques ? Comment les autorités, les institutions et les entreprises peuvent-elles et doivent-elles protéger leurs données critiques contre les cyberattaques ? Comment la politique doit-elle faire face à la menace du cyberespionnage et d'autres cybermenaces ? Quelles sont les mesures urgentes et nécessaires ?

Ces questions et d'autres questions importantes ont été discutées lors du 15e FSS Security Talk à Berne par des experts de renom tels que **le major général Jürgen Setzer** (inspecteur adjoint CIR et CISO, Bundeswehr), **Dr. Myriam Dunn Cavelty** (maître de conférences en études de sécurité, Center for Security Studies (CCS), EPF Zurich), **Nicolas Mayencourt** (Founder & Global CEO, Dreamlab Technologies), **Franz Grüter** (président du conseil d'administration du groupe green.ch ; conseiller national UDC, LU) ainsi que **Johann Alessandroni** (directeur du département Information Security Governance, Excellium Services by Thales Group).

Hans-Jürg Käser, président du FORUM SÉCURITÉ SUISSE, a accueilli les quelque 120 participants au 15e FSS Security Talk par quelques mots d'introduction. Afin de tenir compte du programme serré, c'est le major général Setzer qui a immédiatement commencé à présenter le premier exposé.

Exposé du major général Jürgen Setzer

On demande souvent au major général Setzer comment on peut encore dormir la nuit dans sa fonction d'inspecteur adjoint du cyberespace et de l'espace d'information et de Chief Information Security Officer de la Bundeswehr. Sa réponse est simple : "en étant bien éveillé le jour". La protection du cyberespace et de l'espace d'information est une priorité pour la Bundeswehr. C'est pourquoi le **cyberespace et l'espace d'information (CIR)** de la Bundeswehr ont été érigés en avril 2017 en tant que **domaine d'organisation militaire autonome** et ont ainsi été placés au même niveau que les **autres dimensions que sont la terre, l'air, l'eau et l'espace**.

Le cyberespace et l'espace d'information en tant que domaine d'intervention militaire

L'importance du cyberespace et de l'espace d'information en tant que domaine d'intervention militaire est par exemple très clairement démontrée par l'actuelle guerre d'agression russe contre l'Ukraine. Bien que la couverture médiatique se concentre en grande partie sur les capacités cinétiques conventionnelles des forces armées, on peut constater chaque jour que les **capacités dans le cyberespace et l'espace d'information sont un élément essentiel de la conduite de la guerre**. Les médias, en particulier, sont le théâtre et l'acteur de la guerre de l'information menée par la Russie, dont l'objectif principal est de briser la volonté de défense de l'Ukraine et de ses alliés. L'Allemagne, bien qu'elle ne soit pas partie à la guerre, est exposée en permanence à une influence hybride, que ce soit par des campagnes d'information ou des cyberattaques, dans le but d'influencer la formation de la volonté politique. Les acteurs comprennent aussi bien les cyber-guerriers réguliers des services secrets russes que les organisations et groupements criminels. Il est clair que **les acteurs étatiques utilisent volontiers des acteurs non étatiques pour lancer des attaques et se décharger de leur responsabilité**, ce qui rend difficile l'attribution claire des incidents, tant pour l'Allemagne que pour d'autres pays et alliés. L'attaque de la Russie contre l'Ukraine et les cyberattaques qui l'accompagnent représentent également un danger indirect considérable pour l'Allemagne. La cyberattaque russe contre le service satellite KA-SAT de Viasat, utilisé par l'armée ukrainienne, en est un exemple.

Une importance tout aussi grande du cyberespace et de l'espace d'information dans les conflits militaires peut être observée actuellement dans le contexte de la guerre entre Israël et le Hamas. L'attaque des terroristes du Hamas s'accompagne d'opérations parallèles dans le cyberespace. Des médias d'information importants comme l'agence de presse Jerusalem Post ou un système israélien d'information et d'alerte sur les dangers, qui représente un instrument essentiel et salvateur pour la population israélienne face aux attaques permanentes de roquettes, en ont déjà été victimes.

L'information, ressource clé des sociétés et des forces armées modernes

De telles attaques alimentent naturellement la peur et la confusion au sein de la population. D'autre part, l'objectif de ces attaques est souvent de porter atteinte aux informations de l'adversaire, car celles-ci représentent une ressource clé des sociétés modernes et sont une condition préalable à la disponibilité opérationnelle des forces armées. La sécurité de l'information, c'est-à-dire la protection efficace de la transmission, du traitement et du stockage des informations, revêt donc une importance particulière. "**La supériorité de l'information est en fin de compte une condition préalable à la supériorité décisionnelle, une condition préalable à la supériorité d'efficacité et, à la fin de la journée, une condition préalable à la capacité de victoire des forces armées dans un conflit"**, a souligné le major général en évoquant le rôle clé de l'information.

La Bundeswehr est également la cible de tentatives d'attaques quotidiennes dans le cyberespace. En tant que Chief Information Security Officer, il est heureux de dire qu'aucune de ces attaques n'a encore été couronnée de succès. Mais il faut toujours être prudent avec ces déclarations, car on ne peut jamais exclure à 100 % que quelqu'un se soit déjà introduit dans son propre système et que les mécanismes de protection ne l'aient pas encore remarqué.

Ces attaques montrent qu'il est important d'être à tout moment éveillé, innovant et agile et de vérifier et d'améliorer constamment sa propre architecture de sécurité. Pour ce faire, quatre champs d'action ont été définis : le facteur humain, les concepts et la technique, le développement de l'environnement d'innovation ainsi que la coopération nationale et internationale.

Le facteur humain

Le premier champ d'action, le facteur humain, représente un facteur tout à fait décisif dans la sécurité informatique. D'une part, du point de vue de l'utilisateur ou de l'utilisatrice : **Plus de 80 % des attaques réussies contre la sécurité informatique peuvent être attribuées à la participation involontaire de l'utilisateur ou de l'utilisatrice.** Les méthodes des auteurs sont multiples. Le terme d'ingénierie sociale englobe de nombreuses stratégies visant à influencer et à manipuler les personnes et à provoquer certains comportements, comme par exemple l'octroi d'accès à des données et à des systèmes ainsi que le partage d'informations. Les progrès de l'IA ont également permis d'améliorer les possibilités de tromper les victimes avec succès. Chacun des participants a certainement déjà reçu des e-mails d'hameçonnage, que ce soit sur des adresses e-mail privées, professionnelles ou de service, dont l'apparence est parfois trompeuse. Il est toutefois positif de constater que les attaques dans le contexte de la guerre d'agression russe contre l'Ukraine ont en principe accru la sensibilisation des utilisateurs. Mais cela n'est pas encore suffisant. C'est pourquoi l'armée allemande se soumet à des défis 7 jours sur 7, 24 heures sur 24, afin d'identifier les faiblesses éventuelles avant que d'autres ne les exploitent. Ce faisant, on s'attaque soi-même avec les forces offensives, on sensibilise les collaborateurs et collaboratrices et on renforce la conscience que l'on est quotidiennement sous le feu.

Par ailleurs, les **besoins en personnel spécialisé dans la cybersécurité ont considérablement augmenté et la pénurie de personnel qualifié s'est aggravée, ce qui** a nécessité d'explorer de nouvelles voies pour trouver suffisamment de personnel qualifié. L'accent est donc mis sur la formation. C'est pourquoi la Bundeswehr forme également de manière autonome, parfois dans sa propre école d'informatique ou dans les universités de Hambourg et de Munich.

Concepts, technique, innovation et coopération

Le deuxième champ d'action concerne les concepts et les techniques utilisés. La Bundeswehr dispose de concepts standard de sécurité de l'information. Ceux-ci constituent la base de toutes les formations avant qu'elles ne partent en mission, qu'il s'agisse de missions de gestion normale des crises, comme c'est encore le cas actuellement au Mali ou au Kosovo, ou d'engagements similaires dans le contexte de la dissuasion ou sur le flanc est de l'OTAN, par exemple en Lituanie.

Parallèlement, on s'occupe aussi de concepts et de techniques nouveaux et futurs, respectivement du développement de l'environnement d'innovation, le troisième champ d'action. **La cybersécurité n'est pas un état statique.** Elle nécessite une **adaptation** et **un développement** continus afin de suivre les **cycles d'innovation courts de** la numérisation dans le domaine de la cybersécurité. Dans ce contexte, trois aspects sont particulièrement importants du point de vue de l'environnement d'innovation : L'efficacité, l'orientation vers les besoins et l'agilité.

Pour augmenter l'efficacité, il est tout aussi important d'établir un dialogue sur les technologies de l'information et de l'innovation avec les partenaires de l'économie, comme Bitkom, l'association professionnelle du secteur allemand de l'information et des télécommunications, qu'avec les autorités de sécurité fédérales et régionales, ou encore avec la science et les instituts de recherche. Parallèlement, un dialogue au sein des forces armées doit bien entendu être mis en place afin d'accroître l'orientation vers les besoins. Au sein de la Bundeswehr, le dialogue sur l'innovation mise sur un réseau d'action mis en place entre les responsables de la plateforme de numérisation, le service des achats et les fournisseurs de systèmes informatiques du secteur privé. Ce lien est l'élément clé d'une **transformation numérique rapide** et **durable** et ne fonctionne que si **les utilisateurs**, **les développeurs** et **les fournisseurs sont dans le même bateau dès le début** et collaborent.

En outre, la Bundeswehr dispose également d'acteurs de l'innovation qui dirigent les applications. Il s'agit d'une part du Cyber Innovation Hub, qui est un point central pour tester des solutions commercialisables issues du monde des start-ups. En outre, il y a la "forge BWI" qui, en tant que Coding Force, contribue de manière décisive à la numérisation et à l'automatisation de la Bundeswehr. En outre, une agence cybernétique a été créée pour promouvoir les projets de recherche dans le contexte de la cybersécurité. "**Dans le domaine de la cybersécurité, il n'y a pas de frontière entre la sécurité intérieure et extérieure, et c'est pourquoi les forces de sécurité intérieure et extérieure doivent travailler ensemble pour faire progresser leurs capacités"**, a souligné le major général Setzer une nouvelle fois la nécessité d'une coopération interministérielle et inter-niveaux. C'est dans ce but et pour offrir une marge de manœuvre suffisante au-delà des frontières intérieures et extérieures à l'approche de l'amélioration continue et de l'innovation que cette cyber-agence a été créée. De plus, des coopérations ont été mises en place avec la société Fraunhofer et les deux universités de la Bundeswehr.

"Ce n'est pas un joueur sur le terrain qui détermine l'action, mais de nombreux matchs ensemble".

Le quatrième domaine d'action concerne la coopération et les exercices nationaux et internationaux. La coopération interministérielle au niveau national entre la recherche, les autorités de sécurité et les entreprises est considérée comme d'une importance capitale. La stratégie allemande en matière de cybersécurité donne d'ailleurs des directives claires à ce sujet. Le point de cristallisation en Allemagne

est le centre national de cyberdéfense. Il a été mis en place dès 2011 sous la direction de l'Office fédéral de la sécurité des technologies de l'information (BSI). Il s'agissait du premier forum de coopération étatique dans le contexte de la cybersécurité. Les années suivantes, l'accent a été mis sur le développement successif de ce forum et sur l'augmentation continue du nombre de participants. C'est important, car la cyberdéfense est un jeu d'équipe : "Ce n'est pas un joueur sur le terrain qui détermine l'action, mais plusieurs joueurs ensemble". Mais une chose est claire : sans un capitaine ou un entraîneur convaincant, cela ne fonctionne pas. C'est pourquoi on a décidé de définir des coordinateurs. La Bundeswehr joue toujours le rôle de coordinateur adjoint afin de pouvoir garantir le passage de la paix à la guerre au sein de l'organe de coordination.

Cette instance du centre national de cyberdéfense, conçue comme une plateforme de coordination et de coopération de l'information, apporte ainsi une contribution essentielle à la cybersécurité, dès aujourd'hui et maintenant. **L'État a la responsabilité d'être préparé à un super-GAU numérique, et ce avant que celui-ci ne se produise effectivement.** Pour cela, il est indispensable que nos autorités de sécurité, l'armée fédérale, les communes, les autorités et les entreprises KRITIS s'exercent ensemble, comme cela a été le cas en septembre dernier lors de l'exercice de gestion de crise interministérielle et interpays LÜKEX. Lors des cyberattaques simulées à l'échelle fédérale, l'objectif principal était de maintenir les fonctions de l'État et du gouvernement. Car si celles-ci ne sont plus garanties, le chaos est encouragé. Seuls des exercices communs de ce type peuvent donner des impulsions décisives pour améliorer la résilience dans des scénarios qui ne se sont pas encore produits, mais qui pourraient l'être.

Coopération internationale

L'échange au niveau multilatéral est également important. Dans ce contexte, on se réjouit particulièrement des liens étroits avec les partenaires suisses, que ce soit par exemple à travers les rencontres annuelles des cyber commandants de l'espace DACH ou les séminaires communs germano-suisses sur les systèmes d'information de commandement et les stratégies de données. En outre, le cyberespace et l'espace d'information se réjouissent déjà de la visite du cyber commandant suisse et du chef d'état-major de la formation opérationnelle à Bonn l'année prochaine.

Outre cet échange, l'exercice continu est une des conditions préalables à une cyberdéfense efficace. **Dans le cadre de "COMMON ROOF", les relations avec les amis suisses sont bonnes et solides.** Il s'agit d'un exercice annuel dont le but est d'exercer le développement des capacités des nations DACH en matière d'opérabilité. Dans une perspective d'avenir, le format DACH permet également une collaboration fructueuse. Dans le cadre de l'exercice multilatéral de cyberdéfense de l'année prochaine, les équipes de cyberdéfense et d'intervention d'urgence s'exerceront ensemble dans le format faîtier et, comme prévu initialement, également avec les amis israéliens.

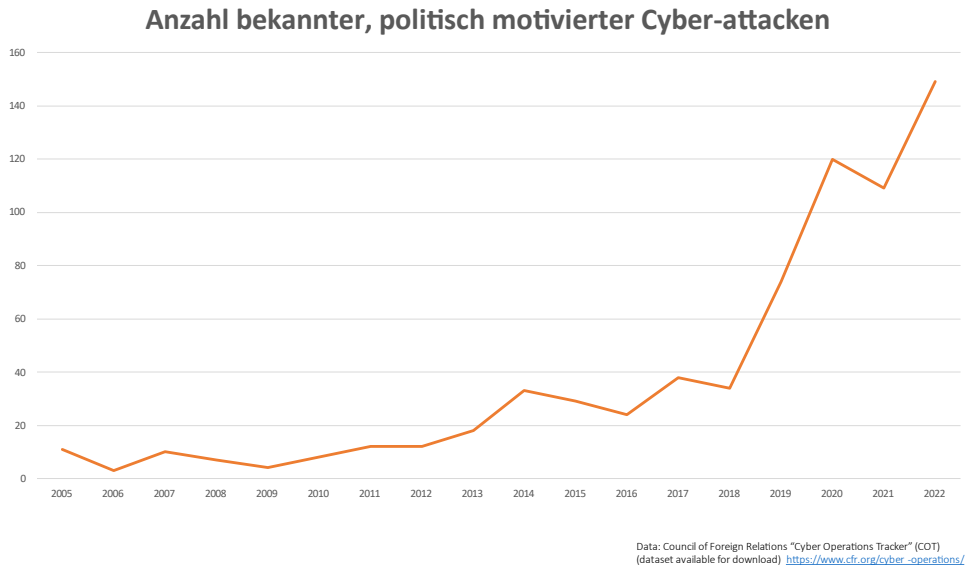
"L'information est la ressource clé de notre société moderne et de nos forces armées. Sa protection, c'est-à-dire la cybersécurité de l'information, est pour nous tous, Allemands et Suisses, à la fois un devoir et un des plus grands défis. Considérons ce défi comme une chance. Une chance de développer nos capacités ensemble, de protéger nos pays et de façonner notre avenir ensemble".

Exposé Dr. Myriam Dunn Cavelty

La deuxième intervenante, Myriam Dunn Cavelty, a mis l'accent sur le cyberespionnage, qu'elle a abordé dans une perspective scientifique. Son objectif était de montrer pourquoi nous parlons surtout d'espionnage lorsqu'il s'agit d'activités étatiques dans le cyberespace et moins d'autres formes courantes de cyberattaques, pour lesquelles il ne serait pas nécessaire de disposer de capacités aussi importantes.

Augmentation des cyberattaques à caractère politique depuis 2017/2018 - le cyberespionnage en tête de liste

Si l'on observe les données, on constate une augmentation massive du nombre de cyberattaques connues publiquement et motivées par des raisons politiques vers 2017/2018. Cette hausse s'explique d'une part par la création et le développement de capacités dans le cyberespace après 2010. Il existe aujourd'hui davantage d'acteurs capables de lancer de telles attaques ciblées. D'autre part, l'augmentation serait également liée à un renforcement des capacités du côté de la défense et des capacités de détection de telles attaques. Comme l'a déjà dit le major général Setzer, de nombreux investissements ont été et sont encore réalisés dans le domaine de la cybersécurité.



Si l'on examine le type d'attaques, on constate que l'espionnage occupe une place prépondérante. Parmi les attaques connues à motivation politique, 70 à 80 % relèvent de l'espionnage. Et il ne s'agit là que des données connues. Si l'on tient compte du fait que l'espionnage est pratiqué le plus secrètement possible, on peut supposer que le nombre effectif est encore plus élevé.

Capacités / Configurations / Contexte - Bonnes raisons pour le cyberespionnage

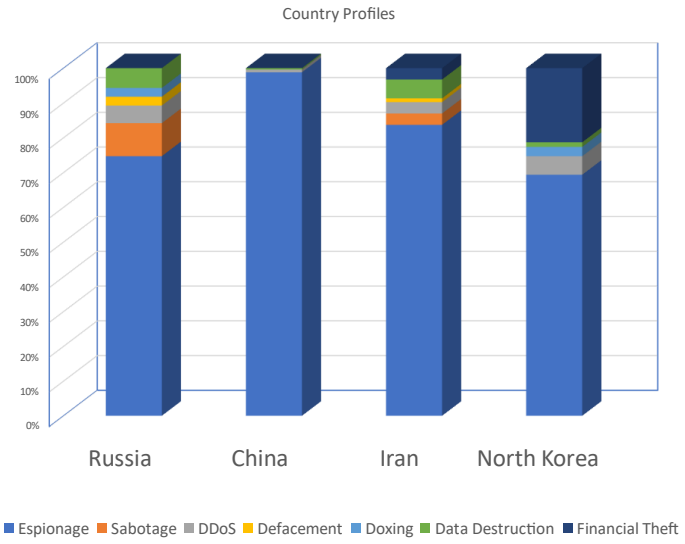
Trois raisons expliquent pourquoi l'espionnage en tant que moyen étatique est si répandu dans le cyberespace : premièrement, les capacités déjà mentionnées ou, dans ce contexte, les **"Advanced Persistent Threats" (APT)**. Ensuite, les **configurations**, qui englobent les caractéristiques techniques des systèmes et la possibilité d'agir sur eux, mais aussi le facteur humain et ses compétences dans le domaine cybernétique. Enfin, le contexte géopolitique et le concept de **"compétition stratégique"** expliquent pourquoi le cyberespionnage a beaucoup de sens pour les Etats.

Capacités

Si l'on aborde le sujet des capacités, il faut d'abord comprendre qu'il existe certaines activités dans le cyberespace qui sont très difficiles à réaliser. "L'idée du hacker assis dans sa cave et appuyant sur n'importe quel bouton pour produire quelque chose de grand doit être effacée de l'esprit des gens dans ces cas-là". Selon lui, cette prise de conscience est nécessaire pour savoir à qui l'on a réellement affaire et quelles mesures peuvent être prises.

Länderprofile

- Seit 2005: 34 Länder führen offensive Cyber-operationen durch
- China, Russland, Iran, Nord Korea verantwortlich für 77% aller Operationen
- Achtung, Visibilität!



Si l'on considère le profil des pays qui ont mené des cyber-opérations de haut niveau depuis 2005, on constate que 34 pays sont concernés. **Environ 77 % d'entre eux** sont des rivaux politiques des États-Unis, à savoir **la Russie, l'Iran, la Chine et la Corée du Nord.** Il est toutefois important de thématiser ici aussi la visibilité. Les données disponibles sont mises à disposition par des entreprises, appelées Threat Intelligence Companies, qui ont pour la plupart leur siège aux Etats-Unis. Celles-ci ont développé pendant des années les capacités et les aptitudes nécessaires à l'enregistrement de telles attaques, alors que d'autres pays n'ont pas ces capacités, ce qui a pour conséquence que la base de données scientifiques est incomplète.

Comme mentionné plus haut, l'espionnage représenterait une grande partie des cyberopérations étatiques du segment supérieur - notamment chez les principaux rivaux des Etats-Unis. Les unités qui mènent ces activités d'espionnage sont également appelées Advanced Persistent Threats (APT). Elles se caractérisent par des capacités hautement développées, qui durent depuis des années et qui émanent de personnes. Outre un **savoir-faire technique approfondi,** ces **cyberopérations seraient** également **très coûteuses**. De ce fait, **les APT** sont **généralement dirigées par l'Etat** et s'**intéressent** aux **données sensibles et précieuses afin de rentabiliser** les efforts déployés dans le cadre de telles opérations.

Configurations

Si l'on s'intéresse aux configurations qui favorisent les cyberopérations, on constate que les attaquants ont besoin de temps pour trouver les vulnérabilités et pour mettre au point les programmes qui permettront d'exploiter les vulnérabilités trouvées. La plupart du temps, cela prend des mois, voire des années. En outre, les cyberopérations seraient rentables si l'on pouvait et voulait agir en cachette, ce qui correspond aux exigences de l'espionnage. Comme l'accès à un réseau ne peut pas être obtenu par la force, **les vulnérabilités existantes** et la **capacité à ne pas être découvert sont importantes**. Si un attaquant se fait repérer dans le système, il risque de perdre l'ensemble des outils coûteux qu'il a développés à grands frais. Les cyberopérations sont également rentables si elles ne visent pas une intensité ou une destruction élevée. Il n'est en effet pas facile de programmer avec précision un effet destructeur et d'en prévoir l'ampleur. Cela signifie également que**, d'un point de vue militaire,** cela n'a **pas beaucoup de sens de vouloir détruire des réseaux avec des cyberopérations** ; au lieu de cela, **la voie physique a plus de sens**. En d'autres termes, plus l'effet recherché est intense et plus l'opération

est complexe, plus l'attaquant a de chances de se faire repérer et de risquer ses investissements. Enfin, les cyberopérations seraient rentables si leur effet ne devait pas être entièrement contrôlé. **Les cyberopérations** se déroulent dans des **systèmes adverses qui ne sont** souvent **pas entièrement connus**, et c'est pourquoi les **effets d'une opération** ne peuvent généralement pas **être entièrement testés ou prédits**. Il en résulte souvent les dommages collatéraux observés dans de nombreuses cyberattaques.

Si l'on réunit maintenant ces 4 points et que l'on regarde quel type de cyberopérations vaut la peine d'être mené sur des réseaux à la sécurité renforcée, on en revient à l'espionnage.

Contexte et concurrence stratégique

Enfin, le contexte géopolitique expliquerait également l'utilisation du cyberespionnage comme moyen d'action étatique. Elle propose la **Strategic Competition** comme cadre permettant de comprendre pourquoi certaines activités peuvent être observées de manière accrue dans le cyberespace. La Strategic Competition est un concept originaire des Etats-Unis. Dans ce concept, on voit un **brouillage** actif **de la guerre et de la paix**, et les cyberopérations s'y prêtent également. Toutes les cyberopérations, par exemple en Ukraine, sont délibérément maintenues sous le seuil de la guerre, sous une forme hybride entre guerre et paix. La compétition stratégique vise à exploiter tous les domaines de puissance, et c'est pourquoi elle se prête également au jeu des grandes puissances. Elle mobilise de très grandes ressources, et si l'on en revient au cyberespionnage, au vol systématique de la propriété intellectuelle, il s'agit là encore d'un moyen judicieux pour les États d'accumuler une ressource de puissance. Il reste certes très difficile de mesurer les effets et les dommages de l'espionnage, même d'un point de vue scientifique. Mais il est désormais clair qu'une **stratégie cumulative**, c'est-à-dire des **attaques répétées, de petite taille et à bas seuil**, sont **plus rentables** qu'une **grande attaque destructrice**. On constate donc que tous ces facteurs favorisent l'utilisation de l'espionnage comme moyen étatique dans le cyberespace.

En conclusion, Mme Dunn Cavelty a toutefois souligné que, même si elle a surtout parlé de cyberespionnage, les capacités de cyberespionnage sont étroitement liées aux capacités de cyberopérations d'un autre type. Il faut donc être conscient qu'avec le **développement des capacités dans le cyberespace observé ces** dernières années, le **risque d'opérations** ayant le potentiel de perturber l'**ordre social de manière significative augmente** également**.**

Exposé Nicolas Mayencourt

Dans son exposé, Nicolas Mayencourt s'est concentré sur les vulnérabilités, c'est-à-dire les surfaces d'attaque et les faiblesses dans le cyberespace, dans le but de les identifier et d'agir en conséquence. Bien que la Suisse soit une petite nation, sa force d'innovation est impressionnante.

Du monde naturel au monde 2.0

Si nous nous penchons sur les vulnérabilités dans le cyberespace, il serait judicieux de jeter d'abord un coup d'œil sur l'endroit d'où nous venons : le beau monde ancien et naturel que les hommes ont fait leur pendant des dizaines de milliers d'années avec leur ADN unique, leur intuition unique et leurs réflexes uniques.

Cela est d'autant plus surprenant, selon lui, que si l'on compare l'homme aux animaux ou à ses ancêtres directs, il leur est inférieur sur de nombreux points. Il peut par exemple courir moins vite et grimper moins bien. Si l'homme s'est malgré tout imposé comme l'espèce dominante, c'est grâce à son intuition et à ses réflexes exceptionnels, mais aussi grâce à deux autres avantages décisifs, notamment en matière d'information : D'une part, l'homme a réussi à **formaliser le savoir**, à le transmettre de génération en génération et à **se constituer** ainsi, au cours de centaines de milliers d'années d'évolution humaine, un **trésor de connaissances et d'expériences**. En outre, il dispose de la capacité décisive de s'**organiser** en **groupes ad hoc**. On connaît certes aussi le comportement grégaire dans le monde animal, par exemple chez les oiseaux et les poissons. Mais la différence est que "les hommes peuvent s'organiser de manière ad hoc, en fonction d'un but, d'un objectif et d'un projet, afin de créer ensemble

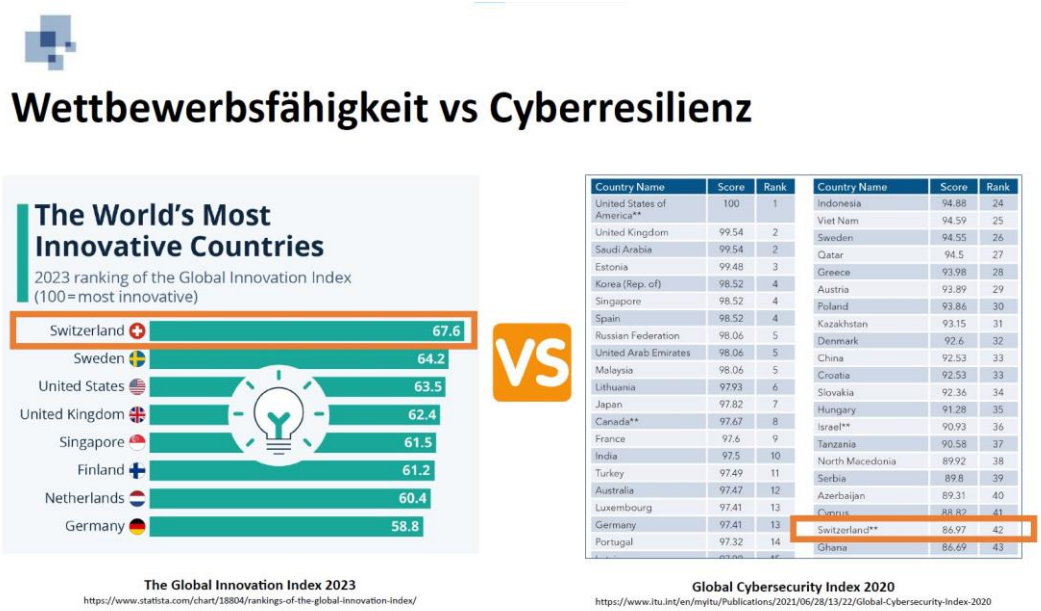
un résultat avantageux, que l'on se connaisse ou non à l'avance". Ces capacités se seraient accumulées au cours de l'évolution et auraient conduit à la première révolution industrielle qui, à bien des égards, aurait constitué l'origine et le fondement de la civilisation moderne, le nouveau monde.

Le cyberespace - abstrait, omniprésent, dangereux

L'homme, avec son humanité unique, a donc réussi à s'imposer comme une espèce gagnante dans les quatre dimensions que sont la terre, l'eau, l'air et l'espace. Mais le monde 2.0, ou plutôt le monde qu'il a créé, va encore plus loin : ainsi, lors de la **troisième révolution industrielle,** l'homme a créé un **nouvel espace unique, fabriqué par l'homme** : **le cyberespace**. L'invention de l'ordinateur et de l'espace numérique ainsi que la mise en réseau via la technologie Internet et d'autres technologies de réseau lui ont permis de donner libre cours à ses innovations sans limites physiques et d'entreprendre des choses qui ne seraient pas possibles dans le monde réel. Ces développements ont été marqués par une vitesse incroyable, qui se poursuit encore aujourd'hui. En l'espace de 50 à 70 ans, le cyberespace a été construit et aujourd'hui, il pénètre et contrôle presque entièrement les dimensions physiques. En même temps, ce cyberespace n'est pas perceptible pour l'homme, il n'est pas accessible aux sens. Il est omniprésent, invisible, et pourtant il contrôle tout. Cette construction est unique, merveilleuse, presque paradoxale, mais aussi très dangereuse, car les dangers et leurs effets immédiats ne sont pas directement perceptibles. L'homme n'en a pas la perception sensorielle - il ne ressent souvent les effets que lorsqu'il est déjà bien trop tard. Il faut absolument garder ce contexte à l'esprit. L'homme est victime de ses propres innovations. Il a développé un espace extrêmement puissant, mais dans lequel ses attributs humains, son intuition, sa sensualité n'ont plus de prise.

Un danger pour l'innovation en Suisse

Cela l'a amené à parler de la Suisse aujourd'hui et ici. Il a fait remarquer que, selon différentes statistiques, la **Suisse est la nation la plus innovante au monde**. La raison de cette force d'innovation peut être résumée simplement : La Suisse peut se le permettre et **investit systématiquement dans la recherche et la formation** depuis de nombreuses années. Résultat : la Suisse est aujourd'hui très innovante ; elle dispose d'un solide paysage de recherche et de développement ; elle est connue pour sa précision et sa qualité ainsi que pour sa neutralité et son indépendance. Ces qualités et vertus doivent toutefois être soigneusement entretenues à l'avenir.



A côté des statistiques et des indices souvent très réjouissants concernant la Suisse, il y aurait toutefois des chiffres clés qui devraient beaucoup moins réjouir les Suisses. L'**indice** de l'Union **internationale des télécommunications (UIT)**, basé sur l'ONU, comprend un cyberclassement concernant la cyberreadiness des nations. La **Suisse** y **occupe une place** plutôt médiocre (**42e)** et tout le monde doit être conscient que cela aura tôt ou tard un impact sur la capacité d'innovation de la Suisse. Dans le monde d'aujourd'hui, les résultats de la recherche sont en fin de compte des données qui sont conservées sur des serveurs. Si ces serveurs ne peuvent pas être protégés, les résultats des investissements dans la recherche et le développement sont transférés vers d'autres nations. Comme l'a dit Myriam Dunn Cavelty, 80% des attaques sont de l'espionnage. C'est pourquoi il est important de se préoccuper davantage de la cybersécurité, de travailler de manière plus ordonnée et de s'assurer que la Suisse se place dans le top 10 dans ce domaine également, afin de protéger en fin de compte son site d'innovation.

Cyber - un cluster mondial de risques

Si l'on s'intéresse à la menace cybernétique, on s'aperçoit qu'il s'agit d'un problème mondial. Selon le World Economic Forum et de nombreuses autres institutions, il existe deux grands groupes de risques auxquels notre monde est confronté : Le premier est le changement climatique et le deuxième est le cyber. Il y a plusieurs raisons à cela. Les dangers auxquels sont confrontés les acteurs étatiques et non étatiques dans le cyberespace ont déjà été bien mis en lumière par les orateurs précédents. En outre, les conséquences sont surtout de nature pécuniaire. En **2021,** les **cyberdommages** déclarés aux assureurs s'élèveront **à 5000 milliards de francs**. Cela correspond déjà au **PIB** de la **troisième économie mondiale** et à près de **50 fois tous les dommages causés par des phénomènes naturels**. Ce sont des dommages et des sommes que l'on ne peut plus simplement ignorer, mais qui doivent entraîner des actions décisives.

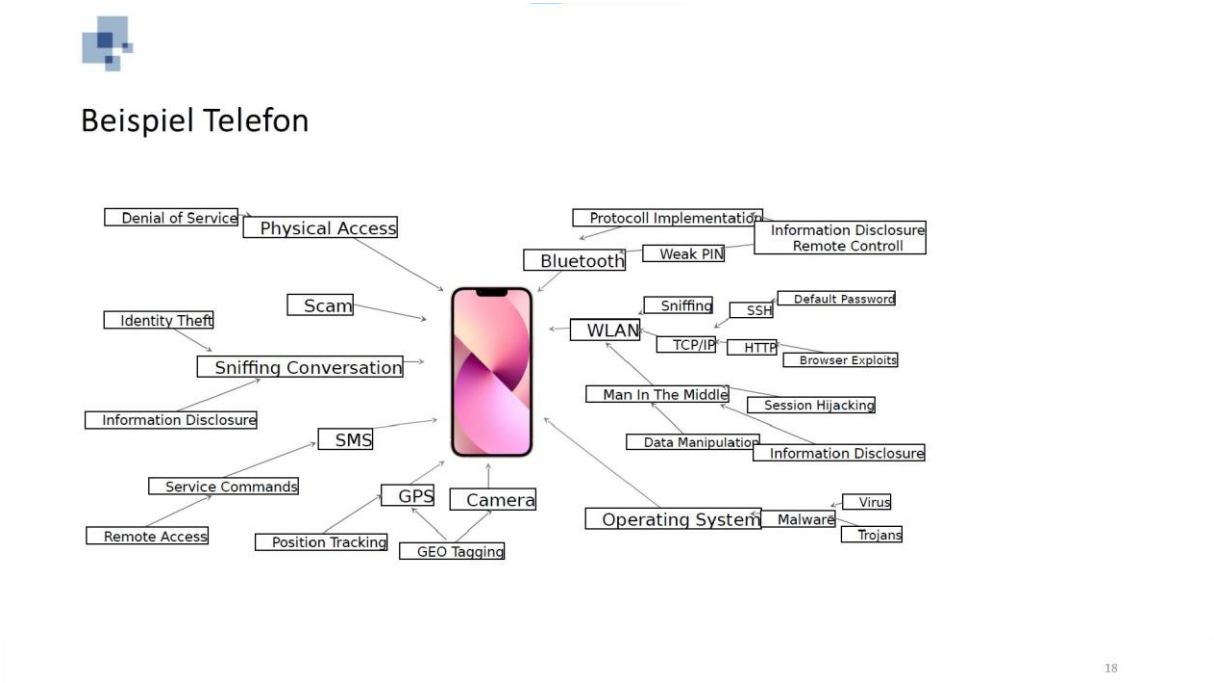
La Suisse est également concernée. La Suisse est elle aussi connectée au cyberespace et n'est pas une île de bienheureux, séparée du reste du cyberespace. On estime qu'en 2021, une entreprise sur trois en Suisse a été victime de cybercriminalité - mais le nombre de cas non recensés devrait être encore bien plus élevé**.**

"En tant que société dans son ensemble, on en fait encore trop peu pour assurer une protection adéquate".

Dans le contexte de l'énorme ampleur des dommages causés par les cyber-attaques, un point lui tient particulièrement à cœur : "Dans le cyberespace, nous aurions un plus grand effet de levier pour nous protéger par rapport aux dangers naturels et autres, et nous pourrions nous défendre contre les agresseurs". Cependant, de nombreuses personnes ne **comprennent toujours pas le cyberespace** en lui-même et les dangers qui y sont liés. Certes, une forte sensibilisation a eu lieu au cours des trois dernières années, mais le sentiment d'être concerné est encore trop minimisé, bien que tout le monde puisse être la cible d'une cyberattaque. En conséquence, la société dans son ensemble ne fait toujours pas assez d'efforts pour aborder le problème de manière adéquate.

La complexité, ennemie de la sécurité

L'exemple de nos téléphones portables illustre bien pourquoi la protection dans le cyberespace est à la fois si importante et si difficile. Les téléphones mobiles d'origine disposaient d'un ensemble de fonctions limité, avec des possibilités d'intervention limitées pour les pirates. Mais l'évolution des téléphones mobiles, à une vitesse inégalée, a entraîné ces dernières années une multiplication de l'ensemble des fonctions de nos appareils, et donc de **leur complexité et de leurs vulnérabilités**.



L'ensemble de l'informatique a connu une évolution comparable au cours des 20 dernières années. Des systèmes simples à l'origine ont littéralement explosé en termes de complexité, et **la complexité est connue pour être l'un des plus grands ennemis de la sécurité**. Sécuriser des systèmes d'un tel niveau de complexité est extrêmement difficile. Si cet état de fait avait été pris en compte de manière plus conséquente au cours des dernières années, nous ne serions pas confrontés aujourd'hui à des montants de dommages aussi énormes.

En Suisse aussi, nous sommes régulièrement victimes et il ne s'agit pas de pointer quelqu'un du doigt, mais plutôt de susciter l'émotion et l'action. Il faut s'améliorer, du gouvernement aux médias, de l'économie à la société dans son ensemble. Si l'on surmonte l'obstacle sensoriel du cyberespace à l'aide d'outils et qu'on le rend visible, on voit alors la masse de vulnérabilités qui se trouvent dans le cyberespace et qui sont connues du public. "**Celui qui laisse la porte du coffre-fort ouverte et accroche un panneau dans la rue ne doit pas s'étonner que les voleurs de données frappent sans pitié"**, a-t-il illustré la situation actuelle dans le cyberespace suisse.

Il n'a pas non plus d'explication définitive sur la manière dont le cyberespace pourrait être entièrement sécurisé, géré et contrôlé. Il serait peut-être utile de faire une pause, d'**analyser en profondeur** l'**évolution** effrénée **des 20 dernières années** et **de traiter** le **cyberespace avec le respect nécessaire**, comme on le fait avec l'espace physique - où l'on ne laisse pas non plus les portes des coffres-forts ouvertes. Et enfin, il faudrait commencer à démystifier la dimension cybernétique et à y intégrer les caractéristiques humaines uniques.

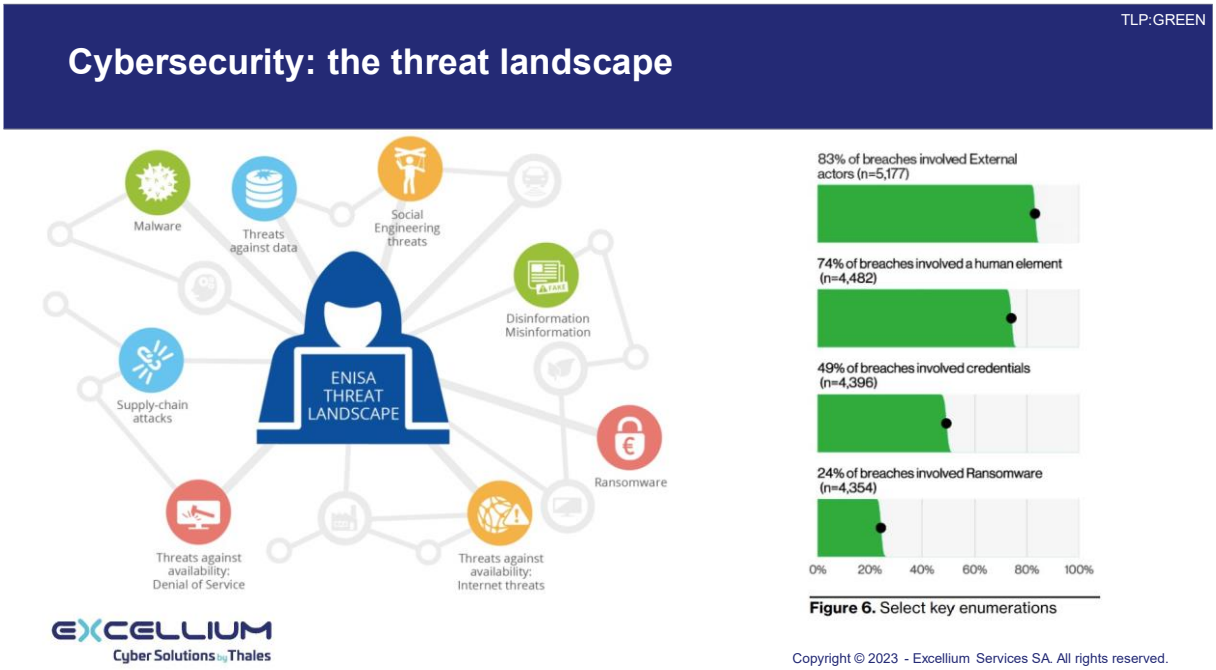
Exposé Johann Alessandroni

Les précieuses contributions précédentes ayant bien cerné le contexte des dangers du cyberespace, Johann Alessandroni a montré comment la cybersécurité peut être aménagée dans la pratique.

Reconnaître, utiliser, transmettre

Lorsque l'on parle de sécurisation des systèmes d'information, il faut d'abord se demander où se situent les risques et comment les gérer. Il ne suffit pas de considérer les systèmes en tant que tels ; le **facteur humain** doit également être pris en compte en tant que facteur important. Commencer par les systèmes et les rendre plus sûrs est déjà un grand défi, mais trouver les bons leviers pour l'homme et

adapter son comportement est encore bien plus difficile. L'importance du facteur humain dans la cybersécurité est également illustrée par les statistiques. **En 2020**, **74 % des cyberattaques étaient liées au facteur humain**. Pour les fabricants de solutions de cybersécurité, cela signifie que le facteur humain ne doit jamais être négligé dans les stratégies de sécurisation des systèmes.



Les statistiques et **les informations** sont généralement importantes pour **comprendre** la **situation des dangers dans le cyberespace,** mais il est encore plus important de savoir comment utiliser les connaissances acquises pour améliorer la cybersécurité. On voit par exemple dans les statistiques que les attaques ont fortement augmenté ces dernières années et que le cyberespionnage est le moyen privilégié au niveau de l'État. La question est maintenant de savoir comment appliquer ces connaissances aux autres niveaux, par exemple non gouvernementaux, afin de mieux se protéger. Les observations faites lors de la guerre en Ukraine en sont un autre exemple. La guerre physique a commencé en février 2022. Or, depuis septembre/octobre 2021, on observe déjà des cyberattaques de groupes russes contre des institutions vitales en Ukraine. La cyber-guerre était donc déjà en cours bien avant que la guerre ne se manifeste sur le champ de bataille. Cette constatation montre que **la cybercriminalité est souvent utilisée de manière proactive comme moyen d'accéder à des informations importantes**. Par conséquent, la cyberdéfense doit également être anticipée afin de se protéger de manière proactive.

Il s'agit donc de transposer toutes ces connaissances aux différents niveaux et secteurs à protéger, qu'il s'agisse du secteur de la santé, de l'industrie ou du secteur financier. L'accent est mis non seulement sur la **protection initiale des systèmes**, **mais aussi sur la capacité de détection et de réaction si une attaque est en cours**. La capacité à reconnaître à temps une compromission de son propre système d'information est élémentaire pour limiter les conséquences d'une attaque potentielle. Les informations obtenues à partir d'une compromission détectée à l'avance permettraient à leur tour d'améliorer leur propre détection précoce. Là encore, il s'agit donc de collecter des informations et de les utiliser pour se protéger efficacement contre les cyberattaques. Il en va de même pour les attaques dont on n'est pas directement victime. Dans ce cas, on pourrait bien sûr se contenter de s'asseoir et de se réjouir d'avoir été épargné. Il serait plus judicieux d'enregistrer les informations de l'attaque observée et de les utiliser pour améliorer la protection de ses propres systèmes.

Gestion proactive et globale des risques

Ces informations tactiques et stratégiques doivent également être utilisées pour vérifier et adapter en permanence l'évaluation des risques. Une telle approche basée sur les risques est déjà pratiquée depuis des années dans de nombreux domaines, y compris en dehors du cybermonde. La masse de cyberattaques observée actuellement dans le cadre des guerres en Ukraine et à Gaza et de leurs événements secondaires doit par exemple toujours être prise en compte dans la propre évaluation des risques. Que ce soit parce que l'on entretient des liens concrets avec les acteurs concernés ou simplement parce que les attaques sont de plus en plus fréquentes et graves. **Le risque d'être soi-même victime d'une attaque a clairement augmenté avec les guerres**. L'évaluation des risques doit donc être constamment développée et adaptée au contexte dans le cadre d'une gestion proactive des risques sur la base des informations tactiques et stratégiques disponibles, et avec elle la propre stratégie de cybersécurité.

Il est essentiel de ne pas attendre qu'un dommage se produise pour agir. Aujourd'hui, les solutions automatisées pour une détection et une réaction précoces sont certes déjà très bonnes. Mais si elles ne sont pas alimentées en amont par les données correspondantes, elles ne peuvent pas déployer suffisamment d'effets et se développer. Plus les informations sont bonnes, fiables et actuelles, plus les possibilités de détection et de réaction automatiques sont avancées et adaptées. Il faut bien sûr tenir compte des différences entre les pays. Si la plupart des informations peuvent être utilisées dans une certaine mesure de manière universelle, les informations contextuelles spécifiques restent extrêmement importantes pour un concept de sécurité adapté à chaque organisation.

Les attaquants cherchent toujours la voie de la résistance la plus facile

Lors de l'élaboration d'un tel concept de sécurité, ou d'une stratégie de cybersécurité, il est important, comme nous l'avons déjà mentionné au début, de ne **pas tenir compte uniquement du niveau technologique, mais de viser une protection globale de ses points finaux**, y compris le facteur humain et la sécurité physique des systèmes et des installations. Négliger l'un de ces domaines, c'est négliger un facteur qui pourrait favoriser une attaque demain. Les attaquants cherchent toujours la voie de la résistance la plus facile. Plus les lignes de défense pour la protection d'un système sont nombreuses, plus les attaquants se concentreront sur d'autres cibles. Ainsi, dès que l'on signale de manière crédible que l'on dispose a priori d'une certaine robustesse et de mesures de sécurité, les attaquants se tournent souvent vers d'autres cibles plus faciles.

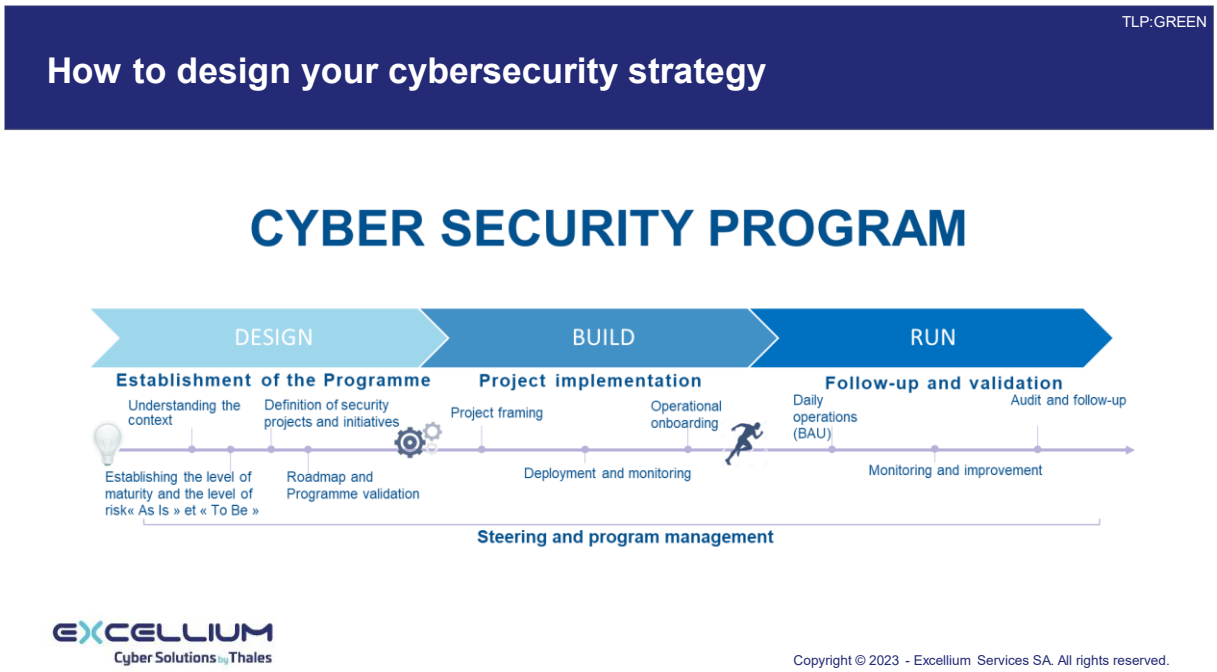
Une question de ressources

Une question importante lors de la mise en œuvre d'une stratégie de cybersécurité est toujours celle de l'ampleur des ressources à allouer. Les ressources disponibles pour la cybersécurité varient d'une organisation à l'autre. Les investissements dans la cybersécurité impliquent toujours des réductions de budget dans d'autres domaines. Heureusement, une **protection de base dans le domaine de la cybersécurité est possible avec relativement peu d'efforts**, mais il est donc important de définir correctement les objectifs dès le début. Sans définition des objectifs, il ne sera pas possible d'établir une stratégie de sécurité structurée, réfléchie et d'une efficacité démontrable. Il faut également se défaire de l'idée d'une quelconque supertechnologie magique capable d'offrir une protection complète. En fin de compte, c'est toujours l'ensemble ou la logique globale des mesures qui détermine leur protection.

Un autre aspect important dont nous devons nous souvenir est le rôle de notre écosystème, c'est-à-dire de notre réseau de relations**. Souvent, nous ne maîtrisons pas nos propres risques**. Les liens étroits qui existent dans le monde d'aujourd'hui font que les attaques contre les partenaires, les personnes et les organisations avec lesquelles on collabore peuvent aussi représenter un risque de sécurité pour nous-mêmes. C'est pourquoi il est important d'examiner de près les éventuelles failles de sécurité qui pourraient se trouver dans les relations avec ses partenaires et de les intégrer dans sa propre stratégie.

Comme nous l'avons déjà mentionné, lorsque l'on parle de cybersécurité, il faut également réfléchir à la manière de réagir si le pire des cas se produit. Les investissements dans la cybersécurité ne servent donc pas seulement à se protéger contre les cyberattaques, mais aussi à les détecter et à réagir en conséquence. On parle alors de gestion de la continuité des activités ou de gestion de crise. Ces points devraient toujours être considérés comme prioritaires dans une stratégie de sécurité. Les entreprises qui subissent les plus grandes conséquences d'une cyberattaque sont toujours celles qui ont négligé ces points importants et n'ont donc pas pu garantir la poursuite de leurs activités.

Pas à pas vers une protection efficace



Si l'on considère le processus classique d'élaboration et de mise en œuvre d'une stratégie de cybersécurité, la **première étape consiste** généralement à **définir** le **contexte**. Comme nous l'avons déjà mentionné, aucune organisation ne ressemble à une autre. Il faut comprendre l'utilité d'une organisation, les risques et l'impact sur l'écosystème afin de pouvoir définir comment la protection dans le domaine cybernétique doit être conçue. Ensuite, il faut **évaluer le niveau de sécurité existant** afin de déterminer comment il est conçu et où il faudrait intervenir pour atteindre les objectifs fixés. Ensuite, les **mesures recommandées sont modélisées**. Il est important de souligner la valeur ajoutée de chaque mesure afin de ne pas se concentrer uniquement sur les coûts. Il convient également de définir des étapes et des indicateurs de performance, de suivre et de discuter des progrès et des activités dans le cadre de bilans réguliers et de contrôles de sécurité.

Conclusion

Comme pour l'élaboration et la mise en œuvre de toute stratégie, il est important de procéder de manière structurée et pragmatique en matière de cybersécurité. Il faut être conscient qu'il n'**existe pas de solutions magiques**. Cela signifie également qu'il faut s'engager dans une **certaine logique** et une **certaine approche** et **fixer des priorités de manière pragmatique afin d**'utiliser au mieux les ressources disponibles. Dans ce contexte, il est également important de se rappeler constamment la logique et la structure de la stratégie et des mesures choisies et de revenir sur les raisons pour lesquelles les mesures choisies sont utiles et sur les objectifs qu'elles permettent d'atteindre. L'**observation de l'écosystème** dans lequel on se trouve et l'**examen constant du contexte** aident également à une compréhension globale. Enfin, il faut **toujours être conscient** des **risques** et adapter ses décisions en fonction de ceux-ci et des conséquences potentielles d'une attaque. Cette façon de penser est essentielle pour aborder activement les projets visant à renforcer sa propre cyber-résilience et être prêt si le pire devait se produire.

La discussion en panel

Les deux exposés ont été suivis d'une **discussion de** haut niveau animée par **Fredy Müller**, directeur du FORUM SÉCURITÉ SUISSE. Outre les quatre intervenants, **Franz Grüter** (président du conseil d'administration du groupe green.ch ; conseiller national UDC, LU) a également participé à la discussion.

Pour commencer, le modérateur s'est adressé à **Franz Grüter** et a voulu savoir si les conclusions des exposés d'introduction l'étonnaient.

Ce dernier a rétorqué qu'il ne parlait pas en tant que conseiller national, mais en tant qu'entrepreneur dans le domaine des centres de calcul et des centres de données, et qu'il fallait tout d'abord souligner le rôle prépondérant de la Suisse en Europe : **"Nous sommes l'un des principaux sites de données en Europe, nous disposons de nombreuses infrastructures et abritons les hubs de presque tous les grands fournisseurs de cloud. De là, nous sommes naturellement aussi exposés et une cible intéressante pour les attaques". Ce** qui est nouveau pour lui, c'est la statistique selon laquelle la Suisse n'occupe que la 42e place dans le classement de la cybersécurité. Selon lui, cela s'explique notamment par le fait que pendant longtemps, on **n'a pas suffisamment pris conscience** des **risques dans le cyberespace, même en politique**. Lorsqu'il a été élu au Conseil national en 2015, il a déposé avec quelques autres parlementaires les premières interventions sur la cybersécurité au Parlement, et à l'époque, beaucoup ne les prenaient pas encore vraiment au sérieux. Ce n'est qu'avec les incidents majeurs qui se sont multipliés en Suisse à partir de 2018 que le sujet a pris de l'importance et que l'on a commencé à s'équiper.

L'espionnage comme moyen d'État

Après ces quelques mots d'introduction, le présentateur s'est tourné vers le **Dr Myriam Dunn Cavelty** et lui a demandé d'approfondir les capacités dont un Etat a besoin pour mener à bien ses activités d'espionnage.

Celle-ci a répondu que le **cadre PETIO**, composé des abréviations de People, Exploits, Toolset, Infrastructure et Organization, était un outil répandu qui décrivait les ressources nécessaires aux cyberactions offensives. Auparavant, on imaginait qu'un groupe de hackers pouvait mener de telles opérations dans une cave, mais ce n'est pas le cas. **"Il faut vraiment des capacités spécifiques et distinctes, et il n'est donc pas surprenant que les Etats qui ont développé leurs capacités dans le cyberespace depuis des décennies soient ceux qui sont les plus actifs aujourd'hui"**, a-t-elle souligné en mettant l'accent sur les exigences élevées des activités d'espionnage dans le cyberespace.

L'espionnage était déjà un moyen répandu par le passé. Mais avec l'avènement du cyberespace, leur apparition a changé et s'est cumulée. Le modérateur a demandé **au major général Setzer** ce que l'apparition de ce danger sous une nouvelle forme signifiait concrètement pour la Bundeswehr dans son quotidien.

Il est vrai que les activités d'espionnage étaient déjà répandues auparavant, mais elles constituent désormais un moyen essentiel pour les Etats dans la dimension du cyberespace et de l'espace d'information. L'objectif de l'espionnage a toujours été d'obtenir des données. Aujourd'hui, ces données sont stockées sous forme numérique sur des serveurs et dans le cloud, et le cyberespionnage est donc un moyen évident pour beaucoup.

A l'inverse, il est bien sûr nécessaire d'une part de mettre en place des fonctions de protection pour protéger ses propres systèmes contre les intrusions extérieures, mais aussi de construire les systèmes de manière à ce qu'ils soient protégés à l'intérieur. "**Il ne peut jamais être exclu qu'un agresseur s'introduise dans un système, et dans ce cas, il faut un système de détection et de réaction qui fonctionne"**, a souligné le major général Setzer en insistant sur la nécessité d'une protection complète.

Pour elle, il est également important que la protection ne soit pas simplement centralisée. Au total, si l'on compte les civils et les militaires, ils sont environ 270 000 dans la Bundeswehr. Ils ont mis en place des responsables de la sécurité de l'information (RSSI) jusqu'au niveau le plus bas de l'organisation, de sorte qu'ils disposent d'un large réseau de capteurs. Enfin, il faut encore préciser que le cyberespionnage est certes très répandu actuellement, mais que si quelqu'un s'est déjà introduit dans un réseau, l'espionnage peut à un moment donné se transformer en sabotage et représenter un danger pour nos infrastructures critiques, sans pour autant franchir le seuil d'un conflit armé. Il cite volontiers le théoricien militaire Clausewitz : "Dans une guerre, il ne s'agit pas de détruire quelqu'un, mais de lui imposer sa propre volonté. Si aucun moyen militaire n'est nécessaire et que le seuil de la guerre ne doit pas être dépassé, alors le cyberespace représente un moyen éprouvé qui est utilisé.

Les cyberattaques sous différents habits

L'animateur a mentionné que les cyberattaques ne devaient pas toujours prendre la forme d'attaques de grande envergure, mais que des attaques récurrentes à bas seuil pouvaient également être très efficaces, et s'est adressé à **Nicolas Mayencourt** en lui demandant s'il observait également une telle activité.

Ce dernier est d'accord et a rétorqué que les attaques à bas seuil peuvent être très efficaces. C'est justement lorsqu'il n'y a pas d'hygiène de l'information et qu'il existe de petites fuites à de nombreux endroits différents qu'un attaquant peut collecter systématiquement des informations précieuses pendant des années. Il serait ainsi possible de générer des images d'informations complètes sans avoir à recourir à de grands piratages techniques pour y accéder. Le terme "persistant" dans l'expression "Advanced Persistent Threat" est également synonyme de cette constance et c'est sur ce point que réside finalement le critère de différenciation par rapport à la criminalité classique. Normalement, les criminels sont opportunistes et n'agissent pas de manière persistante, mais cherchent plutôt des victimes "faciles". Nicolas Mayencourt a laissé entendre la conclusion qui en résulte : **"Pour se protéger des criminels, il ne faut donc pas être le mieux protégé, il faut simplement éviter au maximum d'être le moins bien protégé".**

Le modérateur s'est ensuite tourné vers le **Dr Myriam Dunn Cavelty** pour lui demander quel rôle les événements à forte visibilité, tels que l'affaire Snowden, avaient joué dans la prise de conscience de la cybersécurité depuis 2010.

A ses yeux, ce qui est intéressant à cet égard, c'est que l'affaire Snowden a pour la première fois attiré l'attention du public sur les services de renseignement. Ce n'est que grâce à cette révélation que l'on a appris que les **services de renseignement étaient actifs dans le cyberespace** et avaient développé des capacités correspondantes. Selon elle, de tels événements ont définitivement le potentiel de former la conscience du public.

Concurrence stratégique

L'animateur s'est tourné vers le **major général Setzer** et lui a demandé s'il voyait dans la strategic competition, cette compétition, cette concentration de pouvoir en dessous du seuil de la guerre, une des raisons de l'augmentation des cyberattaques.

Le major-général Setzer a déclaré que pour poser la question de la raison des cyberopérations étatiques, il fallait toujours prendre en compte la question de l'intention. On peut prendre l'exemple de la Chine, qui s'est fixé pour objectif de devenir la première puissance mondiale dans tous les domaines d'ici 2049 au plus tard. Lorsqu'un pays annonce un tel objectif, il organise également toute sa stratégie en fonction de celui-ci. Pour atteindre cet objectif, la Chine n'a pas seulement besoin de puissance militaire, mais aussi d'influence dans les domaines de la science, de l'industrie, etc. Tous les

moyens disponibles, y compris le cyber, seront donc utilisés pour atteindre les objectifs fixés. Il est toutefois important de noter que **la séparation classique entre les actions étatiques dans le cyberespace et le crime organisé n'est souvent plus facile à réaliser aujourd'hui.** Au lieu de cela, on observe même parfois des acteurs qui travaillent le jour pour l'Etat et la nuit pour leur propre compte.

Attribution publique

L'animateur a fait remarquer que l'on avait déjà beaucoup parlé des motivations et des compétences requises pour le cyberespionnage, avant d'aborder le phénomène selon lequel les cybercriminels, lorsqu'ils sont démasqués, sont cités publiquement de manière très intensive. Il a demandé au **Dr Myriam Dunn Cavelty** pourquoi les criminels étaient si exposés.

Il y a deux aspects : Un élément de sécurité informatique doit montrer que les auteurs, leurs méthodes et leurs outils sont connus et qu'il est possible de se protéger. Le deuxième aspect comprend bien sûr aussi une composante politique, appelée **attribution publique**, qui n'existe que **depuis une dizaine d'années.** Cela fait partie de cette concurrence stratégique et est lié à la capacité de pouvoir potentiellement punir quelqu'un plus tard.

Le modérateur a demandé au **major général Setzer** comment on punissait efficacement dans le cyberespace et comment on ripostait dans l'armée allemande lorsqu'elle était attaquée.

Le major général Setzer a répondu qu'il s'agissait d'une question très intéressante. La notion **d'attribution publique est** très importante. En Allemagne, par exemple, il a fallu plus de cinq ans pour que le gouvernement attribue publiquement l'attaque contre le Bundestag et nomme l'agresseur. D'un point de vue stratégique, on réfléchit très soigneusement à de telles attributions, mais elles offrent la possibilité de faire savoir aux agresseurs qu'**une certaine limite a été atteinte**. Sa réponse à la question de savoir ce qui serait fait si la Bundeswehr était attaquée dans le cyberespace et quand la limite d'un conflit armé serait franchie peut être résumée comme suit. Le secrétaire général de l'OTAN a clairement exprimé qu'une attaque dans la dimension cyber, dont l'ampleur serait équivalente à celle d'une attaque conventionnelle dans un conflit armé, ferait l'objet d'une réponse avec les moyens nécessaires.

Le présentateur s'est alors tourné vers le **Dr Myriam Dunn Cavelty pour lui demander** si la classification des attaques par modèle, comme le font depuis peu les Américains, aidait à identifier ces attaques et leurs intentions.

Myriam Dunn Cavelty a répondu que l'appréhension de ce type de cyberattaques s'appelait "penser en termes de campagne". Auparavant, on pensait encore en termes d'attaques individuelles, mais on s'est rendu compte à un moment donné que les auteurs de telles attaques étaient souvent des acteurs similaires. **Il est fréquent que l'arrière-plan des attaques ne devienne visible que lorsque les attaques sont considérées ensemble et que l'on obtient ainsi une image globale.** C'est pour cette raison que l'on est passé à l'examen des effets cumulatifs et non plus des effets individuels. Cela permet même souvent de constater que les conséquences effectives des attaques sont encore plus graves que les conséquences monétaires des différentes attaques, car les informations collectées lors des différentes attaques cumulées peuvent par exemple être encore plus dangereuses.

Le manque d'informations rend difficile l'évaluation de la situation

L'animateur a ensuite demandé à **Franz Grüter** comment il jugeait la situation de la Suisse dans ce contexte.

Ce dernier a commencé à évoquer son mandat de président de la Commission de politique étrangère. Dans le cadre de cette fonction, qu'il occupera encore jusqu'à la fin de l'année, ils ont été confrontés à deux guerres, la guerre en Ukraine et la guerre à Gaza. Pour l'accomplissement de leurs tâches, ils ont en partie recours aux informations du service de renseignement et là aussi, on remarque que seule une certaine partie des informations est transmise. C'est pourquoi il est difficile pour lui aussi d'évaluer la situation dans son intégralité. Il ne peut donc pas non plus porter un jugement définitif sur la Suisse dans le cyberespace.

Sur la base de cette réponse, l'animateur a transmis la question à **Nicolas Mayencourt** et a voulu savoir en outre si des réflexions stratégiques sur la transmission d'informations et la préservation de la souveraineté d'opinion dans les propres rangs faisaient partie de ce jeu.

Celui-ci a répondu que c'était clairement le cas et que cela était devenu nettement plus sensible au cours des dix dernières années. **Aujourd'hui, on peut observer que la perception contribue systématiquement au déroulement de la guerre.** Lors de la guerre en Ukraine, on a pu assister pour la première fois à des campagnes de médias sociaux parfaitement mises en scène par les deux parties. Leur influence sur la perception peut donc être tout à fait décisive, puisqu'elle se répercute finalement sur les décisions budgétaires. Il est donc tout à fait normal que nous ne puissions pas encore savoir beaucoup de choses dans la guerre conventionnelle ou dans la cyber-guerre, car ces connaissances sont actuellement encore d'une importance stratégique.

Il a été demandé à **Johann Alessandroni** s'il savait que les flux d'informations étaient souvent filtrés ou orchestrés et comment il le percevait dans son travail, étant donné que son travail visait précisément à faire connaître les dangers des cyberattaques.

Il a répondu qu'ils observaient eux aussi que seuls certains incidents à la mode apparaissaient dans la presse ou les médias. Parallèlement, ils observent une forte augmentation des incidents qui sont moins perçus par le public. Il serait toutefois important que toutes les attaques soient connues et reçues par le public, d'une part pour que les gens prennent conscience des dangers, et d'autre part parce qu'une compréhension globale des méthodes d'attaque à la base de ces attaques pourrait également être utilisée pour la protection des autres systèmes.

Nouveau monde - anciennes technologies

L'animateur s'est référé à un entretien préliminaire et a noté que le cyberespace actuel était en fait prédestiné à être attaqué. Il a ensuite demandé **à Nicolas Mayencourt** pourquoi cette situation n'avait pas été reconnue ou abordée plus tôt.

Celui-ci a répondu qu'Internet et les technologies de l'information ont été construits pour rendre l'information accessible. Les inventeurs de ces technologies voulaient libérer et partager l'information. Il qualifierait presque la situation qu'il trouve aujourd'hui de "Success-Disaster". **La technologie était si bonne que la société l'a adaptée et absorbée aussi rapidement qu'une éponge sèche**. Mais ces **technologies**, ni le protocole Internet, ni les puces, ni les paradigmes de développement de logiciels, n'**ont jamais été construites avec des concepts de sécurité informatique.** Les fondateurs et les créateurs n'auraient pas pu imaginer un monde tel qu'il est aujourd'hui et n'auraient pas non plus équipé les fondations des technologies actuelles en conséquence. Ce qu'il voit aujourd'hui n'est rien d'autre que le résultat de la mise en place de technologies immatures et de la tentative de combler les lacunes par une politique de pansement, ce qui ne peut toutefois jamais fonctionner complètement, car la technologie de base n'est fondamentalement pas dotée de caractéristiques de sécurité. En fait, il faudrait commencer par ces fondations et les réviser, dit du moins l'ingénieur en lui. Mais l'homme en lui reconnaît aussi que cela ne sera guère possible, car le monde entier est déjà équipé de technologies fondamentalement vulnérables.

L'animateur transmet le sujet au **major général Setzer** et lui demande si la désignation des faiblesses d'Internet est un thème de leurs cours et comment ils abordent le sujet des désastres successifs.

Celui-ci a voulu mettre une chose en avant, à savoir qu'Internet et la numérisation les ont fait progresser. Il faut maintenant faire attention à ne pas jeter le bébé avec l'eau du bain. Ils reconnaissent actuellement successivement que tout a deux côtés. Mais il ne faut pas non plus tout réduire d'un coup. Dans cette compétition dont on parle, celui qui restera à la pointe de la technologie durera au moins aussi longtemps que les autres. Il a utilisé à cet effet l'exemple courant de l'IA. L'IA est un nouveau logiciel avec de nouvelles possibilités. Nous allons les utiliser, nous les utilisons déjà. L'IA comporte des dangers, mais elle peut également aider à la sécurité de l'information et à la protection du système. On peut donc utiliser l'IA pour rendre le système plus résilient, car elle est capable de

détecter des anomalies dans le système beaucoup plus rapidement que ne le ferait un être humain. Dans le développement, l'accent n'est donc pas uniquement mis sur "Fight the problem", dans l'optique que tout ce que vous avez est mauvais, mais principalement sur la manière d'améliorer l'existant. Il cite trois mots-clés à ce sujet. Le premier est la "**sécurité dès la conception**" pour les futurs systèmes, de sorte que le code de sécurité soit inclus dès le départ. Deuxièmement, il faut former les personnes qui s'en servent afin qu'elles puissent les utiliser à bon escient, notamment du point de vue de l'**ingénierie sociale**. Troisièmement, et c'est le plus grand défi, ils doivent créer des procédures pour les "**systèmes existants**" afin de remédier à leurs vulnérabilités. Ceux-ci devraient si possible être remplacés par des systèmes futurs adéquats. Mais sa philosophie est de ne pas se cacher la tête dans le sable, mais de continuer à faire avancer la numérisation et la sécurité à la pointe du progrès.

L'analogie plutôt que la numérisation ?

L'animateur s'interroge sur ce point et demande à **Nicolas Mayencourt** s'il ne serait pas préférable de passer moins de temps dans le monde numérique et de revenir à l'analogique, ce qui nous rendrait moins dépendants du traitement des données par l'IA. Avec une légère touche d'ironie, l'animateur a demandé s'il ne serait pas préférable de noter à nouveau ses mots de passe sur un bout de papier plutôt que de les enregistrer sur Internet.

Nicolas Mayencourt a répondu qu'il existe une règle de base qui est la suivante : **"Qui ne vit pas avec son temps, vit avec son temps".** La numérisation est là pour rester, et elle apporte beaucoup de bonnes choses. Il ne peut que souscrire à cette affirmation. Il y a de très, très nombreux aspects positifs. Son vote à ce stade serait d'arrêter d'être naïf. Il faut accorder à la numérisation et au cyberespace le sérieux nécessaire et les considérer avec le respect requis. Envisager un système d'exploitation pour une centrale nucléaire, dont le contrat de licence stipule "not fit for any purpose" et exclut toute responsabilité, est tout simplement faux. Cela ne peut pas être le but. C'est précisément là qu'il faut intervenir et peut-être ne pas se demander seulement ce que l'on peut faire, mais aussi si cela a un sens et comment on peut le faire de manière judicieuse. Il veut dire par là qu'il ne faut pas arrêter, mais procéder de manière plus contrôlée et plus efficace.

Réglementation internationale

Après cette réponse, le modérateur a abordé la suggestion mentionnée concernant la création d'une réglementation internationale et a demandé **au Dr Myriam Dunn Cavelty** s'il s'agissait d'un sujet d'avenir.

Celle-ci répond que c'est clairement le cas et qu'il existe déjà **des normes et des règles** à différents niveaux, par exemple à l'**OTAN** ou à l'**ONU**. Bien sûr, on discute aussi de réglementations, il y en a déjà dans l'UE et chez nous aussi. Aux États-Unis, il apparaît clairement depuis cette année que l'on souhaite miser sur une réglementation renforcée dans le secteur informatique. Elle a en outre déclaré qu'il n'était pas nécessaire de tout réglementer, mais qu'il fallait procéder avec des têtes lors de la mise en œuvre ultérieure. Mais elle pense que nous y parviendrons, si la volonté est là.

Nicolas Mayencourt a ajouté que nous étions déjà passés par là. A titre d'exemple, il a montré **l'évolution de la voiture**, avec laquelle on peut établir quelques parallèles. En effet, les ceintures de sécurité n'existaient pas au départ, mais en raison de l'accumulation d'accidents graves, tout un ensemble de règles de sécurité a été mis en place au fil du temps, ce qui explique que nous ayons aujourd'hui des ceintures, des airbags et un permis de conduire. Grâce à ce système, l'ampleur des dommages a été réduite au point de se situer aujourd'hui dans un cadre acceptable. De plus, il y a l'Union internationale des communications, sans laquelle il n'y aurait pas de réseau téléphonique aujourd'hui. De nombreuses choses y sont très bien réglées. En ce qui concerne l'Internet, on a longtemps défendu l'idée qu'on ne pouvait de toute façon pas le contrôler, ce qui était faux et l'est

toujours. Les possibilités existent déjà, nous avons aussi les organisations nécessaires, nous devons simplement les utiliser.

Vers la fin, le modérateur s'adresse à nouveau à **Franz Grüter pour lui** poser une question. Il voulait savoir si, selon lui, le développement d'un cyberconseil à Genève, qui permettrait à la Suisse de jouer un rôle de premier plan dans ce domaine, semblait réaliste.

Il a dit qu'il voyait deux initiatives possibles. Dans le premier cas, le Luxembourg les a malheureusement devancés en développant une **e-Embassy**. C'est comparable à un aéroport international où le droit international s'applique. C'est là que le **CICR**, le Comité international de la Croix-Rouge, par exemple, stocke **ses données hautement sensibles**. Leurs données ont donc été déplacées dans un espace international non étatique. Les données se trouvent aujourd'hui au Luxembourg. L'Estonie a également mis en place une infrastructure secondaire complète au Luxembourg après la cyberattaque russe de 2007. Selon lui, la Suisse a raté le coche. Ils pourraient probablement encore le faire, car selon lui, un espace numérique similaire conviendrait très bien à Genève.

L'animateur a demandé dans quelle mesure la topographie unique de la Suisse et les ouvrages qui y sont liés, comme par exemple le tunnel du Gothard, pourraient constituer un avantage en permettant d'y établir des centres de données.

Franz Grüter a répondu qu'il existait des exemples de centres de calcul construits dans des bunkers. Il se réjouit toujours de ces projets, car ils contribuent à l'**image de la Suisse en tant que bunker de données**. En réalité, les risques pour les données stockées ne sont pas de nature physique, ce ne sont pas des cambrioleurs classiques qui y voleraient un surfeur, mais des attaques de pirates. Un centre de calcul dans un bunker serait aussi mal ou aussi bien protégé contre de telles attaques que dans un centre de données traditionnel.

Questions du public

Pour finir, l'animateur a ouvert la session de questions-réponses au public.

Adrian Marti, qui travaille pour la société Ereneos, a alors pris la parole. Il a déclaré qu'ils étaient eux-mêmes conseillers en sécurité de l'information auprès de grandes organisations. Il a demandé aux intervenants comment atteindre cet objectif.

L'animateur, visiblement ravi de la question, a déclaré qu'il s'agissait de sa question finale, mais qu'Adrian Marti l'avait devancé. Il s'est donc adressé aux panélistes en leur demandant comment on pouvait sensibiliser les gens à la sécurité en général.

Nicolas Mayencourt a répondu qu'il pensait que nous avions besoin d'une sorte de **mise à jour de notre contrat social,** car cela nécessiterait une sorte de "mini-mise à jour" de notre part à tous. **La sécurité est fondamentalement un sport d'équipe** qui a besoin de nous tous, sinon cela ne fonctionnera pas. Il faut donc parler des rôles, des droits et des obligations de chaque organisation. Il faut se demander ce que font les Suisses, ce que fait l'économie, ce que fait la recherche, ce que fait l'État, ce que fait l'armée - et les questions les plus importantes à poser sont de savoir comment on connaît la protection des frontières aujourd'hui et si on a besoin de quelque chose de similaire dans le cyberespace. Il a ainsi renvoyé la balle aux représentants politiques.

Le modérateur a fait la transition et a demandé à **Franz Grüter** comment nous pouvions devenir plus résilients et plus conscients de la sécurité.

Comme cela a déjà été mentionné, il s'est récemment rendu dans les pays baltes et également en Israël avant que la guerre n'éclate. Là-bas, les gens expriment souvent le fait qu'en raison de la paix existante depuis de nombreuses années, il existe parfois une certaine "**naïveté" en Suisse**. Nous ne sommes parfois pas assez conscients de ce qui se passe réellement dans le monde. Malgré tout, on peut tirer ici un bilan positif ; un changement de mentalité a eu lieu. On ne sait pas si, il y a huit ou dix ans, autant de personnes auraient pu être réunies ici sur un thème comme celui d'aujourd'hui. Mais aujourd'hui,

on en est plus conscient et les entreprises font de gros efforts, engagent par exemple des spécialistes pour les conseiller, et l'État a également fait des progrès. Au niveau fédéral, l'Office fédéral de la cybersécurité sera par exemple créé l'année prochaine.

Pour conclure, l'animateur s'est une nouvelle fois adressé au **major général Setzer** et lui a demandé comment il ressentait le fait que la population, mais aussi et surtout les jeunes, étaient devenus plus sensibles à la sécurité.

Celui-ci a fait remarquer que les jeunes sont probablement beaucoup plus à l'aise avec la numérisation que ne l'était sa génération. Cependant, les jeunes ont également besoin d'être informés, ce qui n'est pas encore le cas actuellement. Il faut également sensibiliser les établissements d'enseignement. De son point de vue, c'est quelque chose qui doit encore être renforcé, car comme nous l'avons déjà mentionné, la sécurité est un sport d'équipe qui commence par l'individu. **Les cyber-attaques commencent souvent par le maillon le plus faible de la chaîne**. C'est pourquoi la numérisation et la cybersécurité ne sont pas des questions dont seuls quelques-uns doivent s'occuper, mais qui concernent tout le monde. Dans ce contexte, le soutien aux journées de sensibilisation proposées ne peut être qu'encouragé.

Enfin, le présentateur a posé la question finale au **Dr Myriam Dunn Cavelty**.

Elle a fait comprendre qu'elle avait en fait voulu communiquer ce que le général avait dit : L'**éducation et la formation sont en tout cas nécessaires et indispensables**. Elle souhaiterait également que les personnes qui ont peur de la technologie puissent surmonter cette peur et se rendre compte qu'elle est aussi entre leurs mains, car le système est un système créé par l'homme, ce qui signifie qu'il peut aussi être changé. Mais pour cela, les gens doivent surmonter leur peur. Il s'agit en général d'un sujet très humain et elle souhaiterait qu'à l'avenir, les gens aient plus envie d'agir dans ce domaine.

La discussion du panel s'est ainsi terminée et le modérateur a remercié le public pour son attention et les panélistes pour l'intérêt de la discussion.

FORUM SICHERHEIT SCHWEIZ

FORUM SÉCURITÉ SUISSE

c/o MUELLER Consulting & Partner
Gemeindestrasse 48
CH-8032 Zürich

Téléphone +41 44 533 04 00
sekretariat@forum-sicherheit-schweiz.ch