



Les CyberPatrouilleurs

Basé sur une idée originale de la fondation **digiVolution** et de l'ILCE, le concept des CyberPatrouilleurs a fait l'objet en 2022 d'une étude de faisabilité commandée par le *National Cyber Security Center NCSC* (aujourd'hui *Office fédéral de la cybersécurité - OFCS*). Les CyberPatrouilleurs sont désormais reconnus comme partie de la mise en œuvre de la *Cyberstratégie nationale CSN*. Leur marraine, la Conseillère nationale Jacqueline de Quattro, vice-présidente de la Commission de politique de sécurité, a interpellé¹ en 2024 le Conseil fédéral qui a confirmé que le projet s'inscrivait dans le dispositif de cybersécurité de la Confédération et l'OFCS a également reconnu à **digiVolution** la paternité du projet. **Il lui incombe désormais de trouver les moyens financiers et de le réaliser.**

Motivation et défi

Les activités humaines sont entièrement dépendantes des TIC et des multiples services qu'elles délivrent. Un retour à un monde non numérique est impossible et c'est pourquoi, chez **digiVolution**, nous parlons de **mutation**. Comme en biologie, l'évolution est en effet irréversible. La complexité des TIC et leur rapide évolution mettent les organisations et leurs dirigeants dans une situation permanente de stress. Plus personne n'est à l'abri d'actes cybermalveillants, d'incidents nés de négligences ou de l'impréparation de personnes souvent dépassées par l'évolution technologique. Les cas de fraude, de vols de données, de rançonnage, de sabotage, etc. croissent d'année en année. Selon le Rapport Hiscox 2023, 53 % des entreprises interrogées ont déclaré avoir subi une cyberattaque en 2022, contre 48 % l'année précédente. En Suisse, le nombre de cas annoncés augmente de près de 20% chaque année depuis 2020. Les dégâts qui en découlent, jusqu'à la faillite de certaines entreprises, coûtent chaque année plus cher. Sur la base de l'analyse du Bitkom en Allemagne, on peut estimer les pertes subies par la Suisse du fait des cyberrisques à près de 4% de son PIB. Près de 30 milliards CHF ! Et personne ne chiffre la perte de souveraineté de l'individu jusqu'à l'État, du fait de la domination sans partage des géants de la tech et de leurs écosystèmes dont nous sommes toujours plus captifs ?

Comment donc faire passer durablement le message à plus de 620'000 entreprises (dont 90% de TPE/TPI), près de 2'150 communes (dont 50% ont moins de 10'000 habitants), 80'000 à 100'000 associations, 1.67 million d'enfants et de jeunes en formation et 9 millions de citoyens et 1 million d'expatriés? **Avec un moyen massif de diffusion qui s'adresse personnellement à chaque entité** (État / commune, organisation, entreprise, individu) et lui permet de **comprendre sa part de**

¹ <https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaefft?AffairId=20243891>



responsabilité et de l'assumer. Un moyen qui vient compléter toutes les autres initiatives d'éducation et de résilience.

Mission

Le **profil des CyberPatrouilleurs** est large. Ce ne sont pas des informaticiens. Leur mission est de parler aux gens, de les interpeller, de les orienter et conseiller, d'expliquer les enjeux, développer les connaissances du public sur nos institutions (civisme), de lutter contre le harcèlement, etc... non de régler les problèmes techniques² des gens. Ce sont des personnes avec une forte envie de s'engager et de servir autrui et qui possèdent des compétences élevées d'apprentissage et de communication.

Nous leur avons attribué cinq missions :

- **Responsabiliser** – La cybersécurité est une affaire personnelle... au service de tous. Au temps de la mutation numérique, chacun (individu, organisation, entreprise) doit – à son niveau déjà – comprendre les enjeux et contribuer à la sécurité de tous. Être responsable, c'est accomplir sa part.
- **Soutenir** – Les CyberPatrouilleurs vont écouter, comprendre, conseiller et apporter à nos concitoyens et aux entreprises des moyens simples afin que chacun – même modestement – s'engage sur le chemin vertueux de la sécurité numérique. Nous comprenons tous les règles de base de la circulation routière ou de l'hygiène médicale ? Alors faisons de même face aux risques de la mutation numérique.
- **Recruter** – Les métiers liés aux technologies de l'information et de la communication (TIC) manquent de talents. La pénurie s'aggrave d'année en année avec des conséquences croissantes pour les entreprises, notamment en matière de dépendance face aux géants de la tech et de leurs écosystèmes. Les CyberPatrouilleurs (hommes / femmes, jeunes / senior) contribueront à créer de la compétence et à promouvoir les métiers dans le secteur des TIC. Une fois formés, ils feront également bénéficier leurs entreprises et institutions de leurs compétences nouvellement acquises, leur conférant ainsi un avantage compétitif.
- **Observer** – La cybersécurité est un domaine dynamique qui nécessite un effort continu de mise à jour. Selon le département US de justice et de fedpol, seuls 15% des incidents sont portés à la connaissance des autorités. En rassemblant et en partageant leurs observations et expériences avec les autorités et les professionnels du domaine, les CyberPatrouilleurs apporteront une contribution essentielle à



Une CyberPatrouille (1) à l'engagement dans une ville suisse (illustration produite avec Bing)

² Pour de multiples raisons pratiques et légales, cela leur est même interdit.



l'amélioration continue de la cybersécurité des Suisses. C'est en parlant avec les gens sur le terrain que nous aurons les résultats les plus fiables pour ensuite orienter notre sécurité et notre défense.

- **Durabilité** – Les activités numériques sont un important consommateur de ressources. L'IA et le streaming font exploser les besoins. TIC ne signifie pas « virtuel », car au bout il y a des usines bien réelles et une consommation énergétique qui explose et provoque près de 4% des émissions mondiales de CO₂. Et ajoutons les besoins en métaux rares qui constituent un type de déchet difficilement valorisable et générant une pollution non maîtrisée. Les objectifs du développement durable de l'ONU doivent en conséquence aussi faire partie de la mission des CyberPatrouilleurs.

Création de résilience

Nos infrastructures numériques sont dépendantes de multiples facteurs, dont l'énergie électrique, elle-même fragile. Que se passe-t-il en cas de défaillance ? Un solide socle de résilience est donc impératif, qui passe en premier lieu par la capacité des personnes et des dirigeants à comprendre les enjeux complexes de la sécurité de leur environnement numérique et à investir dans leur résilience.

Avec les CyberPatrouilleurs, *digi*Volution apporte une contribution concrète pour élever le niveau de littératie numérique et de cyberhygiène des Suisses et donc le niveau de résilience du pays. Mais chez nous, l'esprit de milice a régressé ces dernières années, réduisant ainsi la capacité de faire percoler dans la société les notions de sécurité, physique, informationnelle et environnementale également. Il faut de nouveaux vecteurs de milice et les CyberPatrouilleurs seront de ceux-ci. Par leur discours, ils contribueront au renforcement des compétences de la population en matière de sécurité comme le promeut *digi*Volution depuis sa création.



Une CyberPatrouille (2) à l'engagement dans une ville suisse (illustration produite avec Bing)

Réalisation

Le lancement du projet dépend de son **financement**. Cette phase clé est en cours et diverses institutions et entreprises s'y intéressent. Il convient de les conquérir définitivement.

Le **programme de formation certifiante** sera au centre. Il prévoit 120 heures réparties en sept chapitres: bases légales, technologie, cybersécurité, cyberhygiène, politique de sécurité et institutions, pédagogie et communication et une **partie pratique**. La formation comprendra en outre un engagement de durée équivalente sur le terrain. La



formation s'appuiera notamment sur plusieurs hautes écoles et une étroite coopération est déjà en place avec l'université de Zürich. Et d'autres institutions sont déjà à bord, notamment la HES Arc de Neuchâtel et la HEG à Genève.

La **mise en œuvre du projet devrait débiter par 3 projets pilotes** qui permettront d'acquérir l'expérience qui servira ensuite à l'extension du projet à tout le pays. Chacun de ces projets aura un public cible particulier : la société, les entreprises et les écoles.

Le projet **d'innovation sociétale VERD³** est aussi en cours de déploiement à l'échelle nationale. Il s'agit d'un système de paiement profitant aux consommateurs, aux commerces et, par ricochet, aux collectivités publiques. Les CyberPatrouilleurs seront l'un des services rattachés au sous-projet **TRÄF** de VERD.

Divers projets (dont eLearningCyber⁴) et stratégies cantonales confiées à **dVCyberGroup**, *bras armé de **digi**Volution*, prévoient d'engager les CyberPatrouilleurs en tant que vecteur de renforcement de la littératie numérique des Suisses.

L'équipe de projet est en cours de constitution. 2026 verra donc enfin le décollage des CyberPatrouilleurs. Avec ce projet et le soutien d'un important réseau de personnes, d'organisations et d'institutions conscientes des défis d'une mutation numérique dynamique, **digi**Volution offrira à la Suisse une carte maîtresse pour maîtriser les défis de la mutation numérique. Et le projet pourra aussi être étendu à d'autres pays...!



³ <https://www.verd.swiss/fr>

⁴ <https://elearningcyber.ch/fr> - une initiative de la Conférence des directrices et directeurs des départements cantonaux de justice et police (CCDJP)