

# AF&E UND WEITERBILDUNG ZWEI WICHTIGE PFEILER DES ILCE IM DIENST DER POLIZEIAUSBILDUNG

November 2021

Sébastien Jaquier

## Inhalt

### Ausbildung

- Verbindung zur NCS
- Digitale Ausbildungsstrategie der Polizei
- Grundausbildung und
- Ausbildungen für Spezialisten/-innen

### Forschungsprojekte

- Grafiken
- Übereinstimmungspunkte und Perspektiven

## Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken 2018–2022

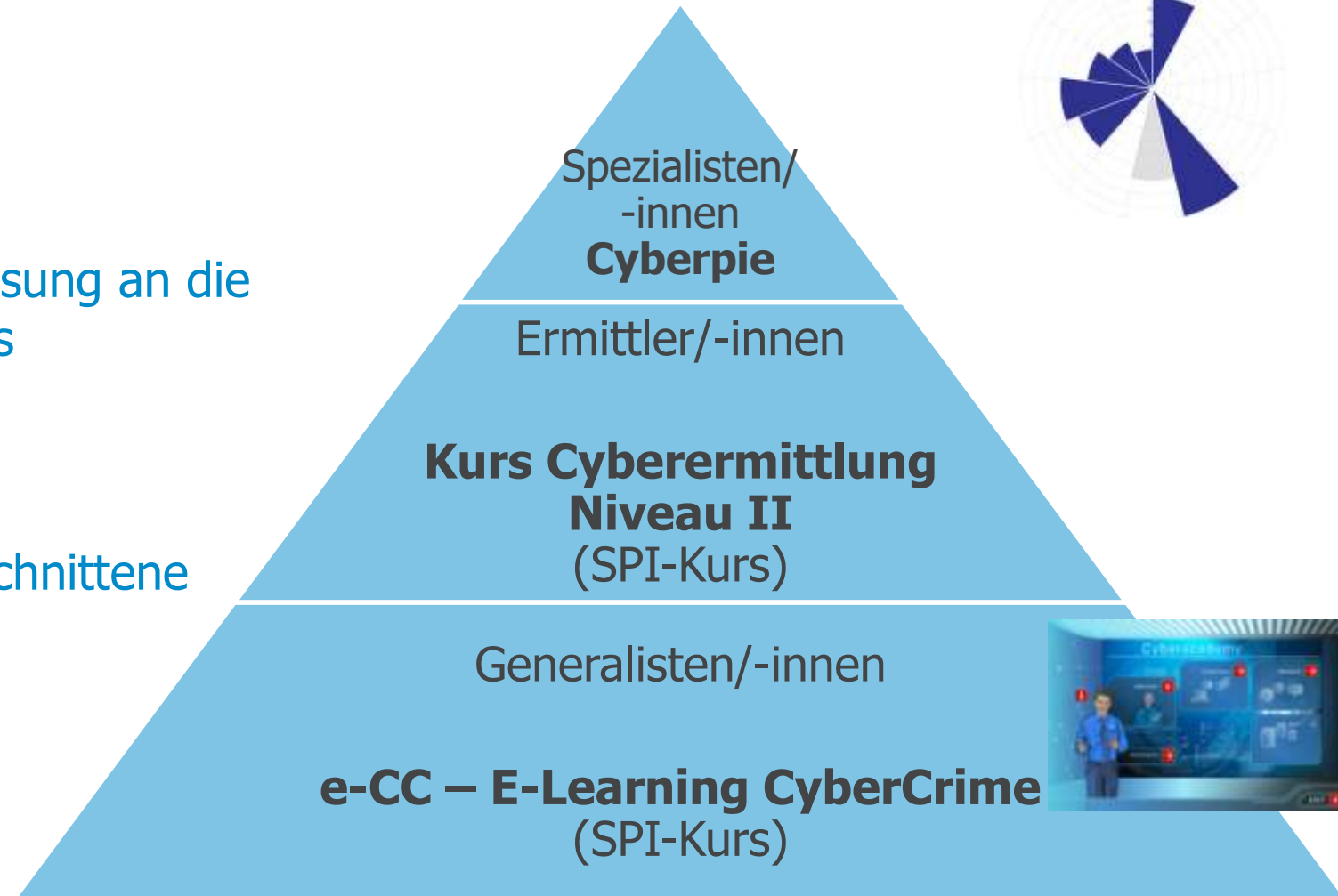
- 10 Handlungsfelder, 29 Massnahmen
- Handlungsfeld: **Strafverfolgung**
  - 18. Cyberkriminalität – eine Bestandsaufnahme
  - 19. Netzwerk zur Unterstützung von Untersuchungen im Bereich Cyberkriminalität
  - 20. Ausbildung in der Bekämpfung von Cyberkriminalität
  - 21. Zentralstelle zur Bekämpfung von Cyberkriminalität
- **Ausbildungskonzept der Polizei im Bereich «Cyber» mit :**
  - e-CC
  - Ausbildung für Ermittlerinnen und Ermittler
  - Bewertungsraster der Ausbildungen für Spezialisten/-innen



# Digitale Ausbildungsstrategie der Polizei

## Grundsätze

- Kompetenzhierarchie
- Kontinuierliche Anpassung an die Bedürfnisse der Praxis
- Modularisierung
- Auf Zielgruppe zugeschnittene Ausbildung





## MES E-LEARNINGS



### E-learning *Cybercrime* (e-CC)

L'e-learning *Cybercrime* a été conçu par l'ISP sur mandat de la CCPCS. Il vous permettra d'acquérir les fondamentaux afin de mener une lutte efficace contre la cybercriminalité, que ce soit dans la prévention ou la répression. Il comporte deux modules et s'adresse à tous les membres des corps de police suisses. Bienvenue à la « Cyberacademy » !

### ATTENTION

Veuillez s'il vous plaît utiliser une des deux dernières versions des navigateurs Internet suivants : Google Chrome, Mozilla Firefox, Internet Explorer 11, Microsoft Edge, Safari.

Lorsque vous interrompez (même pour quelques minutes) votre progression dans le e-CC, IL EST IMPÉRATIF de cliquer sur le bouton EXIT afin de sauvegarder ce que vous avez fait.

Merci de votre compréhension

e-learning Cybercrime_d - Modul 1	Ouvert
e-learning Cybercrime_d - Modul 2	Ouvert
e-learning Cybercrime_f - Module 1	Réussi
e-learning Cybercrime_f - Module 2	Ouvert
e-learning Cybercrime_i - Modulo 1	Ouvert
e-learning Cybercrime_i - Modulo 2	Ouvert

**Max Sieber** begleitet die Teilnehmenden während der ganzen Ausbildung. Er stellt das Tool kurz vor und gibt einige Ratschläge.

**Warum** diese Ausbildung?  
Einige Hintergrundinformationen erklären die **Entwicklung und die Bedeutung von Cyberkriminalität** und die **Polizistinnen**

Das **Klassenzimmer**: Folgende Themen werden didaktisch behandelt:

- Cybercrime-Phänomene

**Test:** Der Test kann erst gemacht werden, wenn alle Aufgaben gelöst sind. Werden 80 % der Aufgaben richtig beantwortet, gilt der Test als bestanden.

Jedes Modul wird mit einem Test abgeschlossen.

Der Test ist nicht summativ und kann bei Nichtbestehen wiederholt werden.

**Aufgaben:** Sie haben zum Ziel, die Polizisten/-innen in eine Situation zu versetzen. Dazu wurden folgende Szenen entwickelt:

- Cybercrime-Phänomene (mehrere Situationen)
- Sachbeschädigung (Spreiereien in einer Schule...)
- Hausdurchsuchung (bei einer der Spreiereien verdächtigten Person)
- Sicherung der Spuren eines Mobiltelefons
- Drohungen / Beleidigungen (E-Mail)
- Handy-Diebstahl
- Hausdurchsuchung – verfahrenstechnische Aspekte

# Ausbildung für Ermittlerinnen und Ermittler

1re journée	2e journée	3e journée	4e journée	5e journée
30' <b>Accueil et introduction</b>	60' <b>La sécurité sur internet</b> BE	180' <b>Traces numériques</b> Sur la base de : <b>Exploitation des données informatiques (FJR)</b>	15' <b>Accueil / introduction</b>	30' <b>Droit de procédure pénale : Investigation secrète et recherches secrètes</b> (y.c. délimitation par rapport au droit policier) VD
15' <b>Travailler avec les moyens didactiques électroniques</b> VD + ILCE	60' <b>Exercice mobilité IP, e-mails frauduleux, NAT/PAT</b> fedpol		105' <b>Étude de cas (type « RentoPlus »)</b>	
60' <b>Systèmes d'exploitation et réseaux informatiques</b> BE	<p style="text-align: center; color: blue; font-weight: bold;">Kurs wird hauptsächlich von Polizisten/-innen geleitet</p> <p style="text-align: center; color: blue; font-weight: bold;">Kontinuierliche Anpassungen</p> <p style="text-align: center; color: blue; font-weight: bold;">Koordination auf nationaler Ebene</p>		60' <b>Historique de navigation et cookies</b> NE	150' <b>OSINF</b> EXT
60' <b>Phénomènes Cyber</b>			60' <b>Télécommunications : technologies et moyens de communication</b> fedpol	Pause de midi
3 x 60' <b>3 blocs d'apprentissage pratique :</b> (s'appuyant sur l'e-CC) - <b>Perquisition IT OSINF</b> Introduction à la recherche en ligne (réseau = données non structurées, les résultats varient selon le lieu d'où se fait la recherche etc.) - <b>Phénomènes Cyber</b> BE JU VD	<p style="text-align: center;">Présentation et entraînement des enquêteurs et spécialistes sur la base d'un exemple de cas</p> <p style="text-align: right;">FR</p>		180' <b>Forensique téléphonie mobile</b> Sur la base de : <b>Exploitation des données d'appareils mobiles (FJR)</b> GE	60' <b>Darknet</b> EXT
		90' <b>Les cryptomonnaies et leur Saisie</b> GE	Pause de midi	
	90' <b>Demande de préservation et collaboration avec les fournisseurs d'accès internet</b> fedpol	60' <b>Étude de cas</b> GE	105' <b>Étude de cas sur l'ensemble de la matière</b> NE VD	
			15' <b>Clôture du cours</b> VD + ILCE	

## Cyberpie – Grundsatz

Baut auf der Kompetenzmatrix auf, welche 13 Bereiche abdeckt

- Mobilfunkforensik
- Computer- und Datenträgerforensik
- Einführung in das Fachgebiet
- Netzwerkforensik
- Fernmeldeüberwachung
- Abklärungen im Internet und in öffentlichen Datenbanken («Open-Source-Recherchen»)
- Fachgebiete
- Analyse
- Informationssicherheit (intern)
- Anwendbares Recht
- Leistungsempfänger/-innen / Partner/-innen
- Informationssicherheit / Datenschutz / Prävention (extern)
- Einsatz Cyberereignis

In jedem Bereich werden in fünf Profilen – davon in drei Spezialprofilen –, die zu erwerbenden Kompetenzen erlangt.

- IT-Ermittlung
- IT-Forensik
- Cybercrime-Analyse

## Cyberpie – Ziele

- *Ausbildungsverantwortliche und Führung: klare Orientierungs- und Entscheidungsbasis*
- *Auszubildendes Personal: Schlüssige Gesamtübersicht über das Ausbildungsangebot*
- *Ausgebildetes Personal: Qualifikation aus der abgeschlossenen Ausbildung*
- *Institute und Schulen: Plattform, um ihr Angebot zu präsentieren*

# Cyberpie – Umsetzung

## CYBERPIE

Formations pour les policiers

Rechercher  IT-Enquête Trier par pertinence  Graph participant-e-s

**Fachkurs Cybercrime**  
Jours de cours : 2  
Jours de pratique : 1

Hacking, Cracking und Malware im Cybercrime-Umfeld

**CAS CY-E, CAS Cybercriminalité option Cyberenquête**  
Jours de cours : 20  
Jours de pratique : 5

Le CAS Cybercriminalité option cyberenquête (CAS CY-E) vise à former les spécialistes des autorités de poursuite pénale (enquêteurs, analystes, procureurs) en matière de lutte contre la criminalité informatique en leur fournissant les outils pertinents pour des enquêtes ayant une composante cyber.

**Investigation et veille sur Internet**  
Jours de cours : 5  
Jours de pratique : 3

Comprendre la nature, le potentiel et les limitations des traces internetiques, saisir les enjeux liés à la qualité des données collectées en ligne, ainsi qu'adopter une démarche forensique pour collecter des données en ligne et assurer la continuité de la preuve numérique

CAS CY-E, CAS Cybercriminalité option Cyberenquête

Topic	Points
Introduction au domaine spécialisé	7
Analyse forensique des ordinateurs et supports de données	0
Analyse forensique de la téléphonie mobile	0
Analyse forensique de réseaux	0
Surveillance des télécommunications	0
Recherches sur internet et Les bases de données publiques (« recherches open source »)	10
Domaines spécialisés	3
Analyse	0
Sécurité informatique (interne)	0
Droit applicable	0
Bénéficiaire des prestations / partenaires	5
Sécurité informatique / protection des données/prévention (externe)	4
Engagement lié à un incident cybernétique	4

- Introduction au domaine spécialisé **7 POINTS**
- Analyse forensique des ordinateurs et supports de données **0 POINTS**
- Analyse forensique de la téléphonie mobile **0 POINTS**
- Analyse forensique de réseaux **0 POINTS**
- Surveillance des télécommunications **0 POINTS**
- Recherches sur internet et Les bases de données publiques (« recherches open source ») **10 POINTS**
- Domaines spécialisés **3 POINTS**
- Analyse **0 POINTS**
- Sécurité informatique (interne) **0 POINTS**
- Droit applicable **0 POINTS**
- Bénéficiaire des prestations / partenaires **5 POINTS**
- Sécurité informatique / protection des données/prévention (externe) **4 POINTS**
- Engagement lié à un incident cybernétique **4 POINTS**

**FERMER**

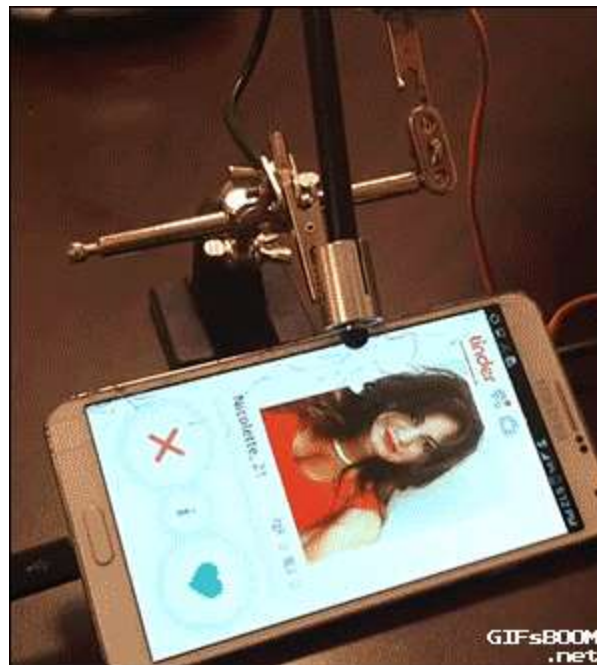
## Projekt «Lovid-19»: *Scambaiting* in der Pandemie

### Das Phänomen genau untersuchen, um:

- die Opfer besser zu verstehen,
- das Vorgehen der Betrüger/-innen zu analysieren,
- neuartige Präventionsmöglichkeiten zu identifizieren,
- Erkenntnisse aus Fachliteratur zu bestätigen oder zu widerlegen.



# Projet «Lovid-19»: *Scambaiting* in der Pandemie



Sarah



Sandra



Christine



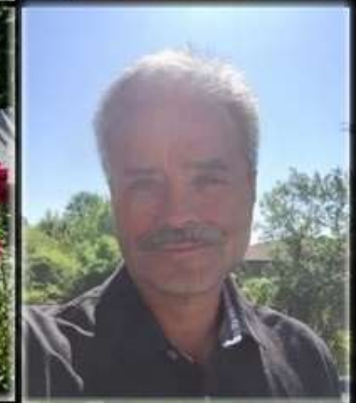
David



Daniel



Martin



## Projekt «Interscam»: Fortsetzung



- Anreiz für *Scambaiting* untersuchen und damit verbunden Wege, um das Phänomen zu unterbinden
- Ethische und juristische Grenzen des *Scambaiting* aus polizeilicher Perspektive untersuchen
- Über die Grundlagen einer IA nachdenken



## Bei Fragen:

Sébastien Jaquier

Doyen de l'ILCE

Tél. direct: +41 79 380 222 7

E-mail: [sebastien.jaquier@he-arc.ch](mailto:sebastien.jaquier@he-arc.ch)

