

Die CyberPatrouilleurs

Das auf einer ursprünglichen Idee der Stiftung **digiVolution** und des ILCE basierende Konzept der CyberPatrouilleurs war 2022 Gegenstand einer Machbarkeitsstudie, die vom *National Cyber Security Center* NCSC (heute *Bundesamt für Cybersicherheit - BACS*) in Auftrag gegeben wurde. Die CyberPatrouilleurs sind nun als Teil der Umsetzung der *nationalen Cyberstrategie* CSN anerkannt. Ihre Patin, Nationalrätin Jacqueline de Quattro, Vizepräsidentin der Sicherheitspolitischen Kommission, wandte sich 2024 an¹ den Bundesrat, der bestätigte, dass das Projekt Teil des Cybersicherheitsdispositivs des Bundes ist, und das BACS erkannte **digiVolution** ebenfalls die Urheberschaft des Projekts zu. **Es liegt nun an ihr, die finanziellen Mittel zu beschaffen und das Projekt umzusetzen.**

Motivation und Herausforderung

Die menschlichen Aktivitäten sind vollständig von IKT und den vielfältigen Dienstleistungen, die sie erbringen, abhängig. Eine Rückkehr zu einer nicht-digitalen Welt ist unmöglich, und deshalb sprechen wir bei **digiVolution** von **Mutation**. Wie in der Biologie ist die Evolution in der Tat unumkehrbar. Die Komplexität der IKT und ihre schnelle Entwicklung versetzen Organisationen und ihre Führungskräfte in eine permanente Stresssituation. Niemand ist mehr vor Cyber-Malware, Vorfällen, die durch Nachlässigkeit oder die Unvorbereitetheit von Personen entstehen, die mit der technologischen Entwicklung oft überfordert sind, sicher. Die Zahl der Fälle von Betrug, Datendiebstahl, Lösegeld, Sabotage usw. nimmt von Jahr zu Jahr zu. Laut dem Hiscox Report 2023 gaben 53 % der befragten Unternehmen an, im Jahr 2022 einen Cyberangriff erlitten zu haben, gegenüber 48 % im Vorjahr. In der Schweiz steigt die Zahl der gemeldeten Fälle seit 2020 jedes Jahr um fast 20 %. Die daraus resultierenden Schäden bis hin zum Konkurs einiger Unternehmen kosten jedes Jahr mehr Geld. Auf der Grundlage der Analyse des Bitkom in Deutschland kann man die Verluste, die der Schweiz durch Cyberrisiken entstehen, auf fast 4% des BIP schätzen. Fast 30 Milliarden CHF! Und niemand beziffert den Verlust der Souveränität vom Einzelnen bis zum Staat aufgrund der ungeteilten Herrschaft der Tech-Giganten und ihrer Ökosysteme, von denen wir immer mehr gefangen genommen werden?

Wie kann man die Botschaft nachhaltig an mehr als 620'000 Unternehmen (davon 90% Kleinunternehmen), ca. 2'150 Gemeinden (davon 50% mit weniger als 10'000 Einwohnern), 80'000 bis 100'000 Vereine, 1,67 Millionen Kinder und Jugendliche in Ausbildung und 9 Millionen Bürgerinnen und Bürger und 1 Million Auslandschweizer weitergeben?

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



Mit einem massiven Verbreitungsmedium, das jede Einrichtung (Staat/Gemeinde, Organisation, Unternehmen, Einzelperson) **persönlich anspricht** und es ihr ermöglicht, **ihren Teil der Verantwortung zu verstehen und zu übernehmen**. Ein Medium, das alle anderen Initiativen für Bildung und Resilienz ergänzt.

Auftrag

Das **Profil der CyberPatrouilleurs** ist breit gefächert. Sie sind keine Computerfachleute. Ihre Aufgabe ist es, mit den Menschen zu sprechen, sie anzusprechen, ihnen Orientierung und Rat zu geben, die Herausforderungen zu erklären, das Wissen der Öffentlichkeit über unsere Institutionen zu erweitern (Bürgersinn), gegen Belästigungen vorzugehen usw., nicht die technischen Probleme² der Leute zu lösen. Sie sind Menschen mit einem starken Wunsch, sich zu engagieren und anderen zu dienen, und verfügen über hohe Lern- und Kommunikationsfähigkeiten.

Wir haben ihnen fünf Aufgaben zugewiesen:

- **Befähigung** - Cybersicherheit ist eine persönliche Angelegenheit ... im Dienste aller. In Zeiten der digitalen Mutation muss jeder (Einzelperson, Organisation, Unternehmen) - bereits auf seiner Ebene - die Herausforderungen verstehen und zur Sicherheit aller beitragen. Verantwortlich zu sein bedeutet, seinen Teil zu erfüllen.
- **Unterstützen** - Die CyberPatrouilleurs werden zuhören, verstehen, beraten und unseren Mitbürgern und Unternehmen einfache Mittel an die Hand geben, damit jeder - auch in bescheidenem Umfang - den tugendhaften Weg der digitalen Sicherheit beschreitet. Wir alle verstehen die Grundregeln des Strassenverkehrs oder der medizinischen Hygiene? Dann sollten wir das auch für die Risiken der digitalen Mutation tun.
- **Anwerben** - Den Berufen im Bereich der Informations- und Kommunikationstechnologie (IKT) mangelt es an Talenten. Der Mangel verschärft sich von Jahr zu Jahr mit zunehmenden Folgen für die Unternehmen, insbesondere in Bezug auf die Abhängigkeit von Tech-Giganten und ihren Ökosystemen. Die CyberPatrouilleurs (Männer / Frauen, Junge / Senioren) werden dazu beitragen, Kompetenzen zu schaffen und Berufe im IKT-Sektor zu fördern. Sobald sie ausgebildet



CyberPatrouilleurs (1) im Einsatz in einer Schweizer Stadt (Abb. mit Bing erstellt).

² Aus vielen praktischen und rechtlichen Gründen ist ihnen dies sogar untersagt.



sind, werden sie ihre neu erworbenen Fähigkeiten auch an ihre Unternehmen und Institutionen weitergeben und ihnen so einen Wettbewerbsvorteil verschaffen.

- **Beobachten** - Cybersicherheit ist ein dynamischer Bereich, der ständige Anstrengungen erfordert, um auf dem neuesten Stand zu bleiben. Laut dem US-Justizministerium und fedpol werden nur 15% der Vorfälle den Behörden zur Kenntnis gebracht. Indem sie ihre Beobachtungen und Erfahrungen sammeln und mit Behörden und Fachleuten auf diesem Gebiet teilen, werden die CyberPatrouilleurs einen wesentlichen Beitrag zur kontinuierlichen Verbesserung der Cybersicherheit der Schweizerinnen und Schweizer leisten. Indem wir mit den Menschen vor Ort sprechen, werden wir die zuverlässigsten Ergebnisse erhalten, an denen wir dann unsere Sicherheit und Verteidigung ausrichten können.
- **Nachhaltigkeit** - Digitale Aktivitäten sind ein grosser Ressourcenverbraucher. KI und Streaming lassen den Bedarf explodieren. IKT bedeutet nicht "virtuell", denn am Ende stehen ganz reale Werke und ein Energieverbrauch, der explodiert und fast 4% der weltweiten CO₂-Emissionen verursacht. Und hinzu kommt der Bedarf an seltene Erde, die eine schwer verwertbare Abfallart darstellen und eine unkontrollierte Umweltverschmutzung verursachen. Die Ziele der Vereinten Nationen für nachhaltige Entwicklung müssen folglich auch Teil der Mission der CyberPatrouilleurs sein.

Schaffung von Resilienz

Unsere digitale Infrastruktur ist von einer Vielzahl von Faktoren abhängig, darunter auch von Strom, der ihrerseits anfällig ist. Was passiert im Falle eines Ausfalls? Ein solides Fundament an Resilienz ist daher zwingend erforderlich, das in erster Linie die Fähigkeit der Menschen und Führungskräfte voraussetzt, die komplexen Herausforderungen für die Sicherheit ihrer digitalen Umgebung zu verstehen und in ihre Resilienz zu investieren.

Mit den CyberPatrouilleurs leistet **dig**iVolution einen konkreten Beitrag zur Erhöhung der digitalen Kompetenz und der Cyberhygiene der Schweizerinnen und Schweizer und damit zur Stärkung der Resilienz des Landes. Aber bei uns ist der Milizgeist in den letzten Jahren zurückgegangen, was die Fähigkeit verringert hat, das Konzept der Sicherheit - physisch, informationell und auch umweltbezogen - in der Gesellschaft zu verankern. Wir brauchen neue Träger der Miliz, und die CyberPatrouilleurs werden diese Träger sein. Durch ihren Diskurs werden sie zur Stärkung der Sicherheitskompetenz der Bevölkerung beitragen, wie es **dig**iVolution seit seiner Gründung fördert.



Ein CyberPatrol (2) beim Einsatz in einer Schweizer Stadt (Abbildung mit Bing erstellt).



Umsetzung

Der Start des Projekts hängt von seiner **Finanzierung** ab. Diese Schlüsselphase ist im Gange und verschiedene Institutionen und Unternehmen interessieren sich für das Projekt. Diese gilt es nun endgültig zu gewinnen.

Im Zentrum wird das **zertifizierende Ausbildungsprogramm** stehen. Es umfasst 120 Stunden, die in sieben Kapitel unterteilt sind: Rechtsgrundlagen, Technologie, Cybersicherheit, Cyberhygiene, Sicherheitspolitik und Institutionen, Pädagogik und Kommunikation sowie ein **praktischer Teil**. Die Ausbildung beinhaltet zudem einen gleich langen Einsatz im Feld. Die Ausbildung wird sich insbesondere auf mehrere Hochschulen stützen, wobei bereits eine enge Zusammenarbeit mit der Universität Zürich besteht. Und auch andere Institutionen sind bereits an Bord, darunter die HES Arc in Neuenburg und die HEG in Genf.

Die **Umsetzung des Projekts soll mit drei Pilotprojekten beginnen**, in denen Erfahrungen gesammelt werden, die später für die Ausweitung des Projekts auf das ganze Land genutzt werden können. Jedes dieser Projekte wird eine bestimmte Zielgruppe haben: die Gesellschaft, Unternehmen und Schulen.

Das **gesellschaftliche Innovationsprojekt VERD³** wird ebenfalls landesweit eingeführt. Dabei handelt es sich um ein Zahlungssystem, das Verbrauchern, Geschäften und in weiterer Folge auch der öffentlichen Hand zugutekommt. Die CyberPatrouilleurs werden eine der Dienstleistungen sein, die dem Unterprojekt **TRÄF** von VERD zugeordnet sind.

Verschiedene Projekte (darunter eLearningCyber⁴) und kantonale Strategien, die der **dV**CyberGroup, dem *bewaffneten Arm* von **digi**Volution, anvertraut wurden, sehen den Einsatz von CyberPatrouilleurs als Mittel zur Stärkung der digitalen Kompetenz der Schweizerinnen und Schweizer vor.

³ <https://www.verd.swiss/fr>

⁴ <https://elearningcyber.ch/fr> - eine Initiative der Konferenz der kantonalen Justiz- und Polizeidirektorinnen und -direktoren (KKJPD)



Das Projektteam wird derzeit zusammengestellt. 2026 wird also endlich der Start der CyberPatrouilleurs erfolgen. Mit diesem Projekt und der Unterstützung eines grossen Netzwerks von Personen, Organisationen und Institutionen, die sich der Herausforderungen einer dynamischen digitalen Mutation bewusst sind, wird *digi*Volution der Schweiz eine Trumpfkarte in die Hand geben, um die Herausforderungen der digitalen Mutation zu meistern. Und das Projekt kann auch auf andere Länder ausgeweitet werden...!

