«C'est d'un nouveau modèle dont nous avons besoin, car à long terme l'actuel n'est pas défendable»

Il n'y a pas de frontières nationales dans le cyberespace, un domaine qui devient toujours plus pertinent sur le plan militaire. Dans une double interview, l'ambassadeur ukrainien en Suisse, Dr Artem Rybchenko et Gérald Vernez, ancien délégué du DDPS pour la cyberdéfense et fondateur de digiVolution, parlent de la situation actuelle, des défis futurs et de solutions possibles.

Interview: Simon Gröflin

Messieurs Rybchenko et Vernez, quelle est l'importance de la relation entre l'Ukraine et la Suisse en matière d'échange d'expériences et de coopération dans le domaine de la cybersécurité?

Gérald Vernez: ancien Délégué du DDPS pour la cyberdéfense, fondateur de la Fondation digiVolution

Gérald Vernez: Je ne m'exprime plus au nom des autorités fédérales et vous me permettrez donc de ne pas commenter les relations entre nos deux États. Ce que je peux cependant dire après mes années au service de la Confédération, c'est que la coopération dans le domaine de la cybersécurité est une importante clé pour le succès. Celui qui n'apprend pas de l'expérience des autres retombera dans les mêmes pièges qu'eux. Échanger permet de réduire nos faiblesses et celles-ci profitent d'abord aux agresseurs.

Artem Rybchenko: C'est à partir de 2014 que la cybersécurité a vraiment gagné en importance pour l'Ukraine, lorsque la guerre hybride a été lancée par la partie russe. Nous voyons bien combien la pression actuelle replace cette question au premier plan. Tout échange d'expériences est donc important pour nous et la Suisse est connue pour ses nombreuses compétences. J'ai assisté aux Swiss Cyber Security Days 2021 et j'y ai gagné beaucoup d'expérience. Malheureusement, il n'y a pas beaucoup d'autres plates-formes de coopération comme la Suisse.

À quelles qualités de la Suisse faites-vous allusion?

A. Rybchenko: La Suisse accorde beaucoup d'importance à la cybersécurité et les technologies utilisées sont d'un standard élevé. Depuis ces dernières années, une coopération a été mise en place entre notre Ministère de la transformation numérique conduit par notre vice-premier ministre et la Suisse. Et plusieurs accords ont été signés entre nos deux pays. Nous apprécions vraiment le contenu et l'importance de cette coopération.

Comment appréciez-vous l'état de préparation de nos pays en cas de cyberguerre?

A. Rybchenko: Malheureusement, nous déplorons chaque année des cyberattaques – généralement le fait d'un seul pays – mais techniquement, les attaques proviennent du monde entier. Chez nous, les infrastructures critiques nationales

Artem Rybchenko, Ambassadeur extraordinaire et plénipotentiaire d'Ukraine en Suisse

sont toujours attaquées. Auparavant, les attaques visaient essentiellement des institutions privées, mais les institutions publiques sont désormais également prises pour cibles. Toutefois, notre expérience progresse fortement dans la lutte contre ces schémas d'attaque.

G. Vernez: Estimer notre état de préparation face à un conflit dans le cyberespace est une des questions les plus ardues. Dans le cyberespace, la Suisse a été jusqu'ici principalement confrontée à de la criminalité et à de l'espionnage. L'année dernière, 24 400 attaques ont été signalées à la police. Mais combien ne l'ont pas été? Dans cette appréciation, de nombreux facteurs entrent en considération, tels que l'état des infrastructures, les technologies déployées, la qualité de la maintenance et du personnel, la capacité de résilience, mais aussi la connaissance et l'anticipation des menaces, les bases légales, etc. En fait nous aurions besoin de déterminer la cybermaturité de la Suisse, mais nous ne savons pas encore le faire à cette échelle.

Quels sont les défis particuliers en matière de lutte contre la criminalité et quel rôle joue la coopération entre les deux pays?

G. Vernez: La coopération ne se décrète pas d'un coup de baguette magique. Elle repose sur deux piliers fragiles qui doivent être constamment entretenus: l'identification des intérêts communs et la confiance. Les intérêts communs ne sont pas difficiles à définir, mais il faut déterminer des priorités claires. Le pilier «confiance» est bien plus compliqué car il s'apparente à la loyauté et se construit dans le temps. Dans tous les cas auxquels j'ai été confronté, cela a pris des années. La confiance est un bien qui s'établit entre des personnes, c'est de l'alchimie.

«L'Ukraine est réputée pour ses jeunes spécialistes en informatique bien formés.»

Artem Rybchenko

A. Rybchenko: Chaque année voit arriver de nouvelles technologies qui ne sont pas uniquement utilisées par les États, mais aussi souvent par des criminels. Réussir à contrôler ces nouvelles technologies est très difficile, mais l'échange d'expérience est un grand avantage. Nous informons donc nos partenaires au sujet de toutes les formes d'agressions auxquelles nous sommes exposés. Cela comprend autant nos voisins «post-soviétiques» que les pays de l'UE. Mais la situation de l'Ukraine est très particulière: d'un côté, nous suivons la voie européenne, mais de l'autre nous sommes dans une situation de «zone tampon» (je n'aime pas beaucoup ce terme) avec encore de nombreuses normes soviétiques. Les institutions de sécurité nationale et de défense sont les principaux responsables pour la cybersécurité, mais nous disposons également d'une police spécialisée pour la poursuite des cyberdélits et la criminalité financière. Chaque pays est organisé un peu différemment et c'est pourquoi un échange actif d'expérience est si important et apporte des avantages déterminants dans la lutte contre la cybercriminalité.

Le chef de l'armée, Thomas Süssli, a plaidé lors des Swiss Cyber Security Days pour un échange renforcé avec le paysage universitaire afin de promouvoir le recrutement de plus d'experts en science des données et en cryptographie. Comment appréciez-vous cet élément?

A. Rybchenko: Le secteur privé joue un rôle important dans les infrastructures informatiques. L'Ukraine est réputée pour ses jeunes informaticiens bien formés. Ce n'est pas pour rien qu'on les nomme «Grains and Brains». L'un des axes de notre enseignement est clairement le secteur des TIC. De nombreux hubs et plates-formes ont été développés au cours des dix dernières années. L'année dernière, ces plates-formes ont également fait l'objet d'un échange d'idées lors d'une rencontre entre notre gouvernement et la conseillère fédérale Sommaruga à Kiev.

G. Vernez: Je partage le point de vue du Chef de l'Armée. Nous devons cependant chasser de nos esprits l'illusion que nous pourrons produire des «cybergénies» en suffisance. Notre formation s'améliore indéniablement aujourd'hui – par exemple, dans le cadre des échanges entre l'armée, les EPF et le campus cyberdéfense d'Armasuisse – et nous serons encore meilleurs à l'avenir. Mais on peut retourner le problème comme on veut, les chiffres d'ICT Formation professionnelle sont clairs: à l'horizon 2026, il manquera au marché du travail suisse près de 20 % des spécialistes en informatique. Ceci étant, disposer d'un personnel compétent est certes crucial, mais ce n'est de loin pas le seul critère. Il nous faut une approche globale.

Du point de vue suisse, comment les concepts de sécurité de l'armée et de cyberdéfense des deux pays se différencient-ils?

G. Vernez: Les points de différence sont nombreux, à commencer par le fait que la Suisse et son armée n'ont pas à faire face à une transformation profonde comme l'affrontent les anciens Etats soviétiques. Malgré tous nos défis, nous vivons dans une situation beaucoup plus linéaire et calme. La Suisse est certes aussi exposée à des cyberattaques disruptives pouvant affecter ses infrastructures vitales, mais elle vit en paix. Actuellement, son armée remplit des missions d'aide, mais elle ne combat pas. Ensuite, notre État fédéral est fortement décentralisé. La culture, la politique, l'éducation, les fondements juridiques… beaucoup de choses sont différentes.

La compagnie d'électricité régionale ukrainienne Kyivoblenergo a été l'un des premiers opérateurs de réseau électrique à être paralysé par une cyberattaque en 2015. L'Ukraine doit-elle souvent faire face à des attaques aussi dévastatrices?

A. Rybchenko: Kyivoblenergo est l'un de nos principaux fournisseurs d'électricité. L'attaque que vous mentionnez était l'une des plus importantes. Comme indiqué précédemment, nos infrastructures critiques nationales sont constamment exposées à de telles attaques. Bien sûr, une telle attaque provoque toujours beaucoup d'anxiété et comporte le risque de perdre beaucoup de données. Les événements de cette ampleur sont toujours très désagréables, mais heureusement ils ne sont pas la norme.

Un tel scénario pourrait-il également se dérouler en Suisse?

G. Vernez: Selon le dernier rapport du Service de renseignement de la Confédération, les rivalités interétatiques sont plus fortes qu'elles ne l'ont été depuis longtemps. Cependant, pour que les États passent à des attaques vraiment disruptives, il doit y avoir une situation conflictuelle évidente. Un cybersabotage parrainé par un État, cela ne tombe pas du ciel. Fort heureusement, la Suisse ne se trouve actuellement pas dans cette situation, mais cela n'empêchera pas un attaquant de pénétrer aujourd'hui dans nos systèmes pour être en mesure de frapper le jour J. La cyberattaque contre SolarWinds aux États-Unis a par exemple montré qu'une fois qu'un attaquant a pénétré les systèmes, il peut rester caché longtemps, puis passer rapidement à une phase de sabotage. La récente attaque contre le Colonial Pipeline sur la côte Est des États-Unis a quant à elle montré que pour extorquer de l'argent, certains groupes n'hésitent plus à s'attaquer directement aux infrastructures vitales. Même les systèmes de santé sont régulièrement pris pour cible. La Suisse n'est pas plus protégée que les autres pays, notre neutralité n'est pas un bouclier. Au contraire, notre pays est une cible lucrative pour le modèle économique des criminels. Et je rappelle que nos infrastructures électriques ont récemment été sévèrement montrées du doigt par l'Office fédéral de l'énergie pour leur niveau misérable de cybersécurité.

Dans quels domaines les deux pays (Suisse et Ukraine) souhaitent-ils intensifier leur coopération?

G. Vernez: Je laisse aux gouvernements le soin de définir leurs stratégies de coopération. La cybersécurité est un jeu d'équipe et comme au football, il faut contrôler l'ensemble du terrain. Il faut donc organiser l'ensemble de la chaîne de cybersécurité. Chaque maillon est important, du fournisseur à l'utilisateur, en passant par le régulateur et l'opérateur. Je crains néanmoins que dans l'actuelle course aux cyberarmements entre attaquants et défenseurs, les premiers fassent la course en tête. Les chiffres sont éloquents. Pour moi, nous avons besoin d'un nouveau modèle digital, car sur le long terme, l'actuel n'est pas défendable. Il faut innover au niveau stratégique. Une grande ambition? Oui, mais la voie actuelle est une impasse si l'on prend en compte tous les paramètres.

«En matière de cybersécurité, la coopération est une clé du succès.»

Gérald Vernez

Quelle serait la bonne approche?

G. Vernez: La question essentielle est de savoir ce dont nous avons réellement besoin pour assurer la prospérité de la Suisse, et non ce que les vendeurs de matériel veulent nous vendre. Nous devrions faire œuvre de sagesse et de sobriété, mais nous en sommes loin. Nous devons aussi identifier clairement nos intérêts et définir ce qui doit être atteint et protégé à tout prix. Nos dépendances sont flagrantes, elles vont devenir insupportables. Ce sont là des questions de souveraineté. Y répondre nécessite de considérer tous les facteurs pertinents et pas seulement la technologie et les pirates. Nous avons besoin d'une approche holistique et systémique et de partenariats avec tous ceux qui partagent nos valeurs. Je pense que la Suisse devra prendre des décisions compliquées.

A. Rybchenko: La Suisse est l'un des quatre premiers investisseurs en Ukraine. Nous parlons chaque deux ans de nos relations diplomatiques. Il existe également une commission économique helvético-ukrainienne. Cette année, nous célébrerons également les 30 ans de notre indépendance. La Suisse a également été l'un des premiers pays à reconnaître notre indépendance. Davos est également important pour nous. L'année dernière, nos présidents s'y sont réunis et ce fut une bonne réunion de lancement pour les années à venir. Il y aura également une réunion à Lugano cette année sur la situation économique après la pandémie. Je pense que si nous pouvons signer une sorte de mémorandum dans le domaine de la cybersécurité, ce sera une très bonne base pour la coopération future.

Quelle est la dernière attaque qui vous a vraiment inquiété?

A. Rybchenko: C'est chaque année plus difficile. Ces dernières années, la majorité des attaques contre les infrastructures ont été plus intenses que dans n'importe quel autre pays européen. Lorsqu'une attaque est dirigée contre plusieurs institutions, vous ne savez jamais comment elle va évoluer. Pendant la pandémie, nous avons souvent eu des échanges avec des entreprises de la fintech. Tout ce qui est en ligne peut être attaqué. Le problème c'est que le côté criminel est souvent plus rapide que le bon côté.

G. Vernez: La guerre traditionnelle poursuit un objectif clé: la destruction de l'adversaire! Mais si vous paralysez son infrastructure, vous n'avez plus besoin de troupes ou de bombes. Si nous n'avons plus d'électricité, c'est tout le système sociétal qui est affecté. Que se passera-t-il lorsque les gens auront soudainement faim et froid pendant des jours? Ils commenceront par tout acheter frénétiquement? Et ensuite? Une action repose sur trois moteurs principaux: la connaissance de l'endroit à attaquer, les moyens pour le faire et la volonté pour passer à l'attaque. Ce qui m'inquiète, ce sont les futures cyberattaques, car sur ces trois facteurs, le seul qui est encore un peu bridé, c'est celui de la volonté. Mais il y a déjà un conflit en cours dans le cyberespace; il se déroule sous le seuil de la guerre. ■