Repubblica e Cantone Ticino

La cybersecurity in Ticino e in Svizzera

Strategie, visione e collaborazioni tra pubblico e privato

Lugano, 6 ottobre 2020

Repubblica e Cantone Ticino

Repubblica e Cantone Ticino

Introduzione

Alessandro Trivilini
Docente-ricercatore del Dipartimento tecnologie innovative, SUPSI
Membro Gruppo «Cyber sicuro»

Repubblica e Cantone
Ticino

Christian Vitta

Consigliere di Stato e Direttore del Dipartimento delle finanze e dell’economia

La rilevanza dei rischi informatici

Top 10 risks in terms of
Likelihood

1. Extreme weather
2. Climate action failure
3. Natural disasters
4. Biodiversity loss
5. Human-made environmental disasters
6. Data fraud or theft
7. Cyberattacks
8. Water crises
9. Global governance failure
10. Asset bubbles

Fonte: World Economic Forum (2020), *The Global Risks Report 2020*, pag. 3.

Europe

Top ten risks in Europe

1. Cyberattacks
2. Asset bubble
3. Interstate conflict
4. Energy price shock
5. Fiscal crises
6. Data fraud or theft
7. Failure of national governance
8. Unemployment or underemployment
9. Large-scale involuntary migration
10. Profound social instability

Fonte: World Economic Forum (2019), *Regional Risks for Doing Business 2019*, pag. 16.

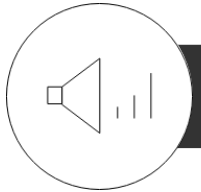
US$ 6’000 miliardi

la stima del **valore dei danni generati dalla cyber-criminalità** che potrebbe essere raggiunta nel 2021.

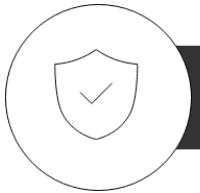
Fonte: World Economic Forum (2020), *The Global Risks Report 2020*, pag. 63.


La digitalizzazione: una sfida globale,
che presenta dei rischi
da trasformare in opportunità.
Rischi informatici
Impatto su cittadini, attività economiche delle aziende e quelle degli attori istituzionali

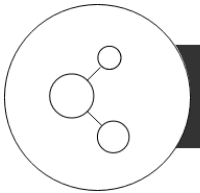
Importante agire, per cogliere le opportunità



Sensibilizzazione e **informazione**



Innovazione e **competitività**



Messa in rete delle competenze


Lo sguardo rivolto al futuro,
per affrontare al meglio la fase di rilancio.

Repubblica e Cantone
Ticino

Norman Gobbi

Presidente del Consiglio di Stato e Direttore del Dipartimento delle istituzioni

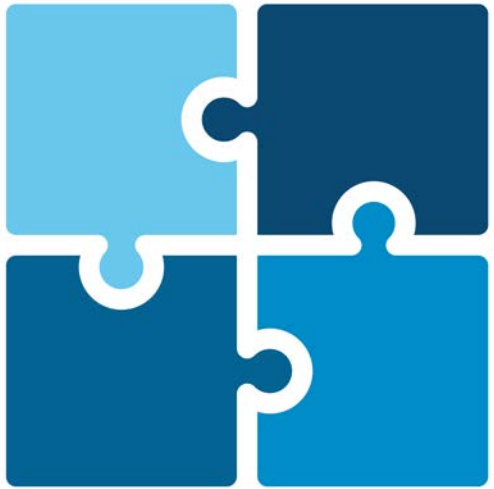
Dipartimento delle istituzioni

Collaborazione interdipartimentale

La digitalizzazione, con le sue opportunità e i suoi rischi, tocca tutti gli ambiti del vivere quotidiano

- Un **lavoro interdipartimentale e interdisciplinare** per un **approccio comune, coordinato e condiviso**

- Il Gruppo di lavoro interdipartimentale “Cyber sicuro” è stato istituito su **proposta del DI e del DFE**



Perché «Cyber sicuro»?

- Le **attività quotidiane** di cittadini, aziende ed enti pubblici sono in gran parte basate su **piattaforme informatiche**
- Gli **attacchi informatici sono sempre più frequenti** e causano gravi danni
- **I reati «classici» si stanno spostando sui canali online**
- Interesse nel creare **prodotti**, **servizi** e … (presunti) **esperti** in sicurezza informatica
- Necessità di un **punto di riferimento cantonale**

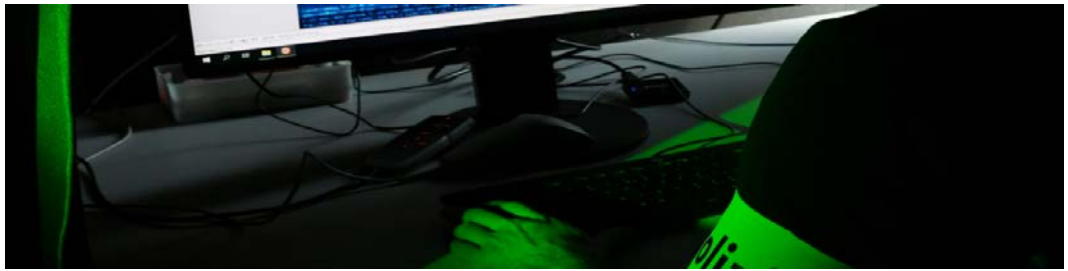
Quarta campagna di prevenzione del DI

Obiettivi e compiti di «Cyber sicuro»

- Essere il **punto di riferimento e di contatto** cantonale per il **Consiglio di Stato, gli enti pubblici, le aziende, la popolazione, le associazioni di categoria e i media**
- **Coordinare l'attività** dei vari attori istituzionali
- **Analizzare i rischi e le minacce** per il nostro territorio
- **Fornire consulenza e supporto al Consiglio di Stato**
- **Elaborare contenuti informativi e di prevenzione**

Obiettivi e compiti di «Cyber sicuro»

- **Fungere da vettore aggregante** in ambito di sicurezza informatica
- **Organizzare eventi istituzionali e attività informative**
- **Sostenere e promuovere iniziative di terzi** di comprovata autorevolezza e valore scientifico



I contatti con la Confederazione

- **Coinvolgimento del Consiglio federale** nella fase di costituzione del Gruppo

- **Scambio di informazioni con le autorità federali**
  - Esercito
  - Fedpol
  - Delegato federale per la cibersicurezza
  - Delegato della Confederazione e dei Cantoni per la Rete integrata svizzera della sicurezza (RSS)
  - Conferenze intercantonali (KKJPD, RK MZF, …)

La cooperazione tra pubblico e privato

Sviluppo di contatti bidirezionali con aziende, professionisti e associazioni di categoria per:

- **Informare su eventuali rischi** in ambito professionale

  Esempio:
  Comunicato stampa sui rischi del telelavoro pubblicato durante la crisi COVID-19

- **Recepire eventuali esigenze** provenienti dalle aziende dalla popolazione
- **Sviluppare attività informative** per professionisti e/o il grande pubblico
- **Mettere in rete le competenze e le conoscenze** pubbliche, private e accademiche

Attività 2020

- Presentazione del portale informativo **www.cybersicuro.ch**

- 23 luglio 2020 Conferenza video
  Come proteggersi dagli attacchi informatici

- 28 maggio 2020 Conferenza video
  Riconoscimento facciale e controllo della distanza sociale post epidemia

La composizione del Gruppo «Cyber sicuro»

- **Luca Filippini**
  Segretario generale del DI
- **Silvano Petrini**
  Direttore Centro sistemi informativi
- **cap Orlando Gnosca**
  Ufficiale Polizia cantonale
- **Daniele Parenti**
  Direttore Centro di risorse didattiche e digitali
- **Alessandro Trivilini**
  Docente-ricercatore Dipartimento tecnologie innovative, SUPSI

Repubblica e Cantone Ticino

Le sfide attuali della cibersicurezza

Florian Schütz

Delegato federale alla cibersicurezza

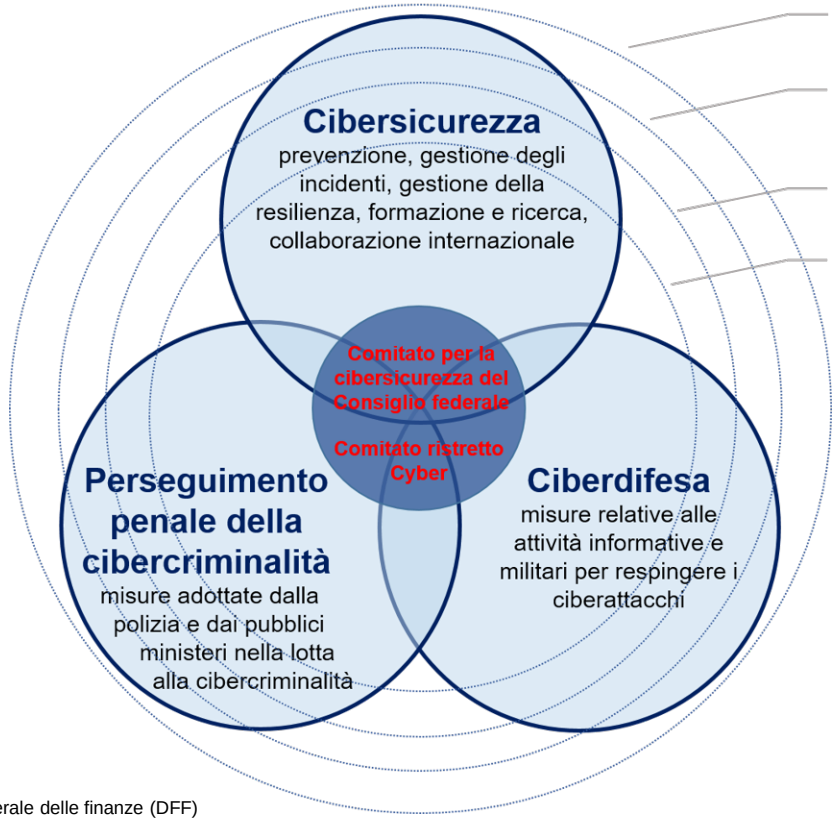
Dipartimento federale delle finanze (DFF)
Centro nazionale per la cibersicurezza (NCSC)

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Panoramica

1	Organizzazione della Confederazione nell’ambito dei ciber-rischi
2	Centro nazionale per la cibersicurezza (NCSC)
3	Sfide per la Svizzera

3 settori dei ciber-rischi



- Collaborazione internazionale
- Confederazione, Cantoni, Comuni
- Economia, università
- Reti, associazioni

Ciber rischi - organizzazione della Confederazione

Dipartimento federale delle finanze (DFF)
Centro nazionale per la cibersicurezza (NCSC)

Ordinanza sulla protezione contro i ciber-rischi nell'Amministrazione federale (OCiber)

- **Disciplina la collaborazione interdipartimentale** nonché la composizione e i compiti del Comitato ristretto Cyber e del Comitato direttivo SNPC
- **Disciplina i compiti e le competenze del delegato alla cibersicurezza**. Egli funge da principale persona di riferimento della Confederazione per le questioni inerenti ai ciber-rischi ed emana le direttive in materia di sicurezza informatica per l'Amministrazione federale
- **Disciplina le competenze per la gestione degli incidenti**: dopo aver consultato i servizi interessati, il NCSC può assumere in seno all'Amministrazione federale la responsabilità principale di ciberincidenti gravi
- **Disciplina gli obblighi di comunicazione:** i fornitori di prestazioni dell'Amministrazione federale hanno l'obbligo di comunicare al NCSC le vulnerabilità e gli incidenti

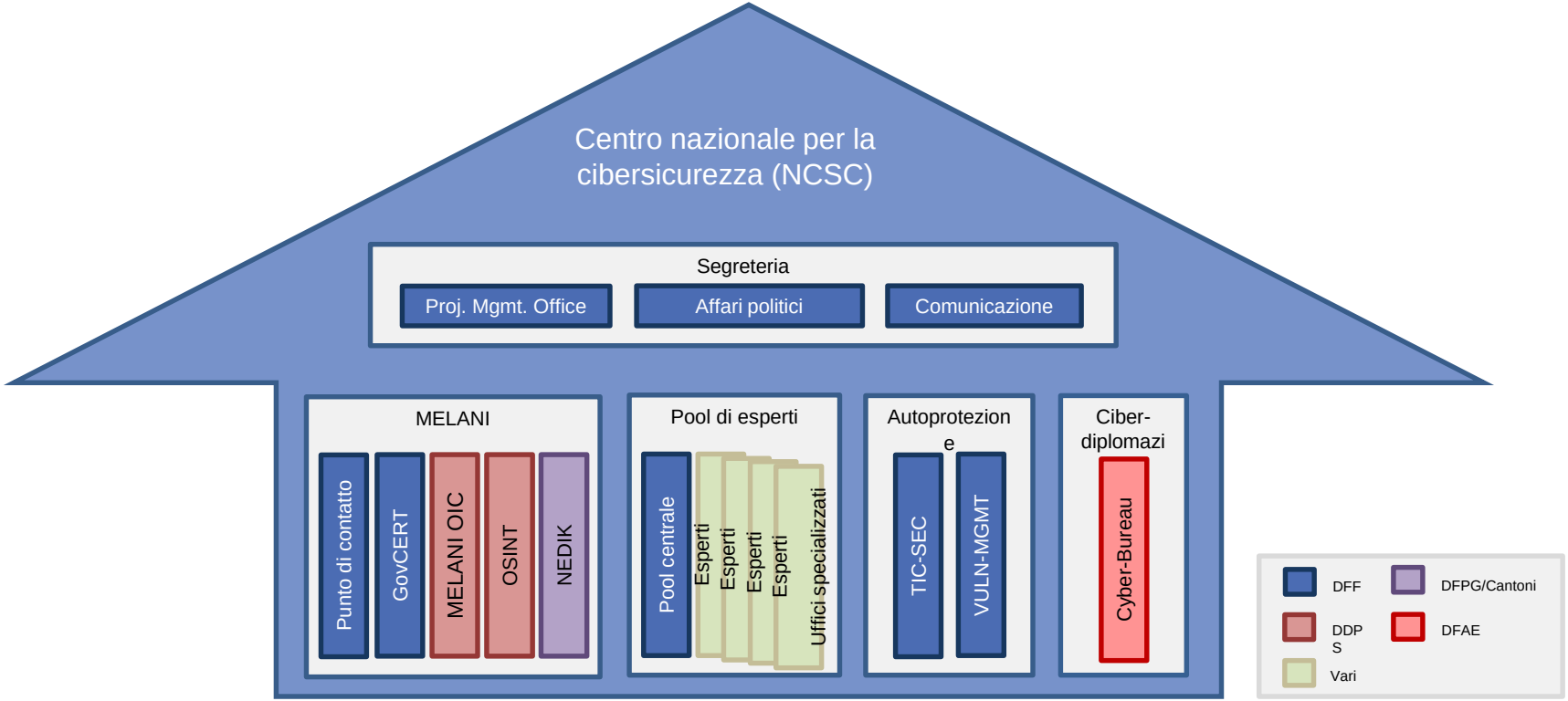
Confronto internazionale

- **Studio concernente l'organizzazione condotto dal Center for Security Studies del Politecnico di Zurigo:**
- Un confronto è possibile solo in misura limitata, l'organizzazione della cibersicurezza deve essere adattata al contesto politico
- Paesi messi a confronto: Germania, Finlandia, Francia, Israele, Italia e Paesi Bassi
- Risultati:

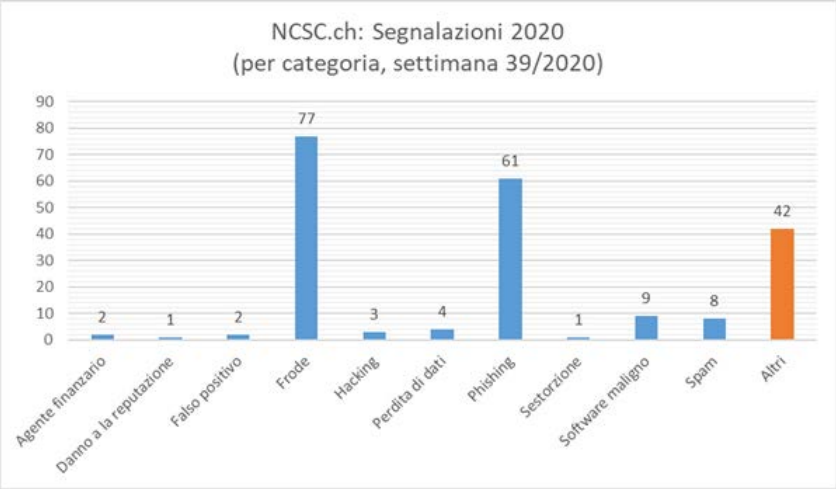
  - Stesse sfide presenti in tutti i Paesi; nessun Paese ha una soluzione definitiva
  - Nessun Paese dispone di un'unica organizzazione competente per tutti i settori
  - Nessun Paese affida la gestione all'esercito.

  È in corso uno studio sullo stato di attuazione della cibersicurezza in Svizzera; il mandato è stato assegnato all'università di Oxford che applicherà il suo modello di maturità alla Svizzera. I risultati saranno disponibili nell'autunno 2020.

Centro nazionale per la cibersicurezza (NCSC)



Cifre attuali NCSC



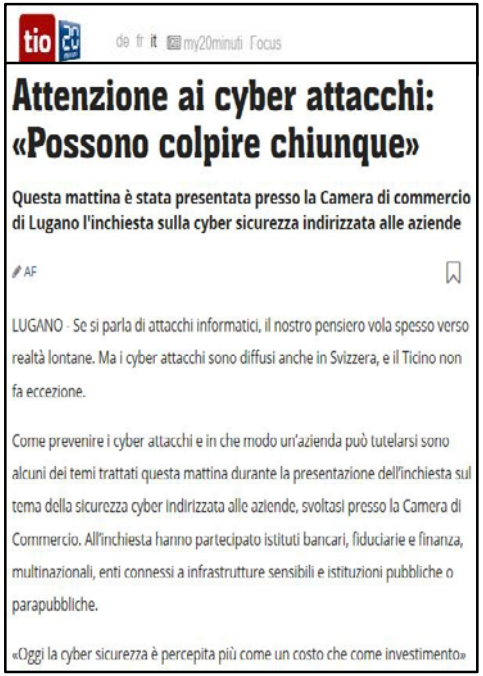
Tipi di incidenti – legati anche al Coronavirus

ticinonews TICINO SVIZZERA ESTERO ECONOMIA SPORT DECODER MAGAZINE ▶ RADIO3I

Coronavirus, occhio ai cyber attacchi

La autorità svizzere avvertono: cyber criminali stanno sfruttano l'attualità per infettare i computer con malware

Le autorità svizzere mettono in guardia da cyber attacchi che sfruttano l'epidemia di coronavirus. I criminali informatici promettono tramite e-mail informazioni sulla situazione, ma tentano in realtà di infettare i computer delle loro vittime. La Centrale d'annuncio e d'analisi per la sicurezza dell'informazione (MELANI) ha comunicato ieri sera tramite Twitter che cyber criminali sfruttano l'attualità legata al coronavirus per infettare i computer con il malware chiamato 'AgentTelsa'.



tio 20 minuti de fr it my20minuti Focus

Attenzione ai cyber attacchi: «Possono colpire chiunque»

Questa mattina è stata presentata presso la Camera di commercio di Lugano l'inchiesta sulla cyber sicurezza indirizzata alle aziende

AF

LUGANO - Se si parla di attacchi informatici, il nostro pensiero vola spesso verso realtà lontane. Ma i cyber attacchi sono diffusi anche in Svizzera, e il Ticino non fa eccezione.

Come prevenire i cyber attacchi e in che modo un'azienda può tutelarsi sono alcuni dei temi trattati questa mattina durante la presentazione dell'inchiesta sul tema della sicurezza cyber indirizzata alle aziende, svoltasi presso la Camera di Commercio. All'inchiesta hanno partecipato istituti bancari, fiduciarie e finanza, multinazionali, enti connessi a infrastrutture sensibili e istituzioni pubbliche o parapubbliche.

«Oggi la cyber sicurezza è percepita più come un costo che come investimento»

tio 20 minuti de fr it my20minuti Focus

Cybersecurity e COVID-19: le nuove minacce su rete

Sono in crescita in tutto il mondo gli attacchi informatici, ma ci sono alcune raccomandazioni per proteggersi

Andrea Palanca, Senior Cyber Security Advisor - Security Lab SagI

Se da un punto di vista sanitario COVID-19 sembra concedere respiro nell'ultimo periodo all'interno del Canton Ticino, dal punto di vista informatico la malattia **continua** ad essere **impietosamente** sfruttata da malintenzionati per condurre **cyberattacchi** ai danni di privati ed aziende.

8 sfide principali della Svizzera

1) Integrazione delle strategie nazionali di sicurezza informatica nel quadro della sicurezza nazionale e/o di una strategia globale
2) Coordinamento dei vari organismi nell'ambito della cibersicurezza
3) Collaborazione internazionale e definizione delle norme
4) Gestione delle crisi
5) Analisi della situazione e delle ciberminacce
6) Sviluppo delle competenze, formazione, informazione e sensibilizzazione
7) Creazione di un quadro di collaborazione efficace con il settore privato
8) Armonizzazione della legislazione

Center for Security Studies (CSS), ETH Zürich

Grazie per l’attenzione

Florian Schütz
Delegato federale alla cibersicurezza

Contatto

Centro nazionale per la cibersicurezza (NCSC)
Segreteria del delegato federale alla cibersicurezza
Bundesgasse 3, 3003 Berna, Svizzera
ncsc@gs-efd.admin.ch

Repubblica e Cantone
Ticino

I Cantoni di fronte ai cyber-rischi

André Duvillard
Delegato della Rete integrata Svizzera per la sicurezza (RSS)

Piano della relazione

Introduzione

1. La Rete integrata Svizzera per la sicurezza (RSS)
2. Digitalizzazione crescente
3. Cyber-rischi e federalismo
4. 2012-2017: primo approccio collaborativo
5. 2018-2022: contributo attivo dei Cantoni
6. Qualche esempio concreto
7. Conclusioni

Introduzione

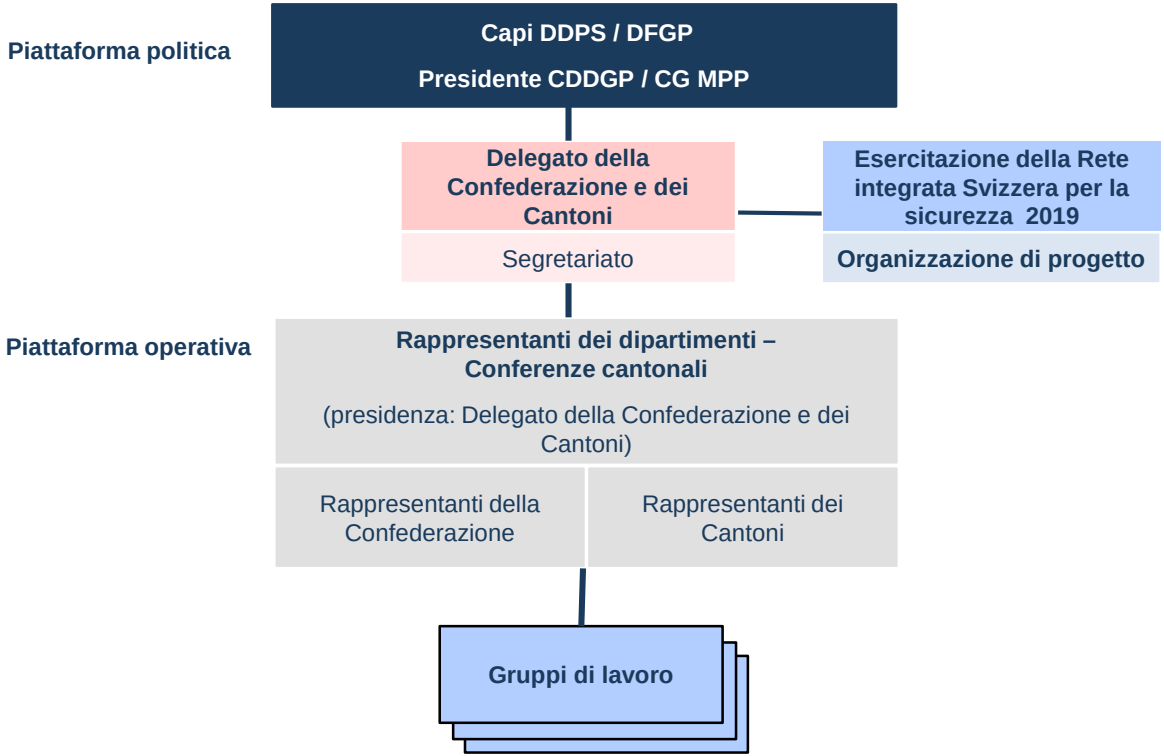
1. La Rete integrata Svizzera per la sicurezza (RSS)

La Rete integrata Svizzera per la sicurezza comprende di principio tutti gli strumenti della politica di sicurezza della Confederazione, dei Cantoni e dei Comuni e i suoi organi servono a garantire la consultazione e il coordinamento necessari per le decisioni, i mezzi e le misure della Confederazione e dei Cantoni volti a far fronte alle sfide comuni in materia di politica di sicurezza.

RAPOLSIC 2016

La parità come principio di base

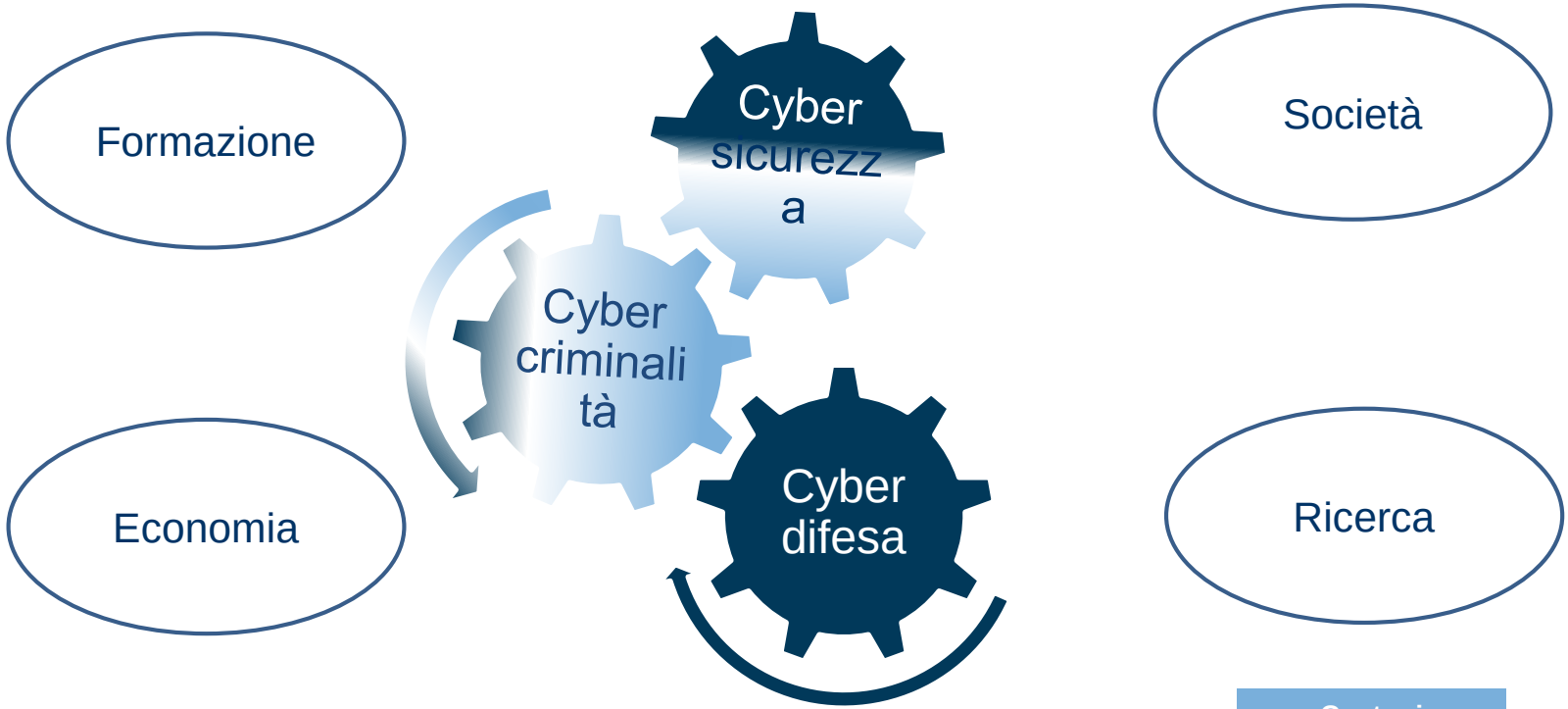
Organigramma RSS



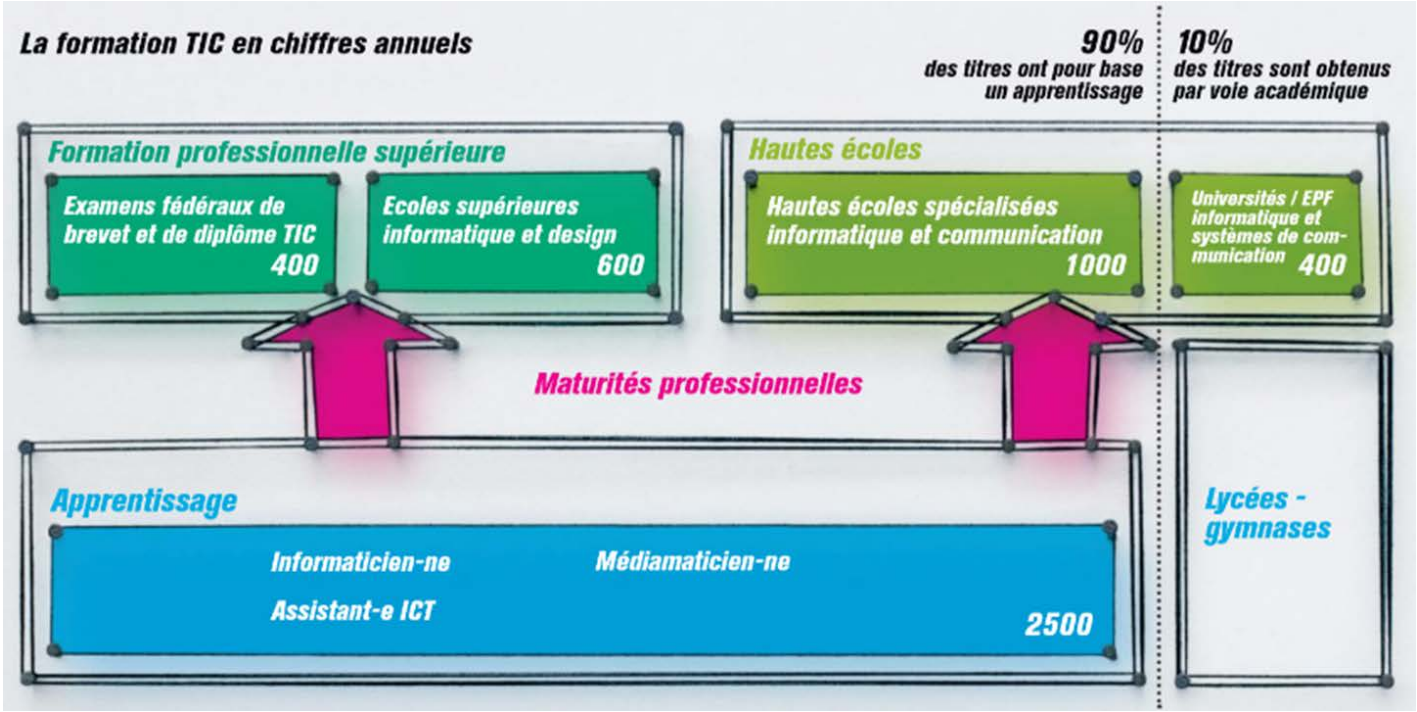
2. Digitalizzazione crescente

§ 3. Cyber-rischi e federalismo

3. Cyber-federalismo



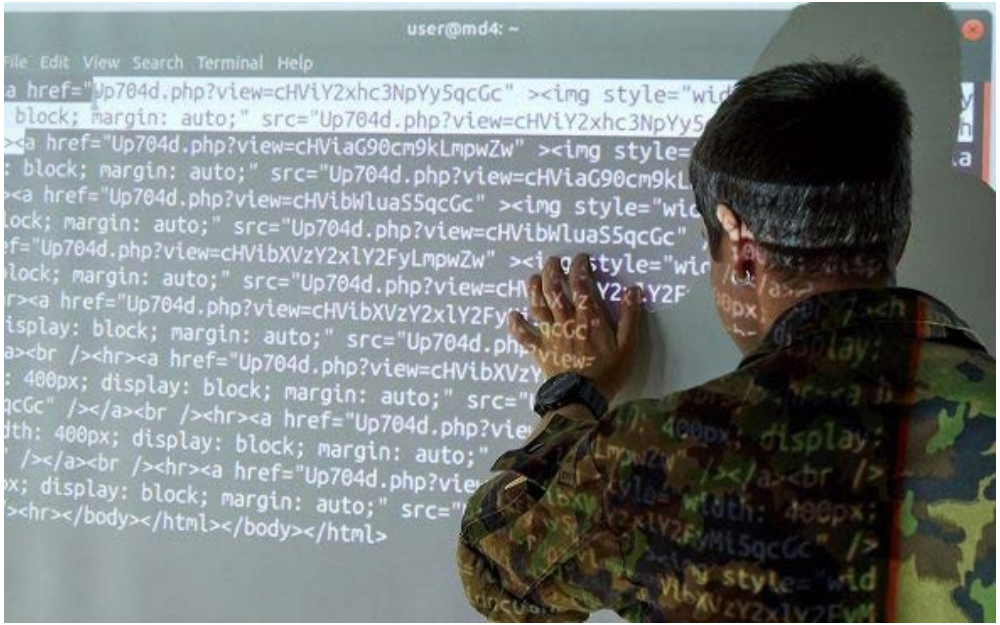
Un grande fabbisogno di specialisti



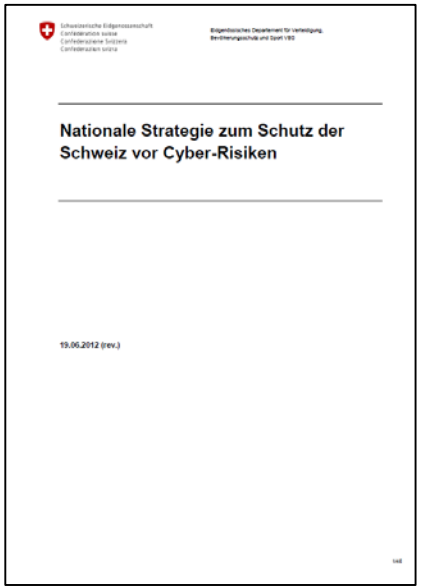
Nel 2026 mancheranno 40'300 specialisti TIC …

Source: ICT-Berufsbildung - 2017

Specialisti in cybersicurezza ed Esercito di milizia



4. 2012–2017: un primo approccio collaborativo

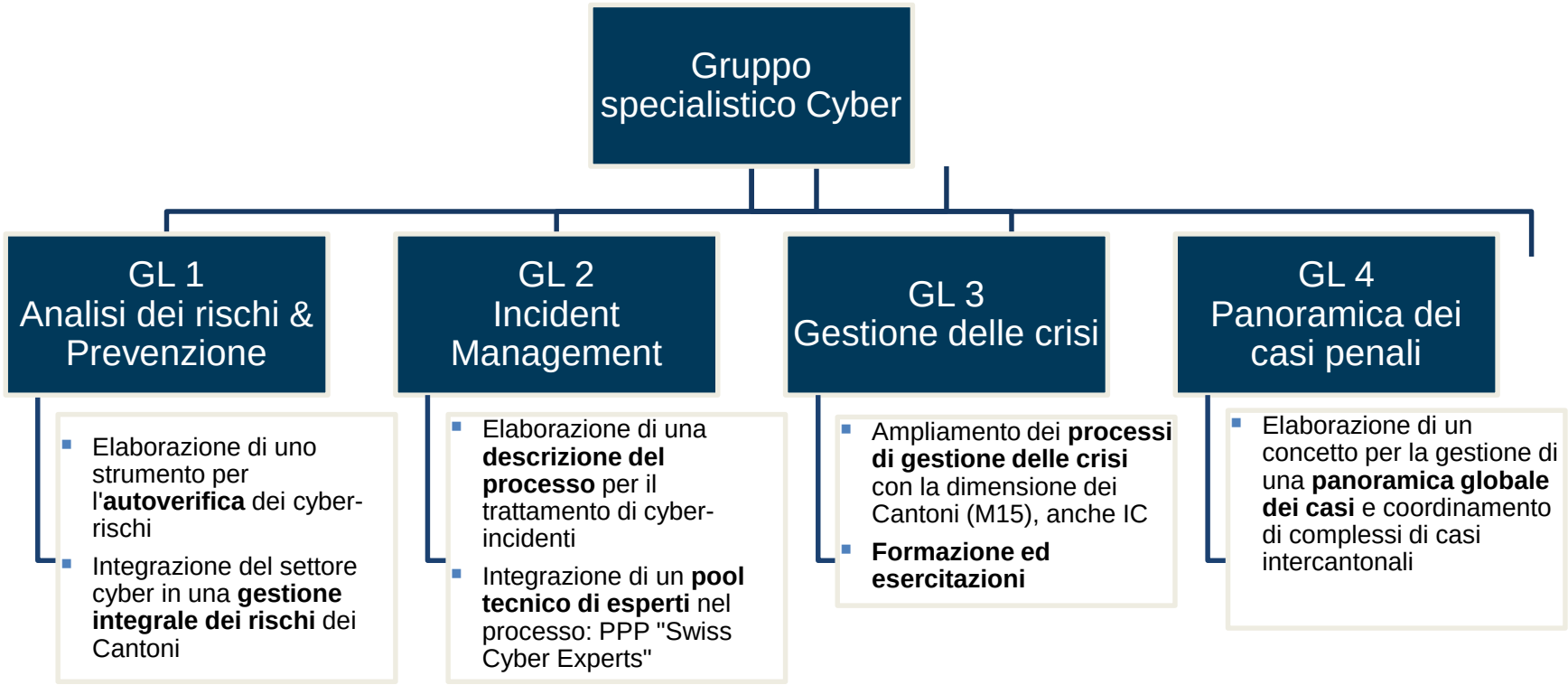

Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken

19.06.2012 (rev.)

Obiettivi:

1. Individuazione precoce delle minacce e dei pericoli
2. Incremento della resistenza delle infrastrutture critiche
3. Riduzione efficace dei cyber-rischi

Gruppo specialistico e gruppi di lavoro (GL) RSS

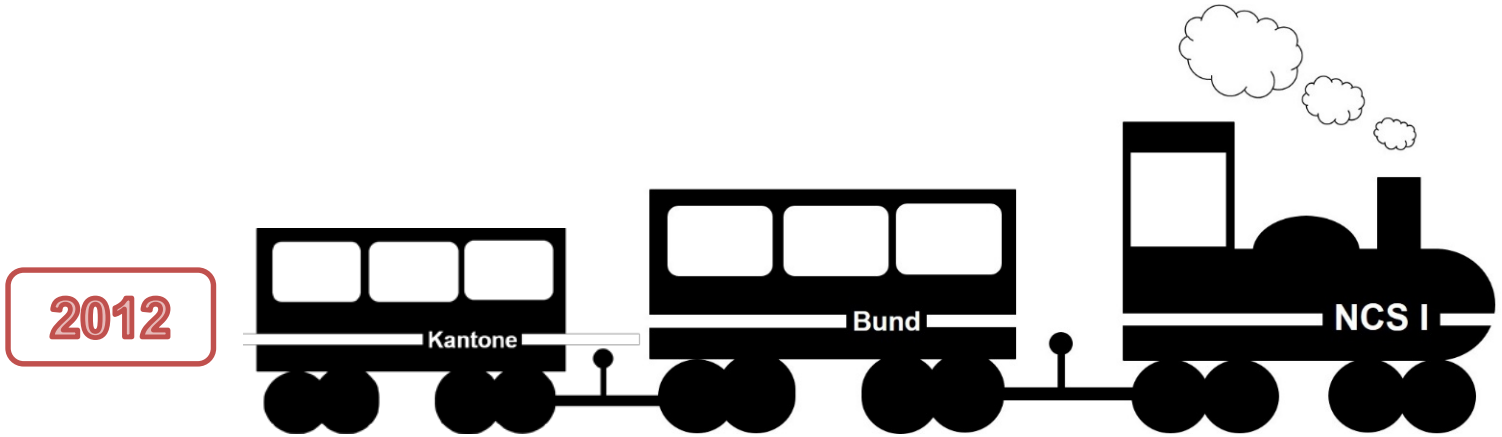


Bilancio dal punto di vista dei Cantoni

- Il gruppo specialistico cyber e suoi quattro gruppi di lavoro funzionano e hanno fornito un contributo importante alla concretizzazione della SNPC nei Cantoni.
- Grazie all'incontro nazionale annuale «Cyber», lo scambio reciproco di informazioni è garantito.
- La collaborazione tra Confederazione e Cantoni ha potuto essere rafforzata.
  - Poiché ora tutti i Cantoni hanno aderito a MELANI, è pure stata migliorata la capacità di reazione.
  - Il coinvolgimento dei Cantoni nelle esercitazioni di gestione delle crisi contribuisce a individuare ed eliminare i punti deboli nella gestione della resilienza.
  - In tutti i settori la collaborazione può tuttavia essere ulteriormente ampliata.

(v. anche Verifica dell'efficacia SNPC, 2016 / Wirksamkeitsüberprüfung NCS, 2016)

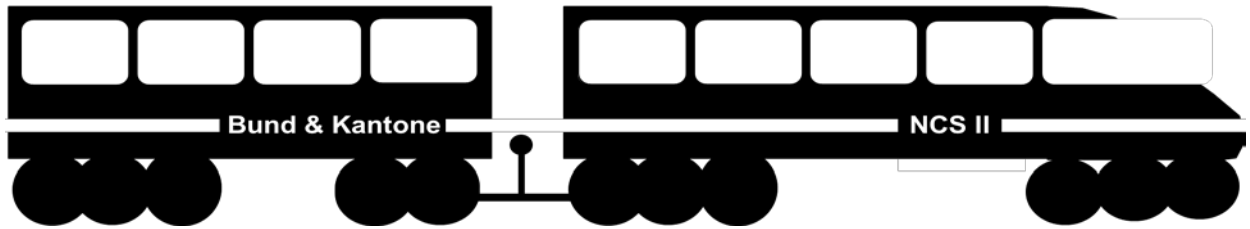
Treno moderato



5. 2018-2022: contributo attivo dei Cantoni

Tempo allegro ma non troppo

2019



Campi d’azione

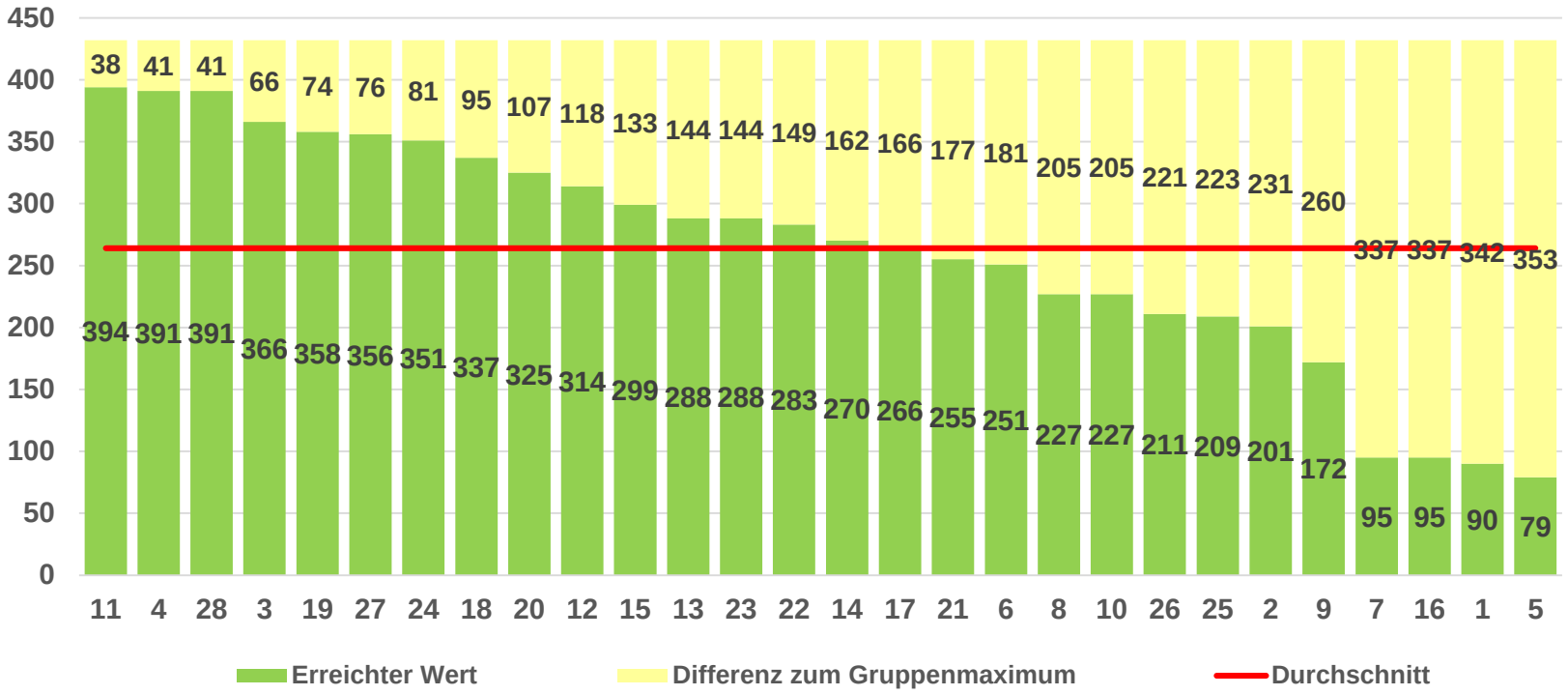
Sviluppo di un concetto di formazione continua e di un modulo per le amministrazioni cantonali

- **Obiettivo:** è essenziale **sviluppare proattivamente le competenze in materia cyber di tutti**.
- Le amministrazioni cantonali e le istituzioni ad esse connesse constituiscono uno dei pilastri del funzionamento della nostra società e per tale motivo devono imperativamente essere formate al riguardo.
- Proporre un **programma di formazione** destinato al personale delle amministrazioni cantonali che definisca chiaramente e in maniera pragmatica gli obiettivi da raggiungere e le competenze a cui si mira.

Strumento di valutazione per migliorare la resilienza informatica nei Cantoni

- **Obettivo:** per migliorare la loro resilienza (capacità di resistenza e di rigenerazione), **i Cantoni analizzano le esigenze minime da soddisfare in materia di processi, competenze e compiti**.
- Utilizzo di uno **strumento di valutazione** concepito dall'Ufficio federale dell'approvvigionamento economico del Paese e adeguato alle loro necessità.
- Tasso di risposta del 96% - risultati positivi.
- La fase di valutazione è iniziata in agosto.
- Presentazione dei risultati in comitati strettamente selezionati.

Valutazione dettagliata



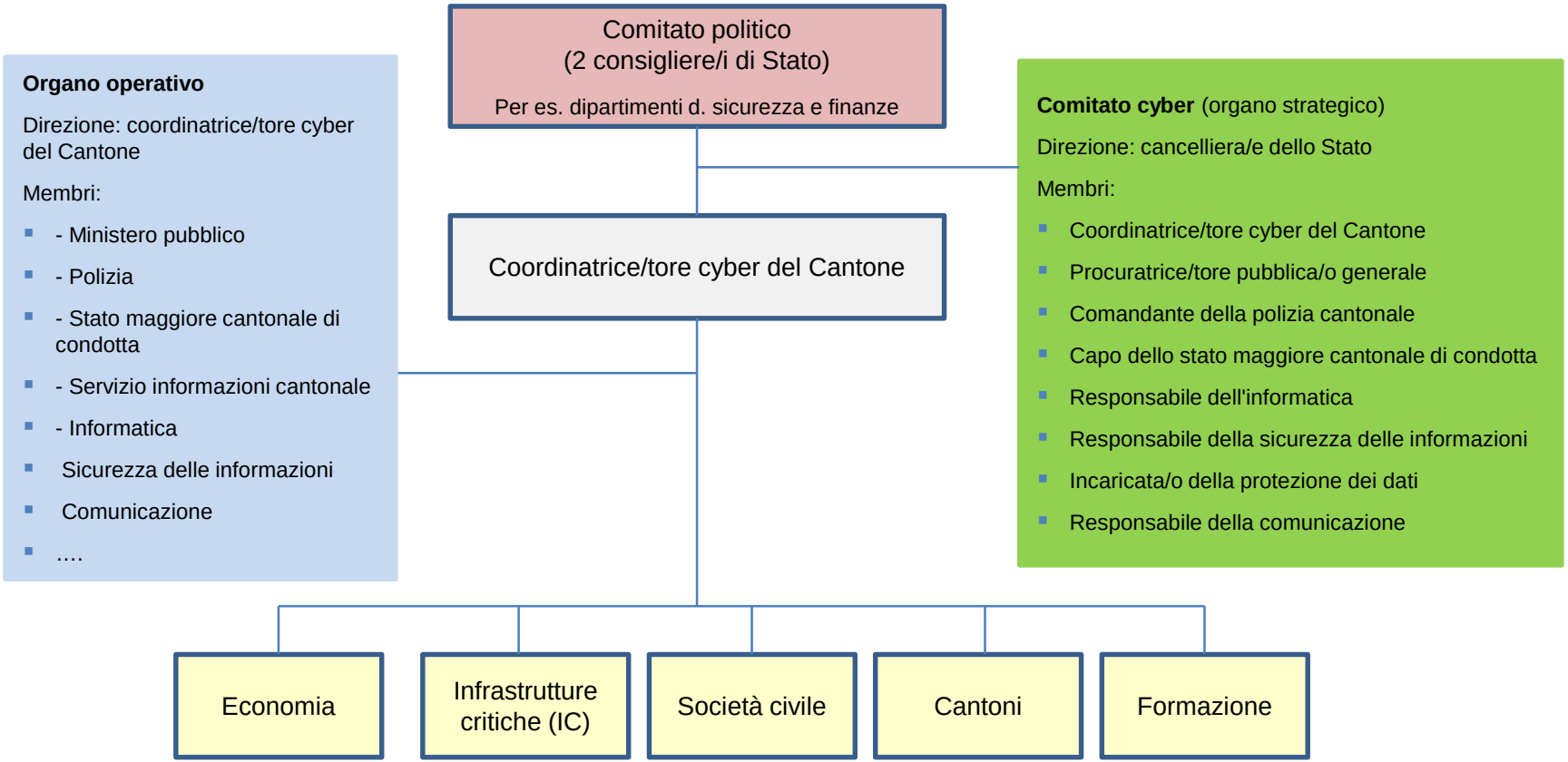
Cyberesercitazione con un’infrastruttura critica (IC) nel campo della sanità

- **Obiettivo:** in caso di crisi, il coordinamento operativo tra Confederazione, Cantoni e gestori di IC funziona e i servizi interessati dispongono di un quadro della situazione aggiornato. La strategia di condotta ha potuto essere verificata nel caso di una crisi che comportava aspetti cyber.
- Ospedale universitario di Zurigo (USZ): unità d'infrastruttura oggetto dell'esercitazione.
- Elaborazione di uno scenario in collaborazione con il gruppo di lavoro in seno all’USZ e MELANI.
- Esercitazione nella forma table-top nel 2021, esercitazione quadro di stato maggiore nel 2022.

Creazione di organizzazioni cantonali per la cybersicurezza

- Creazione, in ogni Cantone, di un'**organizzazione incaricata della cybersicurezza,** sul modello della nuova struttura organizzativa realizzata in ambito cyber a livello di Confederazione.
- Questo servizio cantonale, che detiene la **sovranità budgetaria** e ha la competenza di emanare direttive, segue da vicino la situazione, rappresenta il Cantone in tutte le questioni in ambito cyber, siede nello stato maggiore cantonale di condotta e garantisce il coordinamento in seno al Cantone, tra i Cantoni e con la Confederazione.
- Concetto sviluppato e sottoposto a consultazione.
- Finalizzazione del concetto (traduzione).

Organigramma di un’organizzazione cyber cantonale



Sensibilizzazione dei Comuni

- Connessi alla Confederazione.
- Trattamento di dati sensibili.
- Numerosi prestari di servizi esterni nei piccoli Comuni.
- Si stima che i 2/3 dei Comuni presenti una criticità molto importante in materia di cybersicurezza.

6. Conclusioni

- Non si tratta soltanto di un problema tecnico. Si tratta di una sfida per l'intera società e deve figurare tra le priorità dei decisori (politici, economici, dell'amministrazione ecc.).
- Non occorre inoltre dimenticare che il fattore umano è sempre presente. Analogie con i furti commessi quando porte e finestre sono aperte …
- Il rischio rimarrà sempre, ma dobbiamo ridurlo.
  - Educazione
  - Igiene digitale

Grazie della vostra attenzione…

Repubblica e Cantone Ticino

Lotta alla cybercriminalità

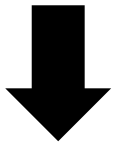
Spunti dal Ticino e NEDIK

cap Orlando Gnosca

Ufficiale della Polizia cantonale e membro del comitato della rete nazionale di sostegno alle indagini nella lotta contro la criminalità informatica


Sondaggio:
Il 98% di tutti gli hacker non indossa un passamontagna davanti al computer

NEDIK



Netzwerk **E**rmittlungsunterstützung **D**igitale **K**riminalitätsbekämpfung

(Rete nazionale di sostegno alle indagini nella lotta contro la criminalità informatica)

Cyber o Ciber ?

Anche l’Accademia della Crusca si è chinata su questo tema

MENU CERCA

Il Messaggero

ITALIA

«Si scrive ciber e non cyber». La sentenza dell'Accademia della Crusca

ITALIA

Giovedì 22 Novembre 2018

… ma noi continuiamo a scriverlo cyber

Il tempo è denaro.

I dati sono denaro.

Minacce informatiche

Cyberdifesa

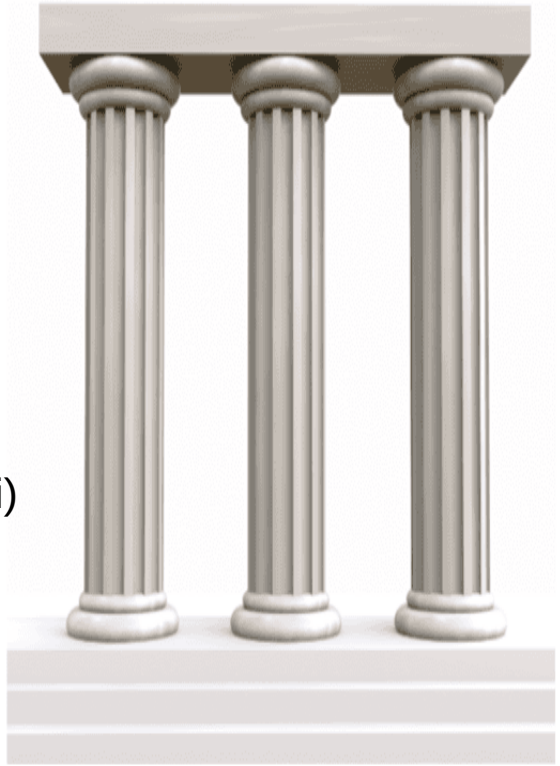
- Difesa nazionale
- Responsabilità: Esercito

Cybersicurezza

- Protezione dei computer e di Internet
- Responsabilità: tutti
  (fornitori, aziende, privati, Confederazione e Cantoni)

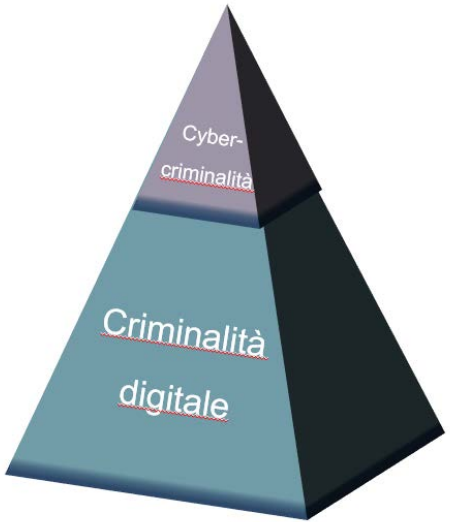
Cybercriminalità

- Procedimento penale e prevenzione
- Responsabilità: forze di Polizia cantonale

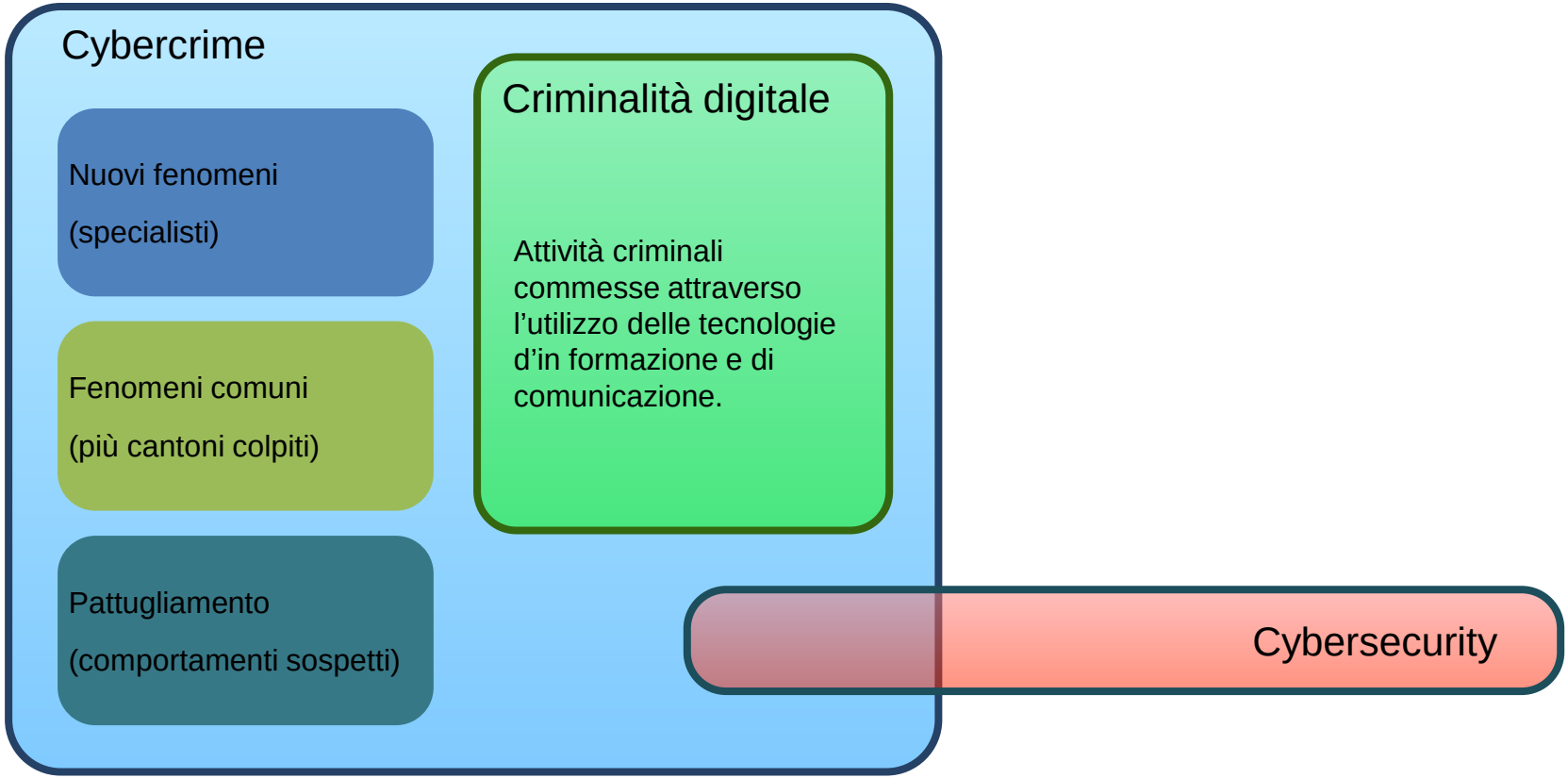


Cybercriminalità - Strategia

- **Cybercriminalità**
  Infrazioni contro i computer, reti e altre forme di ITC
- **Criminalità digitale**
  Infrazioni "classiche" commesse con l'ausilio della moderna tecnologia



Concetti


Cybercrime
Nuovi fenomeni
(specialisti)
Fenomeni comuni
(più cantoni colpiti)
Pattugliamento
(comportamenti sospetti)
Criminalità digitale
Attività criminali commesse attraverso l'utilizzo delle tecnologie d'in formazione e di comunicazione.
Cybersecurity

3 tipologie di attività cyberinvestigativa

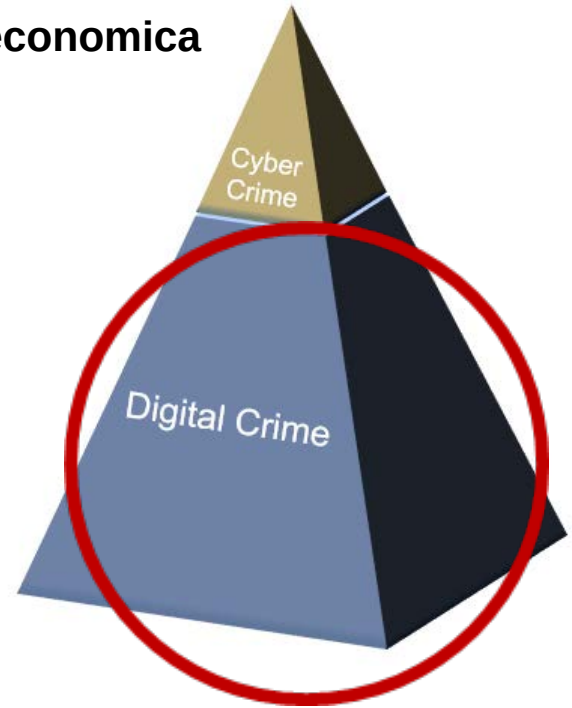
1. **Punto-punto: da autore a vittima.**
   Si hanno buone possibilità di ottenere dei risultati.

2. **Globale (tipo Wonnacry): la Svizzera e il Ticino sono toccati come tanti altri.**
   Poche o nessuna possibilità di fare/ottenere qualcosa.

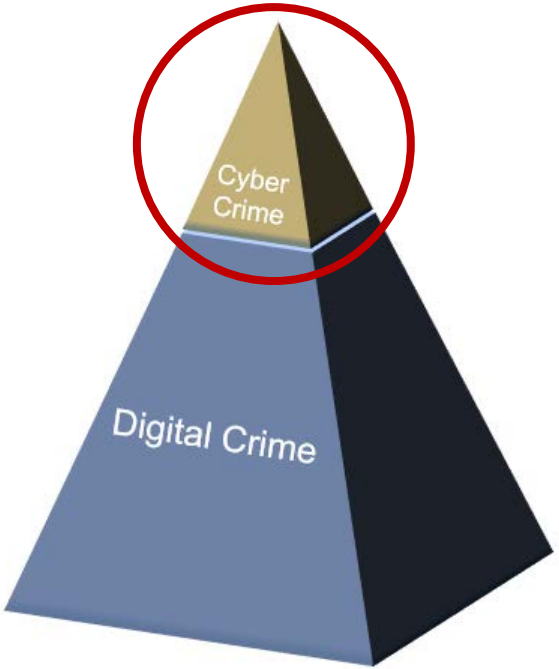
3. **Fenomeni con una base/contatto in Svizzera: come le truffe Microsoft o del CEO.**
   Anche in questo caso poche possibilità di ottenere risultati.

Criminalità economica

Criminalità digitale e criminalità informatica = criminalità economica



Cybercriminalità



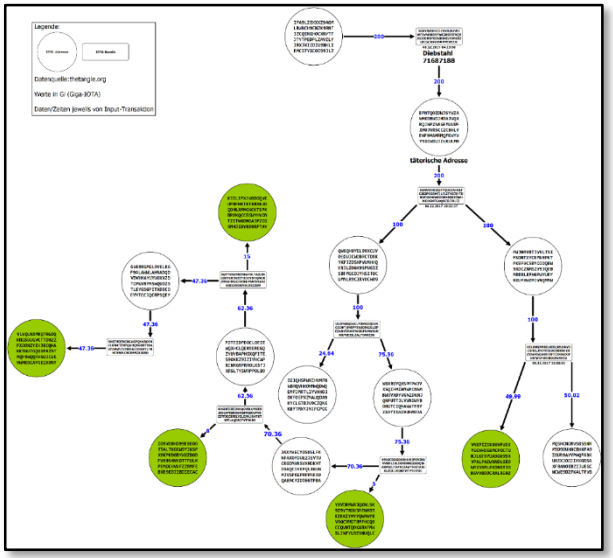
Responsabilità della polizia

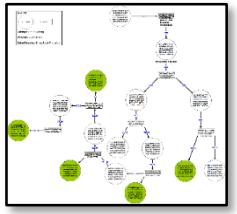
- La protezione e la riparazione delle infrastrutture sono di competenza dei proprietari.
- Il compito della polizia è quello di identificare e localizzare i colpevoli.
- Consigliare e assistere le parti lese.
- La polizia non è interessata ai segreti commerciali e non chiude le vostre infrastrutture.



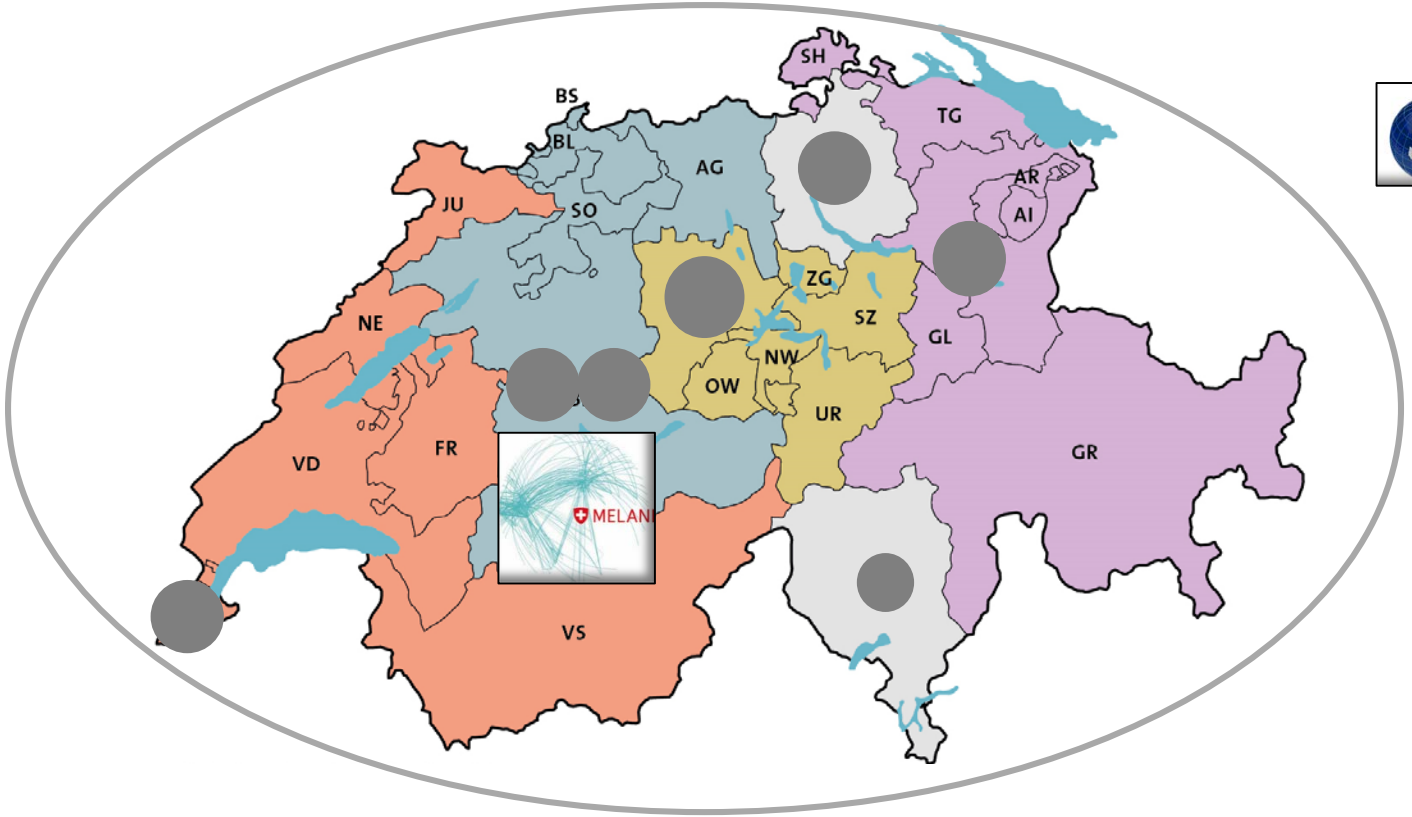

Cosa stanno facendo le forze dell'ordine

- Indagini in Internet
- Ricerca tracce informatiche
- Tracciamento dei flussi finanziari in rete
- Misure di sorveglianza segreta
- Analisi del malware

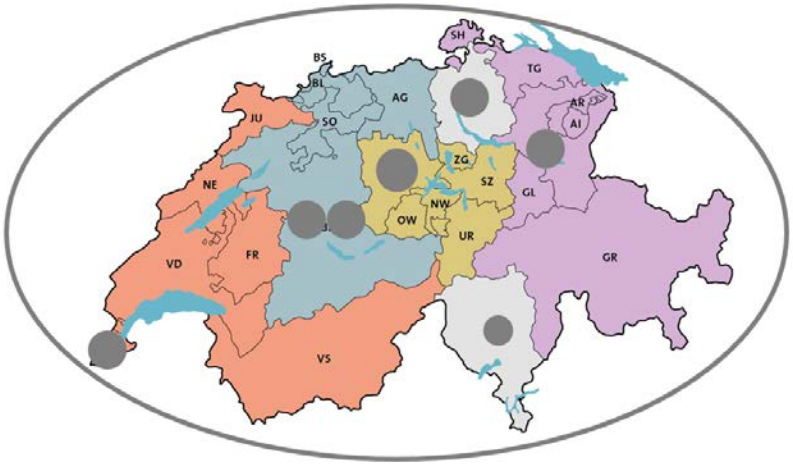




Rete di polizia intercantonale



NEDIK – Compiti e obiettivi



- Procedimento penale
- Prevenzione
- Best Practices
- Istruzione e formazione

Cybercriminalità: Opportunità e sfide

Rete nazionale di sostegno alle indagini nella lotta contro la criminalità informatica

La Conferenza dei Comandanti delle Polizie Cantonali Svizzere mira a mettere in comune le conoscenze specialistiche delle polizie, nella lotta contro la criminalità digitale.

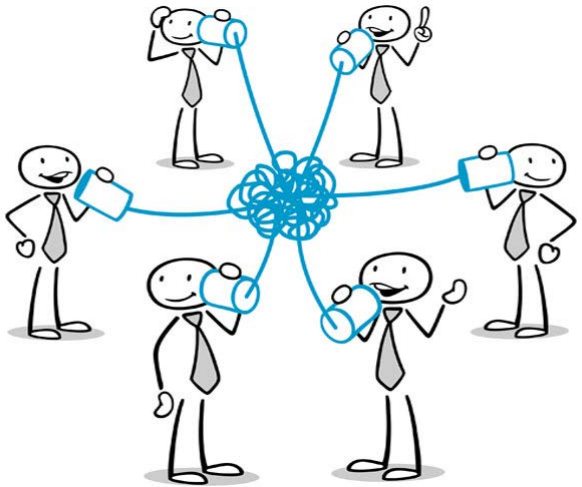
Competenze disponibili all'interno dei corpi di polizia cantonali e di fedpol e inserite in una rete di autorità di polizia per indagare sulla criminalità informatica.

Obiettivi:

- Promozione della cooperazione tra i Cantoni
- Panoramica nazionale della casistica (rete di allerta)
- Catalogo dei prodotti che possono essere ottenuti da altri corpi
- Garantire il trasferimento delle conoscenze
- Collaborazione con le autorità federali come fedpol e NCSC

NEDIK: Obiettivi

- **Promuovere la cooperazione** tra le forze di polizia svizzere nel campo della criminalità informatica per proteggere la popolazione dalla criminalità informatica.
- **Coordinare le azioni** di lotta contro la criminalità informatica in tutti i Cantoni.
- **Scambiare informazioni** all'interno della rete così da coordinare misure preventive e repressive.
- Adattare le **opportunità di formazione e perfezionamento** professionale.



Prevenire la cybercriminalità - Imprese

1 NEDIK - Manuale per piccole e medie imprese per impedire la cribercriminalità.pdf
2 Checklist - Cyberattacco che fare.pdf
3 Checklist - Cyberaggresioni come proteggersi.pdf
4 Checklist - Attacco DDoS che fare.pdf
5 Checkliste - Malware che fare.pdf
6 Autovalutazione per dirigenti d'impresa.pdf
7 Dieci consigli per sventare cyberattacchi.pdf
8 Pronto soccorso in caso un cyberattacco.pdf
9 Consigli per collaboratori.pdf

Da oggi il manuale e le checklist sono presenti sul sito della Polizia cantonale www.polizia.ti.ch.

Prevenire la cybercriminalità - Comuni

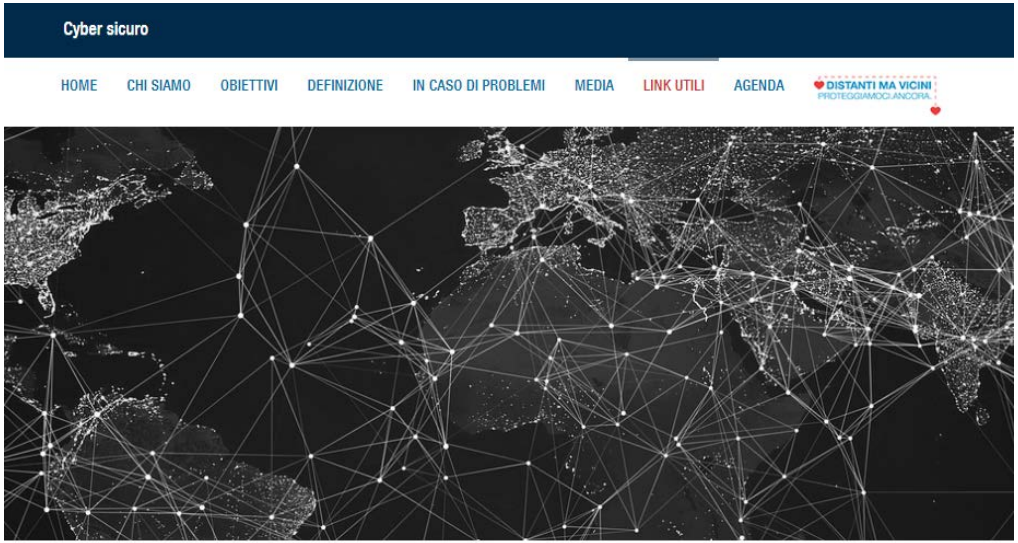
Cybercriminalità – Conclusioni

Se non pagate per un prodotto, voi siete il prodotto.

Cybercriminalità – Qualche conclusione

- Fattore umano
- Tecnologia
- Formazione
- Scremare l’utile
- **ALLARMARE (interno e esterno !!!)**

E non dimenticate …



Link utili

Per meglio circoscrivere il dominio operativo ufficiale per la gestione della sicurezza informatica vengono elencati i seguenti link utili:

- NIST - National Institute of Standards and Technology, Cybersecurity Framework (CSF)
- Europol – Cybercrime
- Polizia Federale Svizzera
- Strategia nazionale per la protezione della Svizzera contro i cyber-rischi (SNPC) 2018-2022
- Prevenzione Svizzera della Criminalità
- Centro nazionale per la cybersicurezza, NCSC (ex-Melani)
- Svizzera e cybercrime
- Sezione Analisi Tracce Informatiche (SATI) della Polizia cantonale
- Giovani e media

Nella linkoteca del sito www.cybersicuro.ch trovate importanti contatti per ottenere informazioni utili.

Ricordate il 117 per le urgenze.

Domande? Dubbi? Angosce? Perplessità? Incognite ?…

È nata un’idea

Repubblica e Cantone Ticino

Conclusioni

Alessandro Trivilini
Docente-ricercatore del Dipartimento tecnologie innovative, SUPSI
Membro Gruppo «Cyber sicuro»

Domande

CYBER
SICURO