Protezione della popolazione

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Ufficio federale della protezione della popolazione UFPP

RIVISTA DI ANALISI DEI RISCHI E PREVENZIONE, PIANIFICAZIONE E ISTRUZIONE, CONDOTTA E INTERVENTO

27 / MARZO 2017

Nuove tecnologie

Cyber-rischi

Pagina **7**

Nicoletta della Valle, direttrice di fedpol

«Il lavoro della polizia è radicalmente cambiato»

Pagina **4**

Cooperazione

Insegnamenti tratti dalla crisi migratoria

Pagina **20**

Istruzione

Compresse allo iodio per l'ambasciata a Vienna

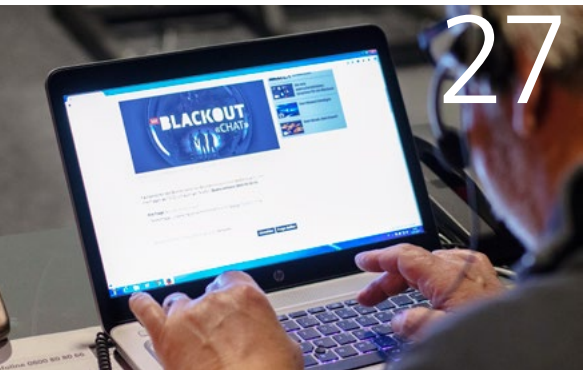
Pagina **22**

Grigioni

Grandi operazioni contro le fiamme

Pagina **32**

www.protpop.ch



EDITORIALE 3

PRIMO PIANO

«Il lavoro della polizia è radicalmente cambiato» 4
Per Nicoletta della Valle, la fedpol è più un organo di polizia che un ufficio federale. Nella sua intervista, la direttrice di fedpol descrive il suo ente come una piattaforma e un fornitore di servizi per i partner nei Cantoni. Parla di criminalità, terrorismo e della passione per il suo lavoro.

DOSSIER: CYBER-RISCHI

Opportunità e rischi delle nuove tecnologie 7
Le nuove tecnologie cambiano sempre più la nostra quotidianità. Ovviamente questi sviluppi offrono molti vantaggi e agevolazioni, ma comportano anche dei rischi, in particolare per la privacy.

Sulle tracce dei truffatori in rete 10
In Svizzera, la centrale d'annuncio MELANI provvede a migliorare continuamente la protezione e la lotta contro i crimini informatici.

Sollecitati i gestori delle infrastrutture critiche 13
Soprattutto gli attacchi cibernetici possono avere gravi conseguenze per infrastrutture critiche come le aziende elettriche e dell'acqua potabile, la sanità o il settore finanziario. La Confederazione s'impegna a riconoscere e a ridurre tali rischi.

Cyber-rischi rilevanti per la protezione della popolazione 16
Un attacco cibernetico potrebbe colpire la capacità operativa della protezione della popolazione? Quali misure sono già state adottate contro tali minacce?

COOPERAZIONE 19

ISTRUZIONE 22

POLITICA 24

CONFEDERAZIONE 25

UFPP 26

CANTONI 28

ASSOCIAZIONI 36

SERVIZI 38

L'ULTIMA PAROLA 39

Immagine di copertina: gli Hacker sfruttano le nuove tecnologie a fini criminali. Fotomontaggio.

Cari lettori

Molte persone si sentono sempre più insicure, anche in Svizzera. Un fattore decisivo per questa insicurezza è la crescente complessità dei sistemi tecnici, cui ci affidiamo nella vita di tutti i giorni. In quasi tutti i settori dell'economia, dello Stato e della società dominano due tendenze fondamentali: l'interconnessione e la digitalizzazione. E la nostra vita privata è condizionata da molte informazioni on-line, anche da algoritmi che non capiamo, da sistemi così complessi da non riuscire a comprenderli nemmeno in modo approssimativo.

«La nostra vita è condizionata da sistemi così complessi da non riuscire a comprenderli nemmeno in modo approssimativo»

Lungi da me condannare questi nuovi sviluppi e le nuove tecnologie, poiché offrono enormi vantaggi ed opportunità. Chi rinuncerebbe oggi alla comodità di consultare direttamente in rete le notizie o gli orari dei mezzi di trasporto? L'interconnessione e la digitalizzazione rendono inoltre molto più efficienti e produttive le aziende. E nel settore della sanità l'interconnessione digitale e la trasmissione rapida delle informazioni possono essere fondamentali per salvare vite umane. Pertanto, un ritorno all'era predigitale non è solo da escludere, ma sarebbe una grande perdita di libertà, efficienza, benessere … e senza dubbio anche una perdita di sicurezza.

La nostra società diventa sempre più efficiente, ma al prezzo di un aumento della vulnerabilità. Dobbiamo vivere con un paradosso: da un lato, la digitalizzazione e l'interconnessione consentono una maggiore sicurezza, dall'altro ci espongono a nuovi rischi. Il tema dei cyber-rischi acquisisce quindi grande importanza anche per la protezione della popolazione. Noi dobbiamo sfruttare le opportunità offerte dalle nuove tecnologie, e intendiamo farlo, ma dobbiamo anche garantire che i sistemi, i dati e le applicazioni utilizzate nella protezione della popolazione siano sicuri. E questa sicurezza è oggi sempre più minacciata nel cyber-spazio.

Vi auguro una buona lettura!

Benno Bühlmann
Direttore dell'Ufficio federale della protezione della popolazione UFPP

Nicoletta della Valle, direttrice di fedpol

«Il lavoro della polizia è radicalmente cambiato»

Per Nicoletta della Valle, la fedpol è più un organo di polizia che un ufficio federale. Nella sua intervista, la direttrice di fedpol descrive il suo ente come una piattaforma e un fornitore di servizi per i partner nei Cantoni. Parla di criminalità, terrorismo e della passione per il suo lavoro.

La sicurezza è la Sua professione, ma le attribuisce importanza anche nella vita privata?
La sicurezza è importante per me come per la maggior parte di noi. Allaccio sempre la cintura di sicurezza in auto e indosso sempre il casco in bicicletta e quando scio.

Quale capo supremo della polizia, non ha particolari paure?
La paura non è mai «un buon consigliere». Viviamo in un Paese sicuro. Lo si vede anche dal fatto che i nostri Consiglieri federali si muovono liberamente e indisturbati. La Svizzera rimane una specie di isola in questo senso. La mia missione è contribuire, insieme agli organi partner, affinché la Svizzera rimanga un Paese sicuro.

Com'è arrivata ad assumere questa importante carica?
Dirigere la fedpol era il lavoro dei miei sogni. Mi sono data quindi da fare per raggiungere questo obiettivo.

Nicoletta della Valle

Dall'agosto 2014, Nicoletta della Valle è direttrice di fedpol, dove aveva già lavorato dal 2006 fino all'inizio del 2012 come vicedirettrice e capo della divisione Risorse. Dal 2012 al 2014 ha diretto il reparto Servizi ed esercizio presso i Servizi psichiatrici della clinica universitaria di Berna (Universitäre Psychiatrische Dienste, UPD), dove per quasi due anni ha assunto anche la funzione di copresidente ad interim della direzione. Negli anni Novanta, ha lavorato come giurista presso l'allora Ufficio federale dell'ambiente, delle foreste e del paesaggio, da ultimo come capo del Servizio giuridico. In seguito ha rivestito la carica di capo dell'Ispettorato e compiti speciali / Servizio dei ricorsi del Dipartimento federale di giustizia e polizia (DFGP). Ha 55 anni e abita a Berna.

Credo che la fedpol sia l'ente più appassionante della Confederazione, perché non siamo un ufficio qualsiasi, ma un organo di polizia.

Che cosa trova di così appassionante nel Suo lavoro?
È un lavoro molto variato. Devo difendere con validi argomenti il nostro preventivo davanti alla relativa commissione parlamentare. Sono infatti responsabile di un'organizzazione di circa mille collaboratori, operativa 24 ore su 24. Ho un ampio ventaglio di compiti politico-strategici ed operativi. È un lavoro di grande responsabilità, ma anche molto appassionante.

Quali sono i compiti strategici?
In tutto il mondo non c'è polizia che ammetterà di avere abbastanza risorse. Impiegare in modo mirato il personale e fissare le priorità sono quindi compiti strategici fondamentali. Ciò richiede a volte decisioni difficili. Devo spiegare alle autorità politiche qual è il nostro scopo e quali sono i nostri servizi. Si tratta di un lavoro di convincimento e di mediazione.

E quali sono i compiti operativi di fedpol?
Sono tutta una serie di compiti. In occasione delle visite di ministri stranieri, la fedpol si occupa, insieme alla polizia cantonale competente, di proteggere gli ospiti e i nostri consiglieri federali. Quando la competenza per i procedimenti penali, ad esempio contro sostenitori del terrorismo, spetta alla Confederazione, noi siamo la polizia criminale del Ministero pubblico della Confederazione. Gestiamo una centrale operativa 24 ore su 24 e siamo l'interfaccia tra le polizie cantonali e le autorità di polizia straniere.

«In tutto il mondo non c'è polizia che ti dirà di avere abbastanza risorse»

Come giudica la collaborazione con i Cantoni?
Funziona sempre meglio. Secondo la costituzione, la sicurezza interna compete generalmente ai Cantoni. Costituiscono un'eccezione i poteri investigativi in occasione di alcuni crimini, come ad esempio in caso di terrorismo o di organizzazioni criminali. La criminalità non si ferma ai confini cantonali e nemmeno a quelli nazionali. Serve quindi la collaborazione di tutti, ossia delle autorità di sicurezza della Confederazione e dei Cantoni. Quale fornitrice di servizi, la Fedpol offre prestazioni di coordinamento ai Cantoni nonché competenze specialistiche e sostegno per la cooperazione con l'estero. Gestiamo sistemi informativi, ad esempio nel campo delle impronte digitali, dei profili DNA, della caccia all'uomo nell'area Schengen. Per conoscere le esigenze dei Cantoni, intratteniamo ottimi rapporti con essi. Sono quindi anche membro della Conferenza dei comandanti di polizia cantonali della Svizzera (CCCPS).

Il federalismo Le crea qualche problema?
Il processo decisionale è a volte faticoso. Il federalismo ha tuttavia molti vantaggi. Se in Svizzera venisse perpetrato un attentato come quello di Parigi, potremmo contare su diverse forze speciali e non solo su quella centrale. È inoltre importante la vicinanza alla popolazione. Non credo

«Credo che la fedpol sia l'ente più appassionante della Confederazione»

nella centralizzazione nazionale della polizia poiché per la Svizzera non sarebbe né utile né realistica.

La polizia deve garantire la sicurezza anche in caso di catastrofe. Quali sono i compiti della fedpol?
Nel settore della protezione della popolazione abbiamo un mandato limitato, come ad esempio proteggere gli edifici federali e le ambasciate straniere. Ma un Cantone potrebbe avere bisogno del nostro sostegno quando si lamentano vittime straniere. In caso di attentati con conseguenze catastrofiche, assumiamo immediatamente un ruolo centrale.

Com'è organizzata la lotta contro il terrorismo?
Quando qualcuno si radicalizza, se ne accorgono dappri-

«La sfida consiste nel portare sotto lo stesso tetto la protezione delle informazioni e l'usabilità»

ma il suo entourage e gli enti comunali e cantonali. Se si radicalizza ulteriormente, la persona finisce nel mirino del Servizio delle attività informative. In caso di un comportamento penalmente perseguibile, la fedpol assume il caso e conduce le indagini di polizia. Se il sospetto è fondato, la fedpol chiede al Ministero pubblico della Confederazione di aprire un procedimento. Sull'esempio della lotta

«La lotta contro la cibercriminalità è una priorità per la fedpol»

contro il terrorismo, si riscontra che sono diversi gli attori e le autorità che devono adempiere i loro compiti. Se non collaboriamo con loro, le operazioni non funzionano. Più di due anni fa, la Svizzera ha creato la Task Force TETRA proprio a tale scopo.

E se dovesse ugualmente verificarsi un attentato terroristico?
In tal caso, la gestione degli eventi sul posto sarebbe di competenza della polizia cantonale e di quella locale. Se dovessero verificarsi contemporaneamente più eventi, la polizia cantonale potrebbe raggiungere in fretta i suoi limiti. Spetterebbe allo stato maggiore della polizia coordinare la loro collaborazione e le loro risorse. In questo stato maggiore è integrata anche la fedpol con la sua organizzazione d'intervento e con i suoi contatti internazionali.

Qual è il livello della collaborazione internazionale?
La collaborazione con l'estero è spesso decisiva. A livello bilaterale, collaboriamo con i Paesi vicini. Mi incontro ogni anno all'Aia con i capi delle polizie europee. È molto importante che le persone si conoscano bene reciprocamente. A livello multilaterale, intratteniamo una stretta collaborazione con le organizzazioni di polizia Interpol ed Europol. E come dispositivi speciali, gestiamo con la Francia e l'Italia rispettivamente a Ginevra e Chiasso due centri per la cooperazione di polizia e doganale, in cui sono rappresentati la polizia cantonale, il Corpo delle guardie di confine e fedpol.

Le minacce informatiche non conoscono confini.
La lotta contro la cybercriminalità è una priorità per la fedpol. Si distinguono due aree: la criminalità quotidiana, quasi sempre correlata con mezzi informatici, soprattutto con gli smartphone e i computer portatili, anche se non ha luogo direttamente in Internet. La seconda area sono i reati direttamente mirati ai computer e ai sistemi informatici.

Oggi si parla molto di criminalità informatica.
La criminalità si sviluppa parallelamente alla nostra quotidianità. Lavoriamo sempre più on-line, così che anche la criminalità opera sempre più in rete. La classica immagine del rapinatore con la pistola in mano e la calzamaglia in testa viene soppiantata dal criminale dietro uno schermo.

E la difesa riesce a tenere il passo?
Purtroppo siamo sempre un passo indietro. Essere tecnologicamente «up to date» è molto difficile. Per non rimanere indietro è indispensabile che le nostre basi giuridiche siano formulate in modo neutrale per quanto concerne la tecnologia.
Negli ultimi venti anni il lavoro della polizia è radicalmente cambiato. La scienza forense analizza sempre meno carta, ma sempre più dati informatici. È impegnativo filtrare tra numerosi terabyte i dati necessari al Ministero pubblico. E ogni agente di polizia dovrebbe essere in grado di esaminare uno smartphone.

E la vostra sicurezza informatica a che punto si trova?
Questo è un tema molto importante per noi, poiché abbiamo a che fare ogni giorno con dati sensibili. La sfida consiste nel garantire allo stesso tempo protezione delle informazioni e usabilità. Per la protezione dati in particolare si tratta di trovare soluzioni intelligenti che facilitino e non ostacolino il lavoro degli agenti di polizia. Dobbiamo ad esempio essere in grado di comunicare in modo mobile e criptato anche durante gli spostamenti e in qualsiasi momento della giornata.

Signora della Valle, La ringraziamo per l'intervista.

Intervistatore:
Kurt Münger
Capo Comunicazione, UFPP

Panoramica

Opportunità e rischi delle nuove tecnologie

Le nuove tecnologie cambiano sempre più la nostra quotidianità. Siamo sempre raggiungibili e connessi. Ma non è cambiato solo il modo in cui ci informiamo e comunichiamo. Possiamo programmare a distanza la lavatrice della nostra casa di vacanza oppure accedere in prima persona alla realtà virtuale. Ovviamente questi sviluppi offrono molti vantaggi e agevolazioni, ma comportano anche dei rischi, in particolare per la privacy.

I sensori, gli attuatori e la rete Internet mobile a banda larga permettono di sorvegliare e comandare a distanza gli apparecchi.

Le nuove tecnologie hanno portato a un'interconnessione globale che arriva a invadere anche la sfera privata dei cittadini.

Il progresso scientifico è inarrestabile. Mentre nel 1995 solo l'1 percento della popolazione mondiale aveva accesso ad Internet, oggi è il 40 percento, e aziende come Google e Facebook lavorano instancabilmente per portare Internet in tutte le zone remote del mondo. In Svizzera, oltre il 90 percento delle famiglie ha accesso ad Internet (per la maggior parte ad alta velocità).
Negli ultimi anni, le tecnologie si sono rapidamente diffuse e sviluppate, hanno cambiato il modo di lavorare e la vita privata e favorito nuovi approcci mentali, e non solo grazie ad Internet. Il lavoro a domicilio, l'orario di lavoro flessibile e gli spazi di lavoro informali progettati dai giganti di Internet sono solo alcuni evidenti esempi di questa nuova cultura professionale. Le nuove tecnologie hanno aperto nuove opportunità, fino allora impensabili, anche per la protezione civile e la gestione delle crisi.

Il lavoro a domicilio, l'orario di lavoro flessibile e gli spazi di lavoro informali progettati dai giganti di Internet sono solo alcuni evidenti esempi di una nuova cultura professionale.

Alle innovazioni e agli scenari di applicazione delle nuove tecnologie è associato un numero infinito di neologismi alla moda, perlopiù in inglese: «Internet of Things», «Big Data», «Contactless Payments», «Wireless-Technologie», «Cloud-Computing», «Blockchain Technologie» e «Virtual Reality», solo per citarne alcune. Le nuove tecnologie cambiano la nostra vita di tutti i giorni e possono avere effetti sia positivi che negativi.

Internet of Things

Il termine «Internet of Things» (IoT) sta a significare che utilizziamo sempre più oggetti intelligenti nella quotidianità: stampanti che ci avvisano quando sostituire la cartuccia del toner, riscaldamenti che ottimizzano da sole il loro consumo. I computer diventano sempre più piccoli, mentre le loro capacità di calcolo e di memoria aumentano e sensori come il GPS, gli accelerometri e le telecamere battono continuamente nuovi record di precisione. Tramite le ormai onnipresenti connessioni Internet senza fili e a banda larga si possono scambiare enormi volumi di dati. Ciò costituisce il presupposto per le nuove applicazioni di sorveglianza e di gestione di edifici, agglomerati urbani e impianti agricoli.

Big Data e Cloud Computing

I dati trasmessi tramite sensori IoT, «Web Traffic» (traffico Internet) o i Social network forniscono ai ricercatori e alle imprese nuove conoscenze sulla società e sull'ambiente. «Big Data» significa che abbiamo accesso a un'enorme, in passato inconcepibile, quantità di dati. Il «Cloud Computing» ci permette di elaborare queste enormi quantità di dati in centri di calcolo facilmente scalabili. La potenza di calcolo può essere affittata in modo flessibile «on-demand».

Tecnologia Blockchain

Un sistema di pagamento tradizionale presuppone un ente centrale, in genere una banca nazionale. Con l'invenzione dei Bitcoin nel 2008 è stato dimostrato per la prima volta che un sistema di pagamento elettronico può funzionare anche in modo diverso. I Bitcoin e la relativa banca dati «Blockchain» consentono di gestire in maniera decentrata processi che in precedenza erano gestiti centralmente. La «Blockchain» garantisce che i soldi vengono trasferiti correttamente e non possano essere rubati.
È interessante notare che la «Blockchain» consente molte più applicazioni che il semplice scambio di denaro. Grazie ai cosiddetti «Smart Contract» è possibile eseguire in modo decentralizzato programmi verificati e accettati a livello globale. Questi consentono ad esempio di utilizzare la «Blockchain» come istanza decisionale per la risoluzione di controversie.

Contactless Payments e Wireless Technology

In molti negozi, oggi i consumatori possono già pagare senza dover inserire la carta di credito nell'apposito lettore. Per i piccoli acquisti non devono più immettere il codice PIN. Si paga «contactless», senza contatto appunto.
Il nostro ambiente tecnico è costituito da un numero sempre minore di cavi: "Wireless LAN», Internet mobile, «Bluetooth», il caricamento di apparecchi senza l'uso di fili o l'apertura a distanza di un'autovettura sono solo al-

cuni esempi. Questo continuo sviluppo porterà a soluzioni sempre più semplici ed eleganti.

Virtual Reality

I display moderni hanno una tale densità di pixel che l'occhio non è più in grado di riconoscere i singoli pixel. Grazie a questo progresso tecnico è ad esempio possibile simulare un effetto 3D molto realistico posizionando con precisione un display per ciascun occhio. Con la «Virtual Reality» si definiscono di regola gli occhiali che riproducono contenuti 3D, consentendo una full immersion. Insieme a un'audio realistica, si raggiunge così un'impressionante sensazione di coinvolgimento diretto. Le soluzioni attuali possono ancora essere migliorate, ma va da sé che queste tecnologie s'imporranno in numerosi settori della nostra vita, dal gioco alla medicina.

Motori di ricerca

I motori di ricerca forniscono un portale per accedere al contenuto inesauribile del web di tutto il mondo. Una ricerca su Internet inizia solitamente con uno o più termini che l'utente digita nel motore di ricerca e che produce tutta una serie di risultati. Selezionando una pagina tra quelle proposte, il motore di ricerca riceve un segnale chiaro sui siti che sono rilevanti per una determinata ricerca. Visto che la maggior parte dei motori di ricerca sono centralizzati e controllati da poche aziende, questa elaborazione delle informazioni pone problemi per la privacy e la neutralità di Internet.

Social Bots

Grazie al costante miglioramento del riconoscimento vocale e dell'intelligenza artificiale, i cosiddetti «Social Bots» possono fungere da assistenti. Che si tratti di un assistente digitale sul nostro smartphone, di un dispositivo installato in modo permanente in casa nostra o di un umanoide mobile: questi assistenti captano incessantemente i rumori dell'ambiente e sono in grado di adattarsi alle nostre abitudini. I vantaggi di queste tecnologie sono evidenti: più compiti vengono assolti dagli assistenti digitali, meglio possiamo concentrarci sulle attività essenziali e interessanti.

Troppa trasparenza

Tutte le suddette tecnologie possono rendere più facile la nostra vita, ma celano anche nuovi rischi che sono difficili da controllare o evitare.
Siamo ormai cyber-uomini: ogni giorno comunichiamo, lavoriamo e apprendiamo tramite il computer e lo smartphone, lasciando un'impronta digitale indelebile. Questa ricopre due dimensioni: la diffusione volontaria della propria immagine, e un comportamento implicitamente mediato. Diffondiamo deliberatamente la nostra auto-immagine ideale per esempio sui social network (Facebook, Linkedin, WhatsApp, ecc.). E trasmettiamo implicitamente la seconda dimensione, ossia il nostro comportamento privato che le grandi società di Internet possono facilmente analizzare e utilizzare per i loro fini. Le nostre caselle postali e agende basate su cloud, i supporti di memorizzazione remota, le nostre abitudini di navigazione Internet e i termini utilizzati nei motori ricerca sono importanti fonti d'informazione. I nostri smartphone, che utilizziamo frequentemente e portiamo sempre con noi, hanno ormai la potenza di calcolo dei computer di qualche anno fa e offrono microfono, GPS, fotocamera e accelerometri. Molti di questi dati sono trasmessi a terzi per analisi. Lunghe ricerche hanno dimostrato che è estremamente difficile proteggere la privacy degli utenti.

Siamo ormai cyber-uomini.

In seguito alla digitalizzazione, i sistemi basati sull'informatica hanno aumentato il potere decisionale su dati e informazioni che ci riguardano. Questi sistemi diventano quindi un bersaglio di attacchi cibernetici e la sicurezza informatica assume un ruolo sempre più importante nella nostra società.

Questioni urgenti

Anche se le nuove tecnologie si sviluppano sempre più velocemente e noi esseri umani siamo ormai strettamente legati alla tecnologia, il legame tra noi e le macchine è ancora molto limitato. Con i nostri sensi, che sia la vista o l'udito, siamo in grado di captare una notevole gamma di informazioni: l'interfaccia dalla macchina all'uomo permette un ricco flusso di informazioni. Al contrario, la trasmissione da uomo a macchina è limitata soprattutto ai comandi vocali, alla digitazione sulla tastiera, vale a dire che si possono trasmettere molto meno informazioni. Quando il flusso di informazioni dall'uomo alla macchina sarà più efficiente, anche le applicazioni informatiche diventeranno molto più efficienti. Ma di conseguenza anche le questioni legate alla sicurezza e alla privacy diventeranno più urgenti.

Quando il flusso di informazioni dall'uomo alla macchina sarà più efficiente, anche le applicazioni informatiche diventeranno molto più efficienti.

Arthur Gervais
Assistente scientifico presso il PF di Zurigo

Centrale d'annuncio MELANI

Sulle tracce dei truffatori in rete

I furti di dati, gli attacchi degli hacker e i tentativi d'estorsione rendono insicura la comunità informatica. In Svizzera, la centrale d'annuncio MELANI provvede a migliorare continuamente la protezione e la lotta contro i crimini informatici.

Non si sa con esattezza quando e dove sia nato e chi l'abbia lanciato, ma trattandosi di una svolta storica, come data di nascita ufficiale del World Wide Web è stata fissata il 6 agosto 1991. Venticinque anni e mezzo fa, il sito web dell'Istituto di ricerca nucleare CERN di Ginevra è stato infatti il primo ente a connettersi alla rete. Internet, che ha reso possibile la navigazione, è però più vecchio. Nel 1977 si è riusciti per la prima volta a collegare tra loro reti informatiche. Quest'anno lo scambio di dati on-line in tutto il mondo compie quindi 40 anni.

L'Europol mette in guardia contro la crescente aggressività della criminalità informatica organizzata.

La ricorrenza passa però in secondo piano, dato che fanno più notizia gli attacchi degli hacker contro computer governativi o i casi d'estorsione in rete. I temi «Hacking-Reality» e «Computer Security» hanno dominato l'agenda del raduno del Chaos Computer Club, tenutosi ad Amburgo alla fine del 2016. Ed Europol mette in guardia contro la «crescente aggressività della criminalità informatica organizzata». In certi Paesi, la criminalità informatica ha addirittura superato quella tradizionale.

Centrale d'annuncio della Confederazione

È impressionante come la «rete», nonostante la sua giovane età, sia diventata indispensabile per la vita quotidiana privata, pubblica ed economica. Negli ultimi tempi sono però aumentate le notizie che pure la fiducia nel mondo dell'informatica virtuale si sia incrinata in poco tempo. Non solo gli esperti d'informatica, ma anche i ricercatori dei trend affermano che la comunicazione digitale sia sull'orlo di una crisi. Il timore di una guerra cibernetica o di una paralisi dei sistemi da parte di hacker criminali ha ormai preso il posto della fiducia illimitata in Internet. Lo scetticismo, generato dall'evidenza che la rete è anche una zona infestata da criminali, cresce ovunque venga utilizzata almeno una postazione di lavoro per agevolare la vita privata o professionale.

Da ormai dodici anni, MELANI riferisce ogni sei mesi sulla situazione dei pericoli.

Non sorprende quindi che anche un professionista di Internet come Max Klaus preferisca spegnere la connessione wireless di casa. D'altra parte è confortante sapere che egli dedichi il suo lavoro per conto della Confederazione esclusivamente alla migliore protezione possibile delle infrastrutture critiche contro gli hacker. Klaus è infatti vicecapo della Centrale d'annuncio e d'analisi per la sicurezza dell'informazione MELANI, che sorveglia la situazione della sicurezza informatica interna e reagisce rapidamente a minacce quali il furto di password, i virus o i malware. L'organo direzione informatica della Confederazione (ODIC) e il Servizio delle attività informative della Confederazione (SIC) hanno istituito questo organo affinché specialisti molto qualificati sorveglino le crescenti minacce di Internet e possano mettere in guardia le potenziali vittime, tra cui gli organi amministrativi e le imprese, da eventuali attacchi informatici in Svizzera. Da ormai dodici anni, MELANI riferisce ogni sei mesi sulla situazione dei pericoli in modo comprensibile per tutti gli utenti di Internet, così da migliorare la sensibilizzazione.

Lo scopo principale è l'allerta precoce

I rapporti interni di uffici o aziende private sono in gran parte ostici e difficili da leggere. I rapporti semestrali di MELANI contengono invece temi appassionanti, come i film sulla criminalità informatica o i romanzi di spionaggio. All'inizio del 2016 si è diffusa pubblicamente la notizia che la fabbrica d'armi RUAG è stata vittima di spionaggio digitale. Alcuni mesi prima, alcuni sconosciuti erano infatti riusciti a infilare un malware nella rete interna dei dati. Il Ministero pubblico della Confederazione sta valutando i danni e indagando sui colpevoli in base alle informazioni raccolte da MELANI. Poco tempo dopo, in

Della sicurezza in Internet dovrebbero occuparsi non solo gli specialisti informatici. MELANI riferisce ogni sei mesi sulla situazione delle minacce, in modo comprensibile per tutti gli utenti.

primavera, migliaia di indirizzi e-mail sono stati rubati dalle banche dati di partiti politici. E l'anno scorso sono state messe in circolazione delle e-mail in cui l'Ufficio federale della protezione della popolazione figurava come falso mittente, con un allegato fasullo su «acqua potabile contaminata» che serviva solo da esca per installare un malware sui computer.

Ogni anno si registrano numerosi attacchi informatici o di phishing di lieve fino a grave entità o addirittura di tipo intimidatorio. Gli scopi principali della centrale d'annuncio creata dalla Confederazione sono l'allerta precoce e la prevenzione. Tra le aziende collegate a MELANI vengono scambiate informazioni riservate. E, se necessario, esse vengono assistite anche nella lotta contro simili attacchi.

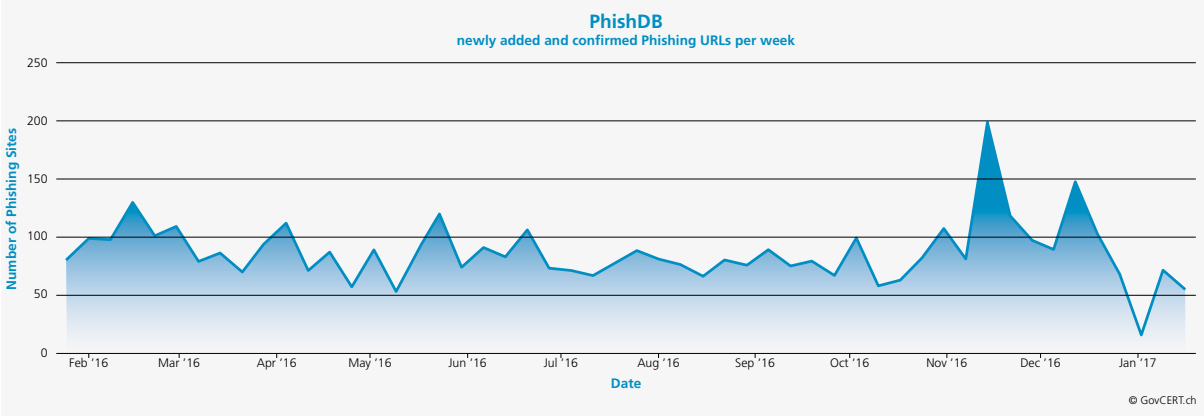
Oltre alle banche e alle imprese di telecomunicazioni, soprattutto le aziende elettriche sono interessate a tali informazioni. E ultimamente anche gli ospedali finiscono nel mirino della cybercriminalità, poiché la loro infrastruttura elettronica molto vulnerabile è particolarmente esposta ai tentativi d'estorsione. «L'obiettivo della maggior parte degli attacchi informatici è quello di appropriarsi di più denaro possibile con il minimo sforzo», riassume Max Klaus.

La cooperazione è benvenuta

Rispetto ad altri Paesi, la Svizzera non prevede alcun obbligo di notifica. Gli attacchi di hacking e i tentativi d'estorsione virtuali vengono quindi comunicati volontariamente dalle persone colpite. Si collabora volentieri con l'ente statale e la fiducia reciproca migliora il dispositivo di sicurezza esistente. L'anno scorso, sono state inoltrate a MELANI ben 6'000 e-mail e combinazioni di password rubate dagli hacker. Il 16 marzo 2016, MELANI ha quindi messo in rete un check accessibile al pubblico per la verifica di tutti i possibili indirizzi di posta elettronica. Questa volta il team di MELANI si è deciso per l'apertura al grande pubblico. Per altri tipi di minacce si procede invece con maggiore discrezione. «Prendiamo accordi di segretezza con le imprese collegate a MELANI e non possiamo quindi pubblicare tutto», precisa Klaus.

Ultimamente anche gli ospedali finiscono nel mirino della cybercriminalità, poiché la loro infrastruttura elettronica molto vulnerabile è particolarmente esposta ai tentativi d'estorsione.

Inizialmente, gli utenti sono stati messi in guardia in particolare contro i virus e i worm. Venivano infatti attaccati



Nel periodo degli acquisti natalizi si assiste a un aumento degli attacchi phishing.

soprattutto portali di e-banking per poter accedere a conti, codici di carte di credito o password. Nel frattempo, l'estorsione è diventato il business più attrattivo per i criminali informatici. Essi rubano informazioni sensibili ad aziende ed enti pubblici oppure ne bloccano l'uso per chiedere un riscatto. Simili attacchi vengono perpetrati contro il settore finanziario, gli shop online e, come detto, anche contro gli ospedali.

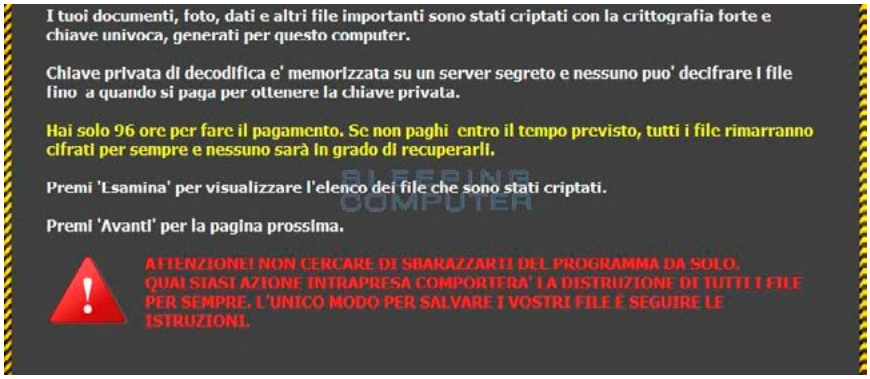
La centrale d'annuncio MELANI intende però anche sensibilizzare e a tal fine organizza, insieme con molte altre organizzazioni, una giornata di «Ransomware-Awareness».

I collaboratori di MELANI non sono né spie né poliziotti. Non possono intervenire di loro iniziativa, ma vengono informati più di chiunque altro sulle minacce informatiche in Svizzera e all'estero. Numerosi enti informatici nazionali o stranieri fanno parte di questa rete.

Sensibilizzare e apprendere

Quale vice capo della centrale d'annuncio, Max Klaus è un professionista molto intervistato dai media per le inchieste su una maggiore sicurezza informatica. Ma non si negano informazioni neppure su MELANI. Gli uffici di Klaus e dei suoi colleghi si trovano nel centro di Berna e sono circondati da altri organi amministrativi federali. L'accesso ai visitatori annunciati viene protetto con le solite precauzioni. Ogni film mostrerebbe entrate con chiuse o una perquisizione per ritirare i telefonini, ma queste precauzioni non sono necessarie in Schwarztorstrasse 51. «Chiuderci a riccio verso l'esterno sarebbe controproducente», afferma Klaus, «poiché senza l'aiuto della popolazione e del settore privato non avremmo alcuna chance». Il lavoro viene inoltre diviso: MELANI non può dare la caccia ai criminali di Internet e deve attenersi scrupolosamente alla protezione dei dati e ad altre leggi. La responsabilità della sicurezza informatica spetta esclusivamente agli utenti. La maggior parte delle grandi aziende ha quindi assunto specialisti propri. E anche la polizia dispone nel frattempo di specialisti responsabili del perseguimento penale dei criminali informatici.

Gli specialisti di MELANI non stanno però solo ad aspettare. I software sconosciuti vengono analizzati internamente e i risultati messi a disposizione di partner scelti. Sappiamo che è difficile che un attacco sia uguale a quello precedente. Ma «più cerchiamo di individuare eventuali vulnerabilità per adottare le contromisure necessarie, più rendiamo difficile il lavoro agli hacker», riassume Klaus. La centrale d'annuncio MELANI intende però anche sensibilizzare e a tal fine organizza, insieme con molte altre organizzazioni, una giornata di «Ransomware-Awareness». I collaboratori che inviano e ricevono e-mail, visitano siti web, si registrano in tali siti o scaricano contenuti comportano il grosso rischio che l'accesso ai dati interni possa essere violato da criminali informatici. «Possiamo continuare a rallegrarci per le numerose innovazioni; ma dobbiamo anche accettare il fatto che bisogna proteggersi nel miglior modo possibile contro le minacce», conclude Max Klaus.



I trojan crittografici (ransomware) sono malware che cifrano i file sul computer della vittima e li rendono inutilizzabili.

Paul Knüsel
Giornalista scientifico

Strategia nazionale per la protezione della Svizzera contro i cyber-rischi (SNPC)

Sollecitati anche i gestori delle infrastrutture critiche

La digitalizzazione e l'interconnessione dell'economia e della società implicano numerosi rischi. Soprattutto gli attacchi cibernetici possono avere gravi conseguenze per infrastrutture critiche come le aziende elettriche e dell'acqua potabile, la sanità o il settore finanziario. La Confederazione s'impegna a riconoscere e a ridurre tali rischi.

Settori critici (SC)	Coordinamento misure SNPC	Sottosettori critici (SSC)
Autorità	UFPP	Rappresentanze diplomatiche e sedi di organizzazioni internazionali
	UFPP	Ricerca e insegnamento
	UFPP	Beni culturali
	UFPP	Parlamento, governo, giustizia, amministrazione
Energia	UFAE	Approvvigionamento di gas naturale
	UFAE	Approvvigionamento di petrolio
	UFAE	Approvvigionamento di energia elettrica
Smaltimento	UFPP	Rifiuti
	UFAE	Acque di scarico
Finanze	UFPP	Banche
	UFPP	Assicurazioni
Sanità pubblica	UFPP	Cure mediche e ospedaliere
	UFPP	Laboratori
Industria	UFAE	Industrie chimiche e farmaceutiche
	UFAE	Industrie elettro-meccaniche e metallurgiche
Informazione e comunicazione	UFAE	Tecnologie dell'informazione
	UFPP	Media
	UFPP	Traffico postale
	UFAE	Telecomunicazioni
Alimentazione	UFAE	Approvvigionamento alimentare
	UFAE	Approvvigionamento idrico
Sicurezza pubblica	UFPP	Esercito
	UFPP	Organizzazioni di primo intervento (polizia, pompieri, sanità)
	UFPP	Protezione civile
Trasporti	UFAE	Traffico aereo
	UFAE	Traffico ferroviario
	UFAE	Traffico navale
	UFAE	Traffico stradale

I sottosettori sono critici poiché

- i loro operatori forniscono prestazioni importanti (e vitali) per la popolazione e l'economia;
- eventuali perturbazioni o interruzioni delle loro prestazioni hanno gravi conseguenze per la popolazione o l'economia;
- rappresentano potenziali pericoli per le persone, gli animali e l'ambiente.

Criticità normale | Criticità elevata | Criticità molto elevata

Secondo la strategia PIC, le infrastrutture critiche vengono attribuite a settori e sottosettori. In totale esistono 10 settori critici e 28 sottosettori critici.

In Internet si celano molti pericoli invisibili. Vi rientrano per esempio gli attacchi cibernetici alla rete elettrica, con conseguenze molto pesanti: paralisi dei mezzi di trasporto pubblici, interruzione della telefonia e di altri mezzi di comunicazione, chiusura di negozi e banche, arresto dei riscaldamenti e impossibilità di pompare l'acqua potabile nelle abitazioni. Gli attacchi cibernetici potrebbero anche mettere in pericolo vite umane quando vengono manipolate apparecchiature mediche di ospedali o informazioni sui pazienti.

È importante essere consapevoli dei pericoli del cyber-spazio e migliorare la resilienza (resistenza e capacità di rigenerazione) delle infrastrutture critiche con misure mirate.

È importante essere consapevoli dei pericoli del cyber-spazio e migliorare la resilienza (resistenza e capacità di rigenerazione) delle infrastrutture critiche con misure mirate. Un ruolo centrale l'assume la protezione delle infrastrutture di informazione e comunicazione. Nel giugno 2012, il Consiglio federale ha approvato la Strategia nazionale per la protezione della Svizzera contro i cyber-rischi (SNPC) e incaricato vari enti federali di attuarle insieme ai partner delle autorità, dell'economia e della società. La strategia persegue i seguenti obiettivi prioritari:

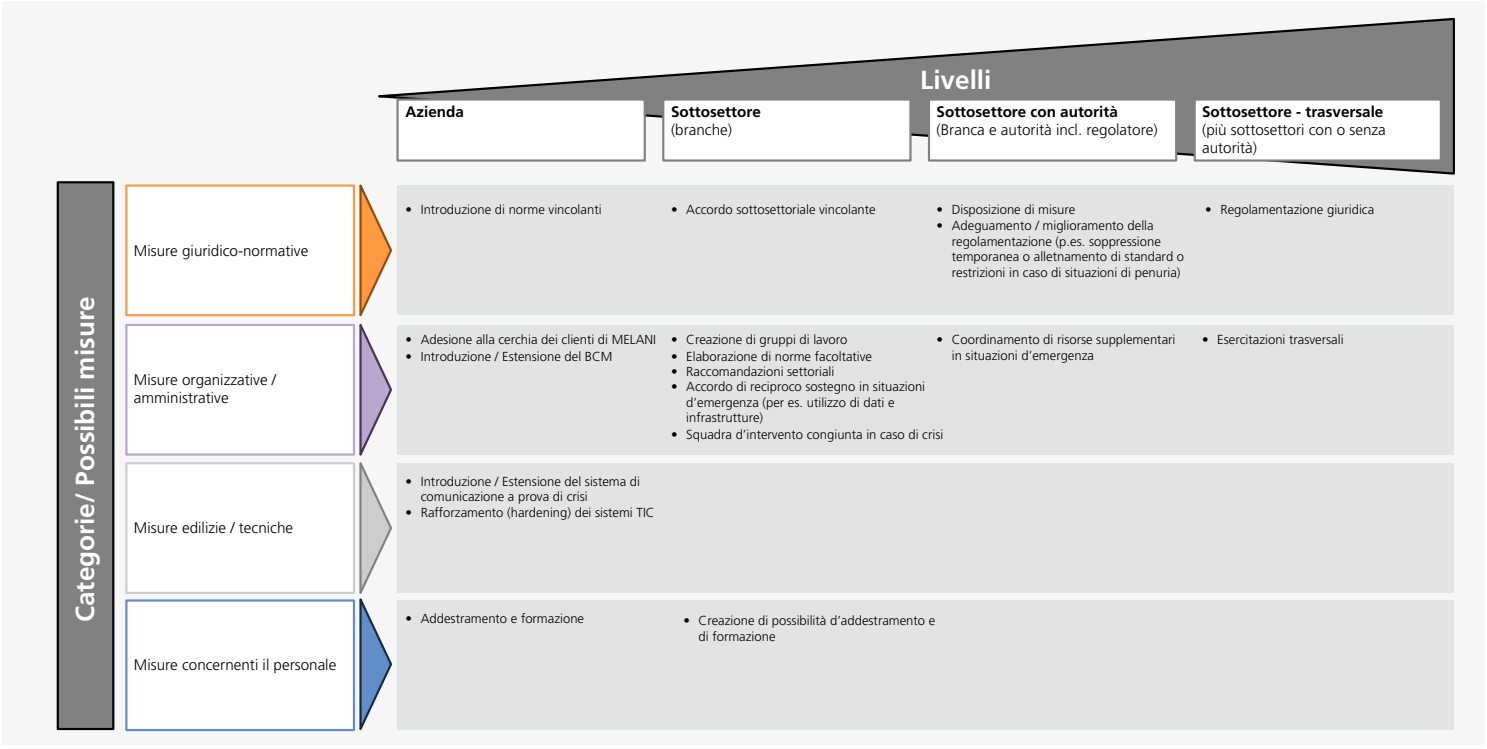
– individuazione precoce delle minacce e dei pericoli nel cyberspazio;
– incremento della resistenza delle infrastrutture critiche agli attacchi;
– riduzione efficace dei cyber-rischi, segnatamente per quanto concerne la cybercriminalità, lo spionaggio informatico e il sabotaggio informatico.

Due uffici, due misure

Per raggiungere questi obiettivi, sono state definite varie misure, alcune delle quali riguardano le infrastrutture critiche. Il Consiglio federale ha incaricato l'Ufficio federale per l'approvvigionamento economico del Paese (UFAE) e l'Ufficio federale della protezione della popolazione (UFPP) di attuare due misure della SNPC. Da un lato si tratta di accertare se esistono rischi che potrebbero portare a gravi perturbazioni o interruzioni di servizi e beni essenziali (ad esempio un arresto su larga scala della sanità o dell'approvvigionamento di elettricità). D'altra parte si tratta di elaborare, sulla base dei risultati di questi accertamenti, ulteriori misure per migliorare la resilienza delle infrastrutture critiche. I lavori saranno incentrati sulle tecnologie d'informazione e di comunicazione (TIC) e sui cyber-rischi.
Di fondamentale importanza sono il coinvolgimento tempestivo e la stretta collaborazione di autorità, gestori delle infrastrutture critiche, associazioni e altri enti. È inoltre importante che le competenze e le responsabilità dei partner rimangano garantite. In particolare, le autorità specializzate devono mantenere la competenza per le regolamentazioni e le normative.

Combinare la SPNC con la strategia nazionale PIC

Le infrastrutture critiche sono suddivise in 28 settori (sottosettori). Uno spettro da esaminare piuttosto ampio



Le misure per migliorare la resilienza delle infrastrutture critiche possono essere adottate a diversi livelli (asse X) e attribuite a diverse categorie (asse y).

quindi. L'UFAE e l'UFPP coordinano i lavori nel quadro della SNPC per 14 sottosettori critici ciascuno (vedi figura 1).
Visto che oggi la maggior parte delle interruzioni non sono causate da attacchi cibernetici, è importante prendere in considerazione altri rischi rilevanti per la protezione delle infrastrutture critiche. L'UFPP adotta pertanto le misure della strategia SPNC in combinazione con la Strategia nazionale per la protezione delle infrastrutture critiche (PIC), che è stata pure approvata dal Consiglio federale nel giugno del 2012. In questo contesto, l'UFPP sta esaminando se oltre ai cyber-rischi, anche un blackout su vasta scala, un grave terremoto o un attacco mirato potrebbe perturbare gravemente i sottosettori critici.
Dal punto di vista metodico, la procedura di verifica e miglioramento della resilienza dei sottosettori critici aderisce in gran parte alle linee direttive PIC, in modo da garantire che i lavori siano congruenti. Le linee direttive PIC si basano su concetti consolidati della gestione dei rischi, delle crisi e della continuità operativa (BCM). Al contrario dei sistemi manageriali, non si pone l'accento sul benessere dell'azienda o delle organizzazioni, bensì su quello della popolazione e delle sue basi esistenziali.

Individuare i punti deboli e i rischi

In una prima fase si valuta la vulnerabilità dei singoli sottosettori alle perturbazioni e interruzioni. A questo scopo si analizza innanzitutto la struttura del sottosettore. I partner sono in grado di sostenersi a vicenda (per es. assunzione di pazienti da parte di un'altra struttura medica)? Per un certo servizio o prodotto sono disponibili diversi fornitori o ne esiste uno solo? I partner sono ben distribuiti su tutto il territorio nazionale o sono concentrati in pochi luoghi o addirittura in un unico luogo? Oltre alla struttura del sottosettore, si valuta la dipendenza dei partner da risorse importanti come la forza lavoro, l'energia, l'ICT, il materiale, le attrezzature, le infrastrutture e la logistica.
In un secondo tempo si valutano, sulla base dei risultati, i potenziali danni causati dai pericoli rilevanti (attacco cibernetico, arresto di ICT, interruzione di corrente, ecc.) e i rischi correlati per la popolazione e l'economia.

Migliorare la resilienza

Partendo dai punti deboli e dai rischi individuati vengono elaborate le misure per migliorare la resilienza. L'approccio basato sui rischi permette di definire misure poco dispendiose, ma comunque molto efficaci per ridurre i rischi. L'obiettivo non è però quello di ridurre qualsiasi tipo di rischio e vulnerabilità, poiché questo tipo di approccio comporterebbe costi sproporzionati.
Le misure possono essere adottate a vari livelli (azienda, branca, più branche con e senza la collaborazione delle autorità) ed assegnate a diverse categorie (misure giuridico-normative, misure organizzative/amministrative, misure edilizie/tecniche, misure concernenti il personale) (vedi figura 2). Per la loro attuazione si applica il principio della sussidiarietà: lo Stato interviene con supporti e disciplinamenti solo laddove le aziende e le organizzazioni non vogliono o non possono migliorare da sole la loro resilienza.

Già prese numerose precauzioni

I rapporti sulle analisi dei rischi e sulle misure dedotte dovranno essere disponibili entro la fine del 2017 per tutti i 28 sottosettori. I lavori finora svolti hanno dimostrato che gran parte dei sottosettori esaminati hanno già adottato numerose misure per prevenire interruzioni e perturbazioni e per ridurre al minimo la durata e le conseguenze in caso d'evento. Tuttavia, vi sono settori che richiedono ulteriori interventi e per i quali potrebbero essere identificate misure volte a migliorare la resilienza.

L'approccio basato sui rischi permette di definire misure poco dispendiose, ma comunque molto efficaci per ridurre i rischi.

Tra queste rientra ad esempio l'inserimento di operatori rilevanti nella cerchia chiusa dei clienti di MELANI (centrale d'annuncio e d'analisi per la sicurezza dell'informazione). Questa cerchia comprende gestori scelti delle infrastrutture critiche, e il compito di MELANI è quello di proteggerli contro i cyber-rischi. Anche la formazione e la sensibilizzazione dei collaboratori contro i pericoli cibernetici o l'elaborazione di piani d'emergenza che permettono di fornire prestazioni preziose in caso d'evento sono annoverabili tra le misure da individuare e mettere in atto.
I rapporti che vengono elaborati insieme alle autorità competenti, alle associazioni e ai gestori delle infrastrutture critiche non sono accessibili al vasto pubblico. Per garantire un'informazione su più ampia scala, per ogni sottosettore viene redatta una scheda informativa che spiega quali sono le prestazioni fornite, le parti coinvolte nonché i punti deboli e i rischi identificati. Queste schede informative sono disponibili nel sito web dell'Organo direzione informatica della Confederazione (ODIC).

Angelika P. Bischof
Collaboratrice scientifica Protezione delle infrastrutture d'informazione critiche, UFPP

Per maggiori informazioni:
www.infraprotection.ch
www.isb.admin.ch

Protezione delle infrastrutture critiche (PIC)

Cyber-rischi rilevanti per la protezione della popolazione

Un attacco cibernetico potrebbe colpire la capacità operativa della protezione della popolazione? Quali misure sono già state adottate contro tali minacce? E quali sono le sfide e le opportunità del futuro? Con l'analisi dei rischi e delle vulnerabilità, l'Ufficio federale della protezione della popolazione (UFPP) cerca di rispondere a tutte queste domande.

Nell'ambito della strategia nazionale per la protezione delle infrastrutture critiche (PIC) e della strategia nazionale per la protezione della Svizzera contro i cyber-rischi (SNPC) viene attualmente valutata e migliorata la resilienza (capacità di resistenza e di rigenerazione) delle infrastrutture critiche. Tra le infrastrutture critiche rientrano anche i partner della protezione della popolazione. In collaborazione con le autorità, le organizzazioni di pronto intervento e la protezione civile, sono stati quindi esaminati i rischi di perturbazione per la polizia, i pompieri, i servizi di soccorso e la protezione civile. Sono stati inclusi anche importanti compiti amministrativi, come ad esempio nel settore dell'allerta e dell'allarme.
Ci si è posti soprattutto la domanda se le principali prestazioni dei settori succitati possano essere gravemente perturbati su larga scala. Oltre ai cyber-rischi, sono state esaminate altre minacce che potrebbero causare simili perturbazioni (blackout, pericoli naturali, ecc.).

I pompieri e i militi della protezione civile vengono solitamente mobilitati tramite telefono o cercapersone, che sono purtroppo molto dipendenti dalla rete pubblica delle telecomunicazioni.

In occasione di diversi workshop e incontri sono stati inizialmente analizzati i compiti principali delle organizzazioni d'intervento in caso di sinistri ordinari, catastrofi e situazioni d'emergenza. L'analisi ha tenuto conto anche di attività preparatorie e preventive come la manutenzione dei rifugi o l'impiego di sistemi di misurazione e di detezione precoce. In seguito sono stati identificati i pericoli che potrebbero perturbare questi compiti.
Gli esperti hanno stimato l'entità dei danni che potrebbero subire la popolazione e l'economia nel caso che le organizzazioni partner non fossero più in grado di adempiere i loro compiti. L'obiettivo era anche quello di individuare i punti deboli che rendono particolarmente pericolosi gli attacchi cibernetici. Le possibili conseguenze degli attacchi cibernetici sono molteplici: potrebbero limitare la comunicazione, distruggere informazioni digitali o manipolare dati importanti e sensibili.

Mobilitazione delle forze d'intervento

Le vulnerabilità, ma anche le misure si possono illustrare facendo riferimento ai tre temi: mobilitazione delle forze d'intervento, ricezione delle chiamate d'emergenza e comunicazione trasversale in caso di catastrofe o di situazione d'emergenza.
Visto che un sinistro ordinario o una catastrofe possono verificarsi in qualsiasi momento, la prontezza operativa delle organizzazioni partner della protezione della popolazione deve essere elevata. La maggioranza dei pompieri e dei militi della protezione civile adempiono i loro compiti in una funzione di milizia e devono essere in grado di spostarsi in pochi minuti da casa o dal posto lavoro al luogo d'intervento. Essi vengono solitamente mobilitati tramite telefono o cercapersone, molto dipendenti dalla rete pubblica delle telecomunicazioni che potrebbe crollare a causa di un blackout.
Tutti i cantoni amministrano ora i dati personali dei militi della protezione civile con il sistema d'informazione sul

In Svizzera vi sono circa 170 centrali d'emergenza (nell'immagine la centrale operativa 114/118 della sezione Protezione & Salvataggio di Zurigo). Quando una centrale va fuori uso, il router dinamico devia la chiamata d'emergenza verso un'altra centrale.

personale dell'esercito (PISA). L'utilizzo di un sistema centralizzato offre molte possibilità, ma comporta anche dei rischi. Le banche dati comprendono, tra l'altro, le strutture di protezione civile, i dati di contatto e le conoscenze dei militi della PCi. La disponibilità di PISA acquisirà a medio termine importanza per la mobilitazione dei militi, anche se l'allarme e le convocazioni d'urgenza continuano ad essere attivate dai sistemi dei Cantoni o delle organizzazioni di protezione civile. Nell'ambito della pianificazione degli imprevisti si tratta quindi di mettere a punto una mobilitazione alternativa delle forze d'intervento.

Chiamate d'emergenza e comunicazione a banda larga

Le organizzazioni di pronto intervento vengono generalmente allertate tramite i numeri d'emergenza già esistenti 112, 117, 118 e 144 o tramite gli impianti antincendio o d'allarme automatici. In Svizzera vi sono circa 170 centrali d'emergenza per i pompieri, la polizia e i servizi sanitari e di soccorso. Ogni centrale è responsabile per una determinata area geografica. Chi ha bisogno di aiuto, contatta la centrale utilizzando le reti pubbliche delle telecomunicazioni. Nelle centrali d'emergenza e d'intervento vengono impiegate diverse tecnologie: telefonia, radiocomunicazione mobile e sistemi di notifica di messaggi scritti, ma anche la rete radio nazionale di sicurezza Polycom. Sistemi integrati riuniscono tutte queste tecnologie e le gestiscono su un'unica interfaccia.

Con la crescente digitalizzazione e centralizzazione cresce anche il pericolo di nuove vulnerabilità.

In caso d'evento, è importante che le informazioni ricevute vengano trasmesse il più presto possibile alle forze d'intervento in modo che queste possano raggiungere il luogo del sinistro in pochi minuti. Quando una centrale va fuori uso, il router dinamico devia la chiamata d'emergenza verso un'altra centrale. Se a subire l'arresto è una grande centrale, le altre centrali potrebbero essere sovraccaricate da un forte aumento di chiamate. Problemi potrebbero insorgere anche quando sono necessarie deviazioni oltre i confini linguistici.
La rete radio di sicurezza Polycom garantisce la comunicazione vocale tra le organizzazioni partner e gli organi di

La rete radio di sicurezza funziona anche quando crolla la rete di comunicazione pubblica.

crisi anche quando crolla la rete di comunicazione pubblica. La protezione della popolazione necessita inoltre di una comunicazione a banda larga per lo scambio di dati. Questa viene ad esempio utilizzata per scambiarsi previsioni meteorologiche in caso d'alluvione o calcoli della direzione del vento in caso di fughe radioattive.

Singole organizzazioni in pericolo

Secondo le analisi dei rischi e delle vulnerabilità, gli attacchi cibernetici costituiscono un grosso rischio per singole organizzazioni di protezione civile, corpi della polizia cantonale o centrali per chiamate d'emergenza. Se le forze di soccorso e d'intervento giungono troppo tardi sul luogo del sinistro, ne potrebbero conseguire gravi danni materiali e persino danni a persone già nel caso di sinistri ordinari come incendi o incidenti.

È invece quasi impossibile perturbare in modo mirato la capacità operativa dell'intera protezione della popolazione con un attacco informatico:

- Una perturbazione può causare danni gravi e/o su scala nazionale alla popolazione e alle sue basi vitali solo se si verifica in concomitanza con una catastrofe o una situazione d'emergenza.
- In molti cantoni, le singole organizzazioni di protezione civile e di pronto intervento mobilitano direttamente le forze d'intervento; una perturbazione simultanea di più unità organizzative è quindi improbabile.
- Nella protezione civile, la separazione dell'amministrazione dei dati dei militi della protezione civile (PISA) e dei sistemi di convocazione rende molto difficile una distruzione o una manipolazione dei dati.
- Polycom permette una comunicazione vocale protetta e trasversale tra le organizzazioni. La pianificazione degli imprevisti prevede inoltre misure come l'allestimento di liste di contatto in forma cartacea.
- La maggior parte degli interventi richiedono pochi mezzi sul posto. Quando la rete di trasmissione principale crolla, rimane possibile la radiocomunicazione. Con la crescente digitalizzazione e centralizzazione cresce anche il pericolo di nuove vulnerabilità.

Sistemi minacciati a livello nazionale

La Confederazione e i Cantoni stanno già facendo grandi sforzi per ridurre i cyber-rischi. Dalle analisi di tutti i sottosettori critici sono stati dedotti diversi campi d'azione e diverse misure per migliorare la loro resilienza. Vi rientrano in particolare lo scambio di informazioni tra le organizzazioni e gli enti specializzati, la loro sensibilizzazione, l'offerta di corsi e l'adozione di misure di sicurezza edili e tecniche. Si propone ad esempio la costruzione di un'ubicazione alternativa per il centro di calcolo o l'esecuzione regolare di backup dei software e delle banche dati. Attuare queste misure spetta alle rispettive organizzazioni e ai rispettivi enti.

Per la PIC e la SNPC è molto importante disporre di una rete di comunicazione fail-safe come la Rete di dati sicura (RDS) attualmente al vaglio dell'UFPP. Alla RDS verranno allacciati la Confederazione, i Cantoni e i gestori delle infrastrutture critiche. Il Consiglio federale ha incaricato il Dipartimento federale della difesa, della protezione civile e dello sport (DDPS) di fare un inventario dettagliato di tutti i sistemi di allarme, di informazione e di comunicazione che sono rilevanti per la protezione della popolazione, in modo che possa decidere come procedere.

Mentre alcuni piani e provvedimenti, come ad esempio la conservazione di liste cartacee di contatti, sono facili da mettere in atto, altri richiedono grossi investimenti. Considerati gli ingenti danni sociali ed economici che potrebbero causare gli attacchi cibernetici, vale comunque la pena investire nel sistema di comunicazione protetto Polycom o in una rete di dati sicura.

Giorgio Ravioli
Collaboratore scientifico Protezione delle infrastrutture critiche, UFPP

Per maggiori informazioni:
www.infraprotection.ch
www.isb.admin.ch

Conferenza internazionale ad Abu Dhabi

Iniziativa a favore della protezione dei beni culturali

I beni culturali minacciati da un conflitto armato devono essere meglio protetti. A tal fine potranno essere temporaneamente trasferiti in Paesi sicuri. In occasione di una conferenza internazionale, cinquanta Stati hanno quindi deciso di creare un nuovo fondo a tale scopo. Essendo il primo Stato ad avere realizzato un deposito protetto, la Svizzera assume un ruolo pionieristico.

Per iniziativa e sotto la direzione di Abu Dhabi (Emirati Arabi) e della Francia, il 2 e 3 dicembre 2016 si è tenuta ad Abu Dhabi la prima conferenza internazionale sulla conservazione sicura di beni culturali provenienti da zone di conflitto. I rappresentanti di cinquanta Paesi e di varie organizzazioni internazionali ed istituzioni private hanno approvato la dichiarazione di Abu Dhabi.
I firmatari vi espongono, in particolare, la loro intenzione di creare un fondo internazionale per la protezione dei beni culturali minacciati da conflitti armati. Tale fondo servirà a finanziare le misure di protezione preventive, nelle situazioni d'emergenza acute, nella lotta contro il traffico illecito di beni culturali e per il restauro dei beni culturali danneggiati. È inoltre prevista la creazione di una rete internazionale di depositi protetti per la custodia temporanea dei beni culturali minacciati.

Forte impegno della Svizzera

Su invito degli organizzatori, l'Ufficio federale della protezione della popolazione (UFPP) ha presentato ad Abu Dhabi i principali traguardi raggiunti dalla protezione dei beni culturali in Svizzera. Con la revisione totale della legge sulla protezione dei beni culturali (LPBC), nel 2015 la Svizzera è diventata il primo Stato al mondo a creare le basi giuridiche per un deposito protetto destinato a custodire, temporaneamente e a titolo fiduciario, beni culturali esteri minacciati. Il progetto è stato nel frattempo realizzato: il deposito protetto è ora disponibile. Grazie ai suoi elevati standard nel campo della PBC, la Svizzera è stata inoltre incaricata di alcune perizie nell'ambito del previsto fondo internazionale.

Conferenza a Kreuzlingen (TG)

Gestione delle catastrofi transfrontaliere

Oltre 200 membri della protezione della popolazione ed esperti provenienti da Germania e Svizzera hanno partecipato alla conferenza specialistica tenutasi il 19 gennaio 2017 a Kreuzlingen (TG) per discutere la gestione di una catastrofe transfrontaliera. In estate si terrà un'esercitazione organizzata dall'Ufficio federale della protezione della popolazione.

I contatti tra i partner della protezione della popolazione delle regioni di confine Lago di Costanza e Foresta nera renana sono molto buoni. Una collaborazione che si intende ulteriormente rafforzare con un'esercitazione anticatastrofe transfrontaliera che si svolgerà in giugno. In collaborazione con le autorità delle regioni di confine, l'UFPP ha sviluppato una sequenza d'esercizio ad hoc.
In una conferenza specialistica tenutasi a Kreuzlingen sono stati discussi e presi accordi nei settori coordinamento delle misure, risorse, comunicazione e informazione. Si è trattato anche di un'occasione unica per favorire la conoscenza reciproca tra i responsabili degli enti coinvolti. Sono state inoltre fornite informazioni dettagliate sugli scenari che saranno esercitati in giugno.

Workshop internazionale di esperti a Zurigo

Insegnamenti tratti dalla crisi migratoria

Durante la crisi migratoria del 2015 sono emersi in tutta Europa i punti di forza e i punti deboli delle strutture e dei processi esistenti per gestire le crisi. Lo scorso autunno, esperti provenienti da Germania, Austria e Svizzera si sono incontrati a Zurigo per condividere le loro esperienze.

Il forte aumento del numero di profughi negli ultimi anni costituisce una grossa sfida per i Paesi europei. Al culmine della crisi migratoria dell'estate e dell'autunno 2015 è stato necessario trovare soluzioni pragmatiche in pochi giorni o addirittura nel giro di poche ore. Sono emersi i punti di forza e i punti deboli delle strutture e dei processi esistenti per gestire le crisi.
Per la protezione della popolazione, gli insegnamenti tratti dalla crisi migratoria sono molto preziosi per prepararsi meglio a catastrofi, crisi e situazioni d'emergenza future. A tal fine è necessaria un'analisi completa, puntuale e critica dei sinistri, che coinvolga i principali partner. Per la Svizzera è particolarmente importante una collaborazione con i Paesi limitrofi poiché l'emergenza profughi è, a conti fatti, una sfida transfrontaliera.

Soltanto in alcuni casi si è fatto ricorso alle strutture della protezione della popolazione, benché esistano procedure prestabilite per affrontare simili crisi.

Per promuovere lo scambio di esperienze tra Germania, Austria e Svizzera, l'Ufficio federale della protezione della popolazione (UFPP) ha organizzato, in collaborazione con il Center for Security Studies CSS del PF di Zurigo, un workshop di due giorni che si terrà a Zurigo alla fine di ottobre 2016. Gli organizzatori hanno potuto contare sulla collaborazione di lunga data tra le autorità di protezione civile dei Paesi limitrofi, che hanno già partecipato in passato a numerosi workshop D-A-CH su varie problematiche della protezione della popolazione (per es. analisi dei rischi e protezione delle infrastrutture critiche).

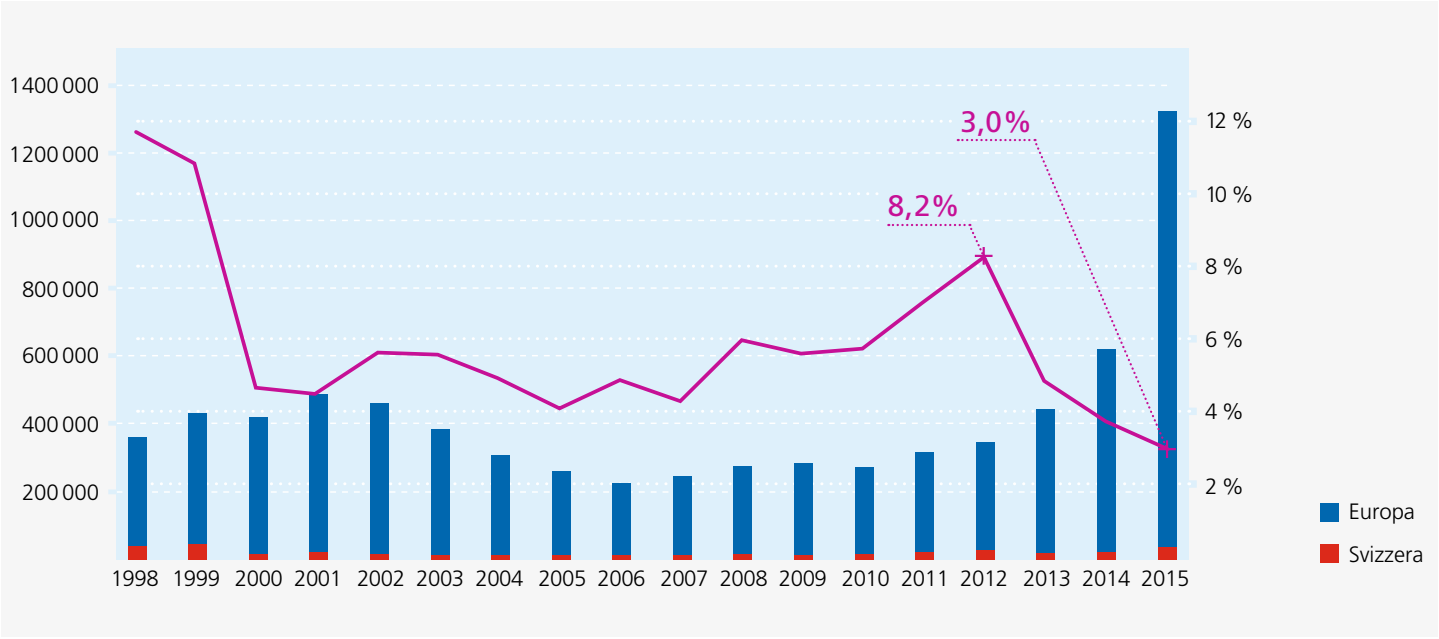
Discussione durante il workshop d'esperti.

Autorità, organizzazioni di soccorso e mondo scientifico

Per la Germania hanno partecipato al workshop l'Ufficio della protezione della popolazione (BBK), l'Ufficio per la migrazione e i rifugiati (BAMF), l'Ufficio dei trasporti delle merci (BAG), il centro di ricerca sulle catastrofi dell'Università di Berlino e gli stati federati di Baviera e Baden-Württemberg. L'Austria era rappresentata dal Ministero degli interni (BMI), dalla regione del Tirolo e dalla Croce Rossa austriaca. Gli interessi della Svizzera erano rappresentati dalla Segreteria di Stato della migrazione (SEM), l'Ufficio federale della protezione della popolazione (UFPP), l'Amministrazione federale delle dogane (AFD), i Cantoni di San Gallo, Vaud e Zurigo e la Croce Rossa Svizzera.
Al centro del workshop vi erano due obiettivi: in primo luogo condividere le esperienze pratiche degli ultimi mesi e discutere le possibili misure per affrontare le future sfide, in secondo luogo identificare le conseguenze per il livello politico-strategico.

Punti forti e punti deboli

Dalla discussione è presto emerso che garantire responsabilità e competenze chiare e affidabili costituisce uno dei compiti più impegnativi durante la crisi dei profughi. Gestire la fase iniziale, in cui si deve far fronte a un numero crescente di migranti, è soprattutto un compito di polizia, mentre le successive necessità di alloggio e assistenza sono problematiche che competono alla politica sociale. Soltanto in alcuni casi si è fatto ricorso alle strutture di protezione della popolazione, benché esistano procedure prestabilite per affrontare simili crisi. Al loro posto sono stati spesso applicati nuovi strumenti operativi che hanno causato ritardi e problemi di coordinamento tra i numerosi attori coinvolti.
I partecipanti hanno dichiarato all'unanimità che, nonostante le difficili condizioni operative, sono state prevalentemente trovate soluzioni pragmatiche ed efficaci per garantire un minimo di assistenza e sicurezza ai profughi. Decisive sono state soprattutto le consultazioni informali tra le autorità nazionali, regionali e locali nonché le organizzazioni di soccorso coinvolte. In particolare, le organiz-



Quota svizzera di migranti nel confronto europeo (fonte: SEM).

zazioni di soccorso hanno affermato che per affrontare le future catastrofi, crisi e situazioni d'emergenza è indispensabile creare processi e strutture prestabilite da regolamenti, ad esempio per il finanziamento delle operazioni di assistenza.

Insegnamenti per il lungo termine

I partecipanti al workshop hanno inoltre discusso quali insegnamenti si possono trarre per il medio e lungo termine. Hanno innanzitutto constatato che l'emergenza profughi non è affatto conclusa. Nei prossimi anni ci si attende piuttosto un nuovo forte aumento dei flussi migratori verso l'Europa. Ciononostante si riscontra una graduale smobilitazione delle strutture necessarie per gestire le crisi. È quindi importante adottare tempestivamente misure per essere in grado di reagire rapidamente a eventuali cambiamenti sul piano operativo. Le organizzazioni della protezione della popolazione dovrebbero assumere un ruolo attivo in questo ambito.

E tutto ciò si collega con un altro punto già ripetutamente citato: l'individuazione tempestiva delle emergenze. Per mancanza di coordinamento e di comunicazione, al culmine della crisi migratoria gli operatori non disponevano sempre di un quadro preciso della situazione, costringendoli a reagire in modo affrettato invece di adottare misure ponderate. Per colmare queste lacune, sarà importante continuare a rafforzare e istituzionalizzare la collaborazione tra i partner ai diversi livelli amministrativi e con i Paesi limitrofi, per esempio tramite esercitazioni transfrontaliere periodiche.

Florian Roth
Senior Researcher, Risk and Resilience Research Team,
Center for Security Studies CSS, ETH Zurigo

Assistenza ai profughi da parte della protezione della popolazione

Gestire un afflusso massiccio di profughi presuppone una stretta collaborazione tra gli enti statali e non statali, in particolare nei settori della sanità, dei servizi sociali e giovanili, della sicurezza pubblica e dell'asilo. Anche le organizzazioni della protezione della popolazione assumono un ruolo importante soprattutto nei settori dei trasporti e della registrazione, dell'allestimento di alloggi di fortuna e della fornitura di pasti, vestiti, cure mediche e sostegno psicosociale.

Esercitazione EMMA II

Strumenti di misurazione e compresse allo iodio per l'ambasciata a Vienna

L'Ufficio federale della protezione della popolazione (UFPP) e il Dipartimento federale degli affari esteri (DFE) hanno esercitato il rapido rifornimento di un'ambasciata con il materiale di protezione necessario in caso d'incidente in una centrale nucleare all'estero. L'obiettivo era quello di migliorare la protezione del personale d'ambasciata e della comunità svizzera in loco in previsione di una reale emergenza.

In seguito all'incidente della centrale nucleare giapponese di Fukushima Daiichi nel marzo 2011, il Consiglio federale ha adottato 56 misure volte a migliorare la protezione d'emergenza in caso di eventi estremi (NOMEX). La Confederazione dispone ora del materiale necessario per proteggere rapidamente i cittadini svizzeri all'estero. L'esercitazione EMMA II (Emergency Management MAterial), svolta a fine novembre 2016, ha permesso di verificare l'intero processo di invio e impiego del materiale d'emergenza.

Scenario fornito dall'Austria

L'esercitazione è stata svolta in collaborazione con l'ambasciata svizzera a Vienna. Vi hanno inoltre partecipato il Centro di gestione delle crisi (KMZ) del Dipartimento federale degli affari esteri (DFAE), l'Aiuto umanitario della Confederazione insediato presso la Direzione dello sviluppo e della cooperazione (DSC) del Dipartimento federale degli affari esteri (DFAE), la Farmacia dell'esercito nonché la Centrale nazionale d'allarme (CENAL), il Centro operativo e di coordinamento nazionale (NOCC) e la sezione Risorse dell'Ufficio federale della protezione della popolazione (UFPP).

Lo scenario, che prevedeva un incidente in una centrale nucleare nell'Europa centro-orientale, era basato sull'esercitazione di radioprotezione austriaca INTREX 12 dell'ottobre 2012.

I preparativi si sono svolti in collaborazione con le autorità austriache. Lo scenario, che prevedeva un incidente in una centrale nucleare nell'Europa centro-orientale, era basato sull'esercitazione di radioprotezione austriaca INTREX 12 svolta nell'ottobre 2012. Ciò ha permesso di simulare in modo realistico anche le procedure delle autorità austriache.
Proprio come accadrebbe in una situazione reale, il copione prevedeva che l'ambasciata e la CENAL venissero a conoscenza dell'incidente dai media quasi contemporaneamente. In caso di simili notizie, la CENAL contatta immediatamente l'Agenzia internazionale per l'energia atomica (AIEA) e avvia uno scambio reciproco di informazioni con il centro di gestione delle crisi del DFAE, che in caso d'emergenza è responsabile per il sostegno del personale del DFAE in loco.

Mezzi di protezione e di misurazione per l'ambasciata

Secondo lo scenario è stato subito chiaro che non si trattava di una notizia infondata e che molto probabilmente c'era stata una fuga radioattiva. Il KMZ ha contattato l'ambasciata, che ha fornito un elenco approssimativo del materiale necessario. Nell'esercitazione si prevedeva che in quel momento in Austria soggiornassero circa 40'000 cittadini Svizzeri.
Il materiale previsto per l'invio comprendeva dosimetri, rateometri di dose assorbita e compresso allo iodio. I dosimetri sono destinati alle persone particolarmente esposte alle radiazioni e forniscono informazioni sulla quantità di radiazioni assorbite. Durante l'intervento, i valori misurati vengono regolarmente trasmessi alla CENAL che provvede alla loro valutazione. Sulla base di questi dati, la CENAL può fornire raccomandazioni precise per la protezione delle persone esposte. In questo modo possono continuare a svolgere i loro compiti fino al raggiungimento del limite stabilito per poi cercare protezione in un locale chiuso.
I rateometri di dose assorbita vengono utilizzati come sensori per misurare la contaminazione radioattiva dell'aria o di oggetti e superfici. Le compresse allo iodio infine, se ingerite per tempo, evitano che lo iodio radioattivo liberato nell'aria in caso d'incidente nucleare venga assorbito dalla tiroide.

Aspetti logistici

D'intesa con la CENAL e il KMZ è stato attivato l'invio del materiale. Il processo d'invio rispetta le procedure standard previste dalla Gestione federale delle risorse (ResMaB), che vengono applicate per tutte le richieste di risorse urgenti nell'ambito della protezione della popolazione. Gli strumenti di misurazione dell'UFPP e le compresse allo iodio della Farmacia dell'esercito sono state portate alla DSC a Wabern e inviate tramite corriere diplomatico. In caso di reale emergenza si potrebbe anche ricorrere all'esperienza dell'Aiuto umanitario della Confederazione per recapitare il materiale all'estero attraverso altri canali. Se necessario, sussiste anche la possibilità di

Il personale dell'ambasciata a Vienna controlla il contenuto del pacco con il materiale inviato dalla Svizzera, contenente dosimetri, strumenti per misurare la radioattività e compresse allo iodio.

mobilitare membri del Corpo svizzero di aiuto umanitario (SCA). L'aggiunta di un termometro ha permesso di rilevare a quali sbalzi termici è stato esposto il delicato pacco durante il suo viaggio fino alla capitale austriaca.

Stato maggiore di crisi a Vienna

A scopo d'esercizio, l'ambasciata a Vienna ha assunto il ruolo di stato maggiore di crisi, incaricato di coordinare le richieste dei cittadini, la protezione del proprio personale, i fattori psicologici e i contatti con le autorità in loco e in patria. Il pacco giunto dalla Svizzera ha costituito una piccola sfida per i collaboratori, dato che quasi nessuno era istruito all'uso degli strumenti di misurazione della radioattività.
In caso di reale emergenza, i dosimetri permetterebbero al personale d'ambasciata di verificare, in modo semplice e affidabile, se può continuare a svolgere i suoi compiti di misurazione o se la dose assorbita è troppo elevata. L'impiego degli strumenti per misurare la radioattività non era invece stabilito in modo definitivo nel copione dell'esercitazione. Avrebbero potuto essere utilizzati sia come sonde di misurazione da impiegare all'interno del perimetro dell'ambasciata, sia come controllo d'entrata, per evitare che persone contaminate entrassero nell'edificio.
L'impiego delle compresse allo iodio era invece chiaramente definito, poiché era previsto solo nel caso in cui non fossero state ottenibili attraverso i canali ufficiali del Paese ospitante. Bisogna assolutamente evitare di creare dei doppioni.

Possibili miglioramenti

Da una prima valutazione dell'esercitazione è emerso che la logistica ha funzionato bene e che l'ambasciata ha potuto essere rapidamente rifornita del materiale necessario nonostante i numerosi enti coinvolti. Occorre invece migliorare la consulenza al personale d'ambasciata e i contatti diretti tra la CENAL e l'ambasciata. Sono inoltre sorte diverse domande pratiche: come viene garantita la distribuzione delle compresse allo iodio all'interno del Paese? Quali informazioni ricevono i cittadini svizzeri assieme alle compresse allo iodio? Come viene comunicato quando è necessario ingerire le compresse? Chi riceve le compresse e quante? Un gruppo di lavoro composto da membri della CENAL e del KMZ si chinerà su questi punti.
Occorre inoltre tenere presente che dopo un incidente in una centrale nucleare potrebbe risultare ancora più difficile mettere a disposizione i mezzi logistici. Dato che raramente vi è un motivo per una collaborazione diretta e che la comunicazione passa di regola attraverso il KMZ, diventa ancora più importante contattarsi rapidamente, individuare le informazioni necessarie e offrire un sostegno semplice e pratico. Solo così è possibile proteggere efficientemente il personale d'ambasciata e la comunità svizzera sul posto.

Christian Fuchs
Capo Comunicazione in caso d'evento, Centrale nazionale d'allarme (CENAL), UFPP

Dal Consiglio federale

Disciplinare l'accesso ai precursori di esplosivi

Consapevole del rischio che terroristi possano procurarsi in Svizzera sostanze chimiche da utilizzare per fabbricare ordigni artigianali, il Consiglio federale intende rendere più difficoltoso l'accesso a tali sostanze. Nella sua seduta del 9 dicembre 2016 ha quindi incaricato il Dipartimento federale di giustizia e polizia (DFGP) di elaborare le basi giuridiche necessarie per disciplinare l'accesso ai cosiddetti precursori di esplosivi.

Gli ultimi attentati in Europa hanno dimostrato che i terroristi fabbricano ordigni artigianali utilizzando sostanze contenute in prodotti destinati all'uso quotidiano come fertilizzanti, prodotti per la pulizia delle piscine e diserbanti. Tali sostanze chimiche, quali il perossido di idrogeno, l'acetone e i nitrati, possono essere utilizzati per fabbricare esplosivi. Questi precursori sono contenuti in prodotti liberamente accessibili in Svizzera, mentre nell'Unione europea il loro commercio è soggetto a regolamentazione. Il rischio che terroristi si procurino i precursori in Svizzera è quindi reale.

Collaborazione con i settori interessati

Su incarico del Consiglio federale, un gruppo di esperti diretto da fedpol ha approfondito la questione su come ostacolare l'accesso ai precursori. Il gruppo di esperti ha lavorato a stretto contatto con i settori interessati.
Per mettere in atto le misure elaborate occorre una nuova legge federale. Il Consiglio federale ha quindi incaricato il DFGP di preparare un avamprogetto di legge da mettere in consultazione e di sottoporglielo entro la fine del 2017.

Un disciplinamento differenziato

Il disciplinamento previsto si applicherà agli acquisti di determinati precursori nel commercio specializzato. Più la concentrazione di un precursore sarà elevata in un prodotto, più severe saranno le restrizioni. Le misure di applicheranno soltanto ai privati, mentre non riguarderanno i professionisti quali gli agricoltori. Il Consiglio federale confida nell'autocontrollo e nella sensibilizzazione dei professionisti.

Dal Consiglio federale

Garantire l'approvvigionamento: un compito per diversi attori

L'Approvvigionamento economico del Paese deve agire a livello interdisciplinare. Solo così è possibile individuare tempestivamente rischi complessi e superare le crisi di approvvigionamento. Sono queste le conclusioni del rapporto 2013–2016 sull'AEP, di cui il Consiglio federale ha preso conoscenza il 2 dicembre 2016.

Nel periodo in esame (2013-2016), l'Approvvigionamento economico del Paese (AEP) ha rivalutato, in base al proprio processo strategico, i rischi per l'approvvigionamento. Inoltre ha analizzato nel dettaglio il proprio orientamento strategico, soffermandosi anche sull'efficacia e sull'operatività di strumenti e misure. Questo ciclo quadriennale si conclude con il rapporto sull'AEP, che passa in rassegna le principali attività, descrive le lacune da colmare e annuncia le prossime sfide.

I processi di approvvigionamento sono esposti a rischi sempre più difficili da prevedere. Tra il 2013 e il 2016 l'AEP è dovuto intervenire a causa di una penuria di oli minerali e del ripetuto esaurimento degli stock di medicinali. Ogni volta si è dovuto ricorrere alle scorte obbligatorie. Inoltre, la carenza di prodotti a base di oli minerali dell'autunno 2015 ha dimostrato che crisi di questo tipo sono dovute alla concomitanza di una serie di fattori molto diversi tra loro.

Rapporto sull'estate canicolare 2015

Gestita bene, ma esiste un potenziale di miglioramento

Nell'estate del 2015 in Svizzera si è verificato per la seconda volta dopo il 2003 un lungo periodo di canicola accompagnato da una grande siccità. In alcune regioni del Paese si è registrato il mese di luglio più caldo dall'inizio delle misurazioni. Particolarmente colpita è stata la popolazione delle città. Il rapporto della Confederazione «La canicule et la sécheresse de l'été 2015: impacts sur l'homme et l'environnement» (La canicola e la siccità dell'estate 2015: ripercussioni sull'uomo e sull'ambiente) analizza questi eventi, illustra le ripercussioni e trae insegnamenti per il futuro.

Nel complesso, la siccità dell'estate 2015 è stata gestita meglio rispetto al 2003, anno in cui si è verificato l'ultimo periodo di canicola di rilievo, grazie alle misure adottate a partire da allora. La canicola ha tuttavia avuto notevoli ripercussioni sulla salute della popolazione. In estate, infatti, si sono registrati ottocento decessi in più rispetto alla media degli altri anni. La mortalità nei mesi estivi del 2015 si è quindi attestata quasi allo stesso livello di quella dell'estate canicolare del 2003.

Nella gestione della canicola sono tuttavia stati registrati anche dei successi. Nella regione del Lemano, dove dopo il 2003 sono stati introdotti dei piani per far fronte alla canicola, gli speciali provvedimenti destinati alle persone a rischio hanno consentito di ridurre notevolmente la mortalità rispetto al 2003. Si prevede che a causa dei cambiamenti climatici in futuro i periodi di canicola saranno più frequenti.

È pertanto estremamente importante esaminare nei dettagli le misure dei cantoni e trarre insegnamenti da quelle di successo. Tra queste vi sono l'informazione ai gruppi a rischio (per es. anziani) e al personale di cura sui comportamenti corretti da adottare in caso di canicola. Inoltre, occorre emanare un'unica allerta canicola per l'intera Svizzera. Le misure contro la canicola, in parte di natura molto diversa, devono essere coordinate e dei piani specifici devono assolutamente essere attuati nei cantoni a rischio elevato.

Effetto forno nelle città

Ad essere maggiormente colpita dalla canicola è soprattutto la popolazione delle città e degli agglomerati urbani. I suoli impermeabilizzati delle città immagazzinano il calore, aumentando di conseguenza la temperatura. Inoltre, di notte le temperature si abbassano solo di poco. Per far fronte a queste isole termiche, sempre più numerose, sono necessarie superfici verdi e zone d'ombra. Inoltre, nonostante l'esigenza di uno sviluppo centripeto delle città, nelle regioni colpite vanno garantiti o migliorati l'afflusso e la circolazione di aria fresca dalle zone periurbane.

Le ripercussioni di canicola e siccità su piante e animali possono essere valutate solo a distanza di anni. A seconda delle condizioni meteorologiche, nei prossimi anni la natura potrà compensare in misura più o meno elevata gli effetti dell'anno estremo 2015. Per garantire l'approvvigionamento di acqua potabile in ogni parte del Paese anche durante i periodi di siccità, la Confederazione raccomanda l'elaborazione di un piano di utilizzazione specifico, il collegamento delle reti di approvvigionamento idrico e in ogni caso fare capo ad almeno due fonti indipendenti.

Proteggere il clima invece di combattere i sintomi

Tutte le misure di adattamento servono di fatto soltanto a lottare contro i sintomi. Le misure di adattamento sono possibili e sostenibili dal punto di vista finanziario soltanto se si riesce a mitigare i cambiamenti climatici.

Il rapporto (tedesco e francese) è disponibile qui:
www.bafu.admin.ch/uz-1629-d
www.bafu.admin.ch/uz-1629-f

ITC 2017

Nuove istruzioni tecniche per le costruzioni di protezione

A inizio anno sono entrate in vigore le nuove «Istruzioni tecniche per la costruzione e il dimensionamento delle costruzioni di protezione» (ITC 2017). I progetti già iniziati possono essere ultimati in base alle vecchie prescrizioni.

Il principio secondo cui le costruzioni di protezione devono garantire una protezione di base contro gli effetti delle armi moderne non cambia neppure con le nuove istruzioni. L'Ufficio federale della protezione della popolazione ha tuttavia adattato le istruzioni tecniche per la costruzione e il dimensionamento delle costruzioni di protezione allo stato attuale delle conoscenze in ambito tecnico, alle norme più attuali e alle prescrizioni tecniche in vigore.
L'aggiornamento delle istruzioni tecniche (ITC 1994) si è reso necessario in particolare a seguito dell'introduzione di nuove norme SIA. Dal 1994 le costruzioni di protezione vengono realizzate in modo unitario secondo le ITC 1994. Anche se si fondano su un principio di dimensionamento autonomo, queste tengono conto anche delle norme SIA.
Le ITC 2017 sono vincolanti per la pianificazione delle costruzioni di protezione. Indicano ad esempio l'altezza massima consentita per gli edifici sovrastanti i rifugi e elencano le misure supplementari che devono essere adottate nell'ambito della sicurezza antisismica degli edifici. Sono state inasprite in particolare le esigenze in materia di verifica della capacità portante a taglio.
I progetti iniziati prima del 1° luglio 2017 possono ancora essere pianificati e realizzati secondo le ITC 1994.

Prova delle sirene 2017

Il 99 per cento ha funzionato perfettamente

In occasione della prova delle sirene del 1° febbraio 2017, il 99 percento delle sirene ha funzionato in modo ineccepibile. Le lacune riscontrate verranno colmate al più presto. L'allarme della popolazione in caso di catastrofe rimane così garantito.

In Svizzera ci sono circa 7'200 sirene per dare l'allarme generale alla popolazione in caso di pericolo, di cui circa 5'000 sirene fisse e circa 2'200 sirene mobili. Delle sirene fisse circa 600 sono sirene combinate, utilizzate per diffondere sia l'allarme generale, sia l'allarme acqua. Grazie al nuovo sistema di telecomando Polyalert, è stato possibile rilevare i risultati della prova il giorno stesso.
La valutazione dell'Ufficio federale della protezione della popolazione (UFPP) conferma che il 99 percento delle sirene fisse testate hanno funzionato in modo ineccepibile. Presso 61 sirene sono stati riscontrati dei difetti. Questo risultato rispecchia i valori degli anni precedenti.
I cantoni e i comuni sono tenuti a riparare o a sostituire immediatamente le sirene difettose. L'immediata eliminazione dei difetti riscontrati durante la prova annuale permette di garantire un'elevata affidabilità delle sirene.

Vetrina di Swisstopo presso l'UFPP

Geoportale pluripremiato

Negli ultimi anni, map.geo.admin.ch, il geoportale della Confederazione, ha vinto diversi premi. I dati dell'Inventario della protezione dei beni culturali (Inventario PBC 2009) sono parte integrante dei geodati nazionali. Sotto il titolo di «SwissGuesser» è disponibile anche un quiz che permette di mettere alla prova le proprie conoscenze sui luoghi in cui si trovano i vari beni culturali in Svizzera.
Per informazione e ringraziamento agli uffici federali che vi hanno partecipato, da qualche tempo sta circolando una vetrina mobile con i premi vinti da geo.admin.ch. L'esposizione itinerante farà tappa presso l'Ufficio federale della protezione della popolazione (UFPP) dal 1° al 28 aprile 2017.

Maggiori informazioni sulla mostra itinerante e i premi vinti da SwissTopo si trovano nel sito: www.geo.admin.ch/awards

Programma di SRF1 dedicato al tema «blackout»

L'UFPP davanti alle telecamere e dietro le quinte

Il 2 gennaio di quest'anno, la televisione svizzero-tedesca SRF1 ha trasmesso un programma fuori dal consueto. Nell'ambito di una trasmissione di nove ore, si è cercato di mostrare, nel modo più realistico possibile, le conseguenze che avrebbe un blackout su vasta scala o una penuria di elettricità di lunga durata sulla nostra vita pubblica e privata. L'obiettivo era quello di sensibilizzare la popolazione sull'importanza di un approvvigionamento elettrico funzionante in una società altamente interconnessa come la nostra, soprattutto dal punto di vista della sicurezza. L'Ufficio federale della protezione della popolazione (UFPP) ha affiancato il team di produzione della SFR nella pianificazione e realizzazione della trasmissione. Le analisi dei pericoli effettuate dall'UFPP sono servite da base per il documentario, nel quale sono state simulate in modo molto realistico le conseguenze di un blackout. Un team televisivo ha realizzato delle riprese nella Centrale nazionale d'allarme dell'UFPP. Personale specializzato dell'UFPP ha assistito il team della redazione fornendo consigli e stabilendo contatti con altri specialisti. Durante la trasmissione, Benno Bühlmann, direttore dell'UFPP, e Stefan Brem, capo Analisi dei rischi e coordinamento della ricerca, hanno risposto alle domande del presentatore Urs Gredig.

Domande degli spettatori

I collaboratori dell'UFPP hanno lavorato anche dietro le quinte. Per tutta la durata della trasmissione, 15 esperti dell'UFPP hanno infatti risposto alle domande poste dagli spettatori per telefono e via chat. Il nuovo record di domande in un programma della SRF dimostra il grande interesse della popolazione per questo tema. Le domande e le osservazioni dei telespettatori sono state molto pertinenti e costruttive, e molti hanno ringraziato per l'ottima qualità delle informazioni fornite. Il grande lavoro svolto è stato ampiamente ricompensato ed è valso la pena sia per il team di SRF, sia per l'UFPP.

Collaborazione tra la protezione civile di Basilea Città e le Aziende industriali di Basilea IWB

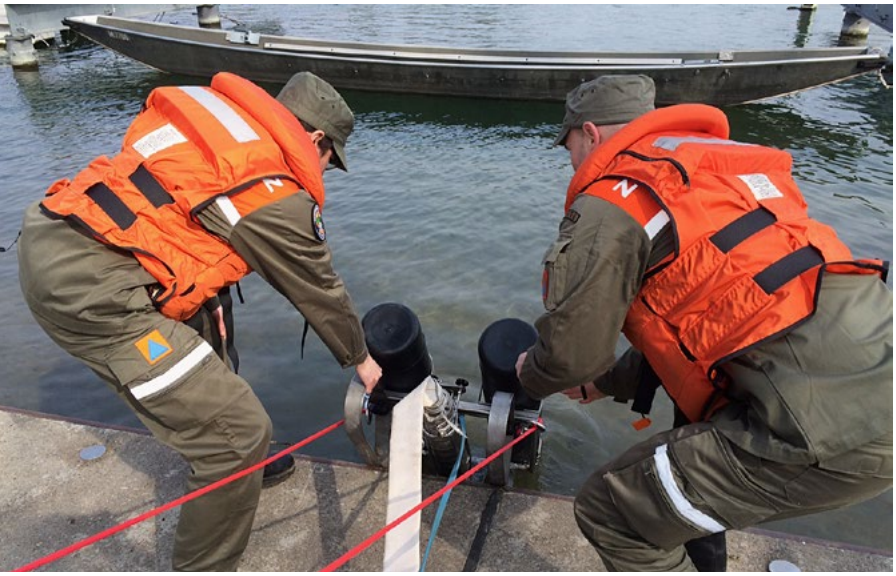
Impianti mobili per trattare l'acqua potabile

Il Cantone di Basilea-Città dispone di impianti per trattare l'acqua potabile in caso di situazioni d'emergenza. Le Aziende industriali di Basilea (IWB) e la protezione civile di Basilea Città sono così in grado di rifornire in poche ore fino a 160'000 persone con l'acqua necessaria.

In Svizzera, i cantoni sono tenuti a garantire l'approvvigionamento della popolazione con acqua potabile. L'Ordinanza sulla garanzia dell'approvvigionamento con acqua potabile in situazioni d'emergenza garantisce le condizioni e la quantità di acqua potabile che devono essere disponibili in caso d'emergenza. Si parla di situazione d'emergenza quando la normale fornitura di acqua potabile è minacciata, limitata o interrotta da un evento naturale, un incidente, un atto di sabotaggio o da operazioni belliche. L'ordinanza prevede che la normale fornitura di acqua potabile sia garantita il più a lungo possibile, che i guasti siano riparati nel minor tempo possibile e che la quantità d'acqua necessaria per sopravvivere sia disponibile in qualsiasi momento:

- fino al terzo giorno, il più possibile;
- dal quarto giorno, 4 litri per persona al giorno (per gli animali da reddito, 60 litri per unità di bestiame di grossa taglia al giorno);
- dal sesto giorno: 15 litri per persona al giorno (negli ospedali e nelle case di cura, 100 litri per persona al giorno; nelle aziende che producono beni d'importanza vitale, la quantità necessaria).

Per il Canton Basilea Città la quantità necessaria per la sopravvivenza è di circa 800 mila litri di acqua potabile al giorno. A titolo di paragone, il consumo giornaliero normale ammonta a 70 milioni di litri e può crescere fino al doppio nei mesi estivi.



La protezione civile Basilea Città dispone di una «sezione Acqua potabile» che può essere mobilitata nel giro di poche ore.

La cellula cantonale di crisi assume il comando

Per creare i presupposti per la fornitura di acqua potabile in situazioni d'emergenza, i cantoni elaborano concetti d'emergenza adeguati alle loro condizioni specifiche. La Società svizzera dell'Industria del gas e delle acque (SSIGA) ha elaborato, come ausilio pratico, una guida per la pianificazione e la realizzazione dell'approvvigionamento d'acqua potabile in situazioni d'emergenza (TWN). Questa guida serve da base per il concetto basilese che definisce i poteri e le responsabilità in caso d'emergenza.
Le Aziende industriali di Basilea (IWB) non sono responsabili per la fornitura di acqua potabile nel cantone di Basilea-Città solo nella quotidianità, ma anche per garantire la fornitura il più a lungo possibile in caso d'approvvigionamento limitato. L'obiettivo è quindi il rapido ripristino della normale rete d'approvvigionamento. La cellula di crisi cantonale (CCC) assume il comando in caso d'interruzione del normale approvvigionamento idrico. E decide in merito all'installazione della rete idrica d'emergenza.
Il concetto d'emergenza serve alla CCC da ausilio decisionale e riassume le possibili misure in una matrice. A seconda del numero di persone colpite, delle condizioni locali, del quadro temporale e dell'urgenza, vengono proposte misure diverse. Vi rientrano la distribuzione di bottiglie d'acqua, la fornitura d'acqua con autocisterne e l'approvvigionamento di acqua potabile dalle rete dei comuni limitrofi, ma anche l'uso dei pozzi freatici d'emergenza e il conseguente trattamento dell'acqua con impianti mobili.

Il concetto d'emergenza per l'acqua potabile si fonda sugli impianti di trattamento

Basilea ha optato per l'acquisto di impianti di trattamento mobili poiché un'eventuale penuria d'acqua potabile in caso di un'interruzione della rete idrica non sarebbe risolvibile con altre misure. I quattro impianti di trattamento mobili, che permettono di rifornire 40 mila persone ciascuno, offrono tutta una serie di vantaggi. Grazie ai pozzi d'emergenza disponibili nell'area metropolitana, la popolazione può essere rifornita con acqua potabile a livello locale. In caso di contaminazione dei pozzi d'emergenza, i sistemi mobili possono essere utilizzati in luoghi alternativi o per le acque di superficie. Permettono inoltre di trat-

Un impianto di trattamento mobile può produrre acqua potabile per 40'000 persone.

tare grandi quantità di acqua per pulire gli impianti di approvvigionamento che sono fuori uso.
Lo svantaggio degli impianti di trattamento mobili è che la popolazione deve andare a prendere per conto proprio l'acqua necessaria per la sopravvivenza. Tuttavia, i sistemi mobili vengono impiegati solo quando le altre misure non sono più efficaci. Il loro valore come mezzo flessibile per le emergenze mette quindi in secondo piano questo inconveniente.

La sezione Acqua potabile della protezione civile Basilea Città

Gli impianti di trattamento mobili hanno una tradizione a Basilea. Ciò è in parte attribuibile al fatto che l'approvvigionamento di acqua potabile nel Cantone di Basilea Città si basa in larga percentuale sulle acque del Reno. Quando il Reno non è disponibile per diverso tempo (mesi) come fonte di acqua, l'approvvigionamento idrico nel Cantone è limitato. Grazie agli impianti di trattamento mobili è però possibile ripiegare su fonti d'acqua alternative come i pozzi freatici d'emergenza.
La Protezione Civile Basilea Città svolge un ruolo importante nel concetto d'emergenza. La sua sezione Acqua potabile può essere mobilitata nel giro di poche ore. La protezione civile assicura l'istruzione e l'uso degli impianti con l'assistenza di dipendenti dell'IBW. Senza questa collaborazione, l'uso degli impianti di trasformazione mobili sarebbe impossibile. In caso d'interruzione della rete idrica, essendo impegnati soprattutto nel ripristino degli impianti d'approvvigionamento idrico, i collaboratori dell'IWB non possono gestire contemporaneamente anche gli impianti di trattamento mobili.

«Blackout»

L'anno scorso, la Radio Televisione Svizzera (SRF) ha filmato la collaborazione efficiente tra la squadra di pronto intervento «Acqua potabile» della protezione civile Basilea Città e l'IWB. Il servizio è stato trasmesso il 2 gennaio 2017 in occasione della giornata dedicata al «Blackout», per mostrare quali sono gli effetti di una prolungata mancanza di corrente in Svizzera sull'approvvigionamento idrico. Sia prima che durante le riprese, i partecipanti si sono resi conto del fatto che un «blackout» di diversi giorni è non solo possibile in qualsiasi momento, ma soprattutto connesso con conseguenze di ampia portata per l'approvvigionamento idrico. Il concetto basilese costituisce la base per far fronte a tali emergenze nel Cantone.

Franz Näf
Capo team Istruzione/Intervento, Ufficio del militare e della protezione civile di Basilea Città

La Televisione svizzera filma come una cisterna (autocarro verde sullo sfondo) viene riempita con acqua potabile.

Canton Argovia

Rimodernamento dell'ubicazione di condotta protetta

Il Canton Argovia sta risanando l'ubicazione di condotta protetta del Consiglio di Stato e dello Stato maggiore cantonale di condotta. L'impianto rimodernato e ampliato sarà disponibile nel primo trimestre del 2018.

Con l'inizio dei lavori l'8 dicembre 2016, il Canton Argovia ha dato ufficialmente inizio al risanamento dell'ubicazione di condotta protetta del Consiglio di Stato e dello stato maggiore cantonale di condotta.

Gli accertamenti relativi all'uso futuro dell'ubicazione di condotta protetta dello Stato maggiore cantonale di condotta (SMCC) sono iniziati nel 2014. L'analisi dei rischi del Canton Argovia mostra chiaramente che in caso di scenari quali un blackout esteso, un terremoto o un incidente in una centrale nucleare lo SMCC dipende da un'ubicazione protetta. Lo SMCC necessita inoltre di mezzi di comunicazione funzionanti.

Ubicazione ormai vetusta

Considerata l'età dell'impianto protetto, realizzato nel 1978, il bisogno di rimodernamento è elevato, dato che diverse misure di risanamento edilizio e tecnico necessarie sono state tenute in sospeso per accertamenti. Affinché lo SMCC sia in grado di adempiere i suoi compiti di condotta in qualsiasi momento, i sistemi, le installazioni e il gruppo elettrogeno d'emergenza, ormai vetusti, devono essere rimessi a nuovo e al passo con i tempi.
Dopo il nulla osta della direttrice del Dipartimento della sanità e della socialità all'utilizzo futuro dell'impianto di protezione e quindi al suo risanamento, è stato possibile compiere i primi accertamenti in collaborazione con l'Ufficio federale della protezione della popolazione (UFPP).
In un passo successivo si è trattato di verificare lo stato dell'impianto e di stabilire le misure di risanamento necessarie. Durante la progettazione si è deciso che nell'ubicazione di condotta potesse essere integrata anche la centrale per le chiamate d'emergenza della polizia cantonale argoviese.
Si tratta ora di attuare tutta una serie di misure:

- risanare l'involucro dell'edificio;
- sostituire la centrale telefonica;
- aggiornare i sistemi informatici e telematici;
- adattare i locali alle esigenze dello SMCC;
- installare un'ubicazione d'emergenza per la centrale d'emergenza cantonale;
- installare un posto di attivazione ridondante per le sirene (telecomando Polyalert);
- ottimizzare l'aspetto tecnico-energetico in vista di un maggiore uso per rapporti ed esercitazioni;
- rimodernare la cucina secondo le prescrizioni in materia di derrate alimentari;
- potenziare il gruppo elettrogeno d'emergenza.

Credito d'impegno per 3,9 milioni di franchi

Su richiesta del Consiglio di Stato, il 22 novembre 2016 il Gran Consiglio argoviese ha approvato un credito d'impegno indicativo per la realizzazione del progetto di risanamento per un importo di 3,9 milioni di franchi. L'UFPP partecipa con un sussidio di 2,1 milioni di franchi, mentre la polizia cantonale contribuisce con 130'000 franchi.
Neppure un mese più tardi, l'8 dicembre 2016 hanno avuto inizio i lavori di risanamento. Hanno presenziato all'evento rappresentanti dell'UFPP, del comune di Gränichen dove si trova l'impianto, della scuola agraria Liebegg di Gränichen, dei pianificatori, del Canton Argovia e dello SMCC argoviese. Nello stesso mese sono state inoltrate al comune, per verifica e decisione, le domande di costruzione per l'antenna Polycom e GSM nonché per il nuovo pozzo di presa e di scarico dell'aria. Se i lavori procederanno secondo i piani, i lavori di risanamento saranno conclusi entro l'anno e l'impianto potrà essere consegnato allo SMCC già nel primo trimestre del 2018.

Protezione della popolazione nel Canton Berna

Conclusa l'analisi dei pericoli 2015

Con il titolo «Analisi dei pericoli 2015», il Canton Berna ha compiuto un'analisi sistematica dei rischi per i 352 comuni del suo territorio ed elaborato una guida per colmare le lacune esistenti nella pianificazione d'emergenza comunale.

Il Canton Berna sta effettuando dal 1995 delle analisi dei pericoli a livello comunale. La legislazione cantonale obbliga infatti i comuni a individuare periodicamente i principali pericoli che li minacciano.
Nell'ambito dell'analisi dei pericoli 2015, l'Ufficio della protezione della popolazione, dello sport e degli affari militari del Canton Berna (BSM) ha valutato, insieme agli specialisti e agli altri enti cantonali competenti, venti pericoli per tutti i comuni bernesi. Ora i comuni dispongono di un'analisi dei pericoli conforme agli standard metodologici attuali. Rispetto a quelle precedenti, questa analisi permette di confrontare tra loro sia i comuni, sia i diversi pericoli. Inoltre, ogni singola valutazione si basa su criteri chiari.
I risultati delle analisi dei rischi 2015 vengono pubblicati nel geoportale del Canton Berna e resi quindi accessibili al pubblico sotto forma di mappe. In tal modo, oltre a comunicare ufficialmente la conclusione del progetto, il BSM rafforza anche la consapevolezza dei rischi presso la popolazione.

Guida online per la «pianificazione d'emergenza»

L'analisi dei pericoli serve agli organi di condotta civili a livello comunale e di circondario per le loro pianificazioni in vista dei rischi rilevanti. Il BSM ha elaborato un'apposita guida sulla pianificazione d'emergenza per agevolare l'analisi dei pericoli e la valutazione dei rischi associati. Questa permette, sulla base di un semplice questionario, di individuare le lacune e di colmarle nell'ambito della pianificazione d'emergenza comunale. Per ogni pericolo considerato sono disponibili informazioni supplementari, modelli o promemoria che verranno completati e aggiornati man mano.

Per maggiori informazioni: www.be.ch/geoportal

I comuni bernesi dispongono di un'analisi dei pericoli conforme agli standard metodologici attuali.

Collaborazione tra Glarona e Grigioni

Istruzione congiunta di protezione civile

In futuro i militi della protezione civile glaronese verranno istruiti a Coira insieme ai loro colleghi grigionesi. I due cantoni hanno infatti sottoscritto una lettera di intenti.

I due cantoni di montagna Grigioni e Glarona hanno esigenze simili nel campo della protezione civile. Sfruttano già oggi numerose sinergie che accomunano gli orientamenti delle organizzazioni di protezione civile dei due cantoni. L'attuale struttura dei pionieri addetti alla lotta contro le epizoozie del cantone di Glarona si basa ad esempio sul concetto grigionese e agisce in stretta collaborazione.
La cooperazione è una grande opportunità per sviluppare ulteriormente le organizzazioni di protezione civile dei due cantoni ed affermare la sede Meiersboden di Coira come centro d'istruzione congiunto. Grazie a questa condivisione, i due cantoni si aspettano importanti risparmi. I militi della protezione civile glaronese, finora istruiti a Svitto, Cham e Sempach, dovranno fare meno strada per recarsi ai corsi e potranno pianificare in modo più flessibile la loro formazione.

Facce soddisfatte: in prima fila i consiglieri di Stato Christian Rathgeb (GR, a sinistra) e Andrea Bettiga (GL), in seconda fila (da sinistra) Martin Bühler, capo dell'ufficio grigionese del militare e della protezione civile, Daniel Spadin, segretario di dipartimento (GR) e Andrea Bottoni, capo della divisione glaronese del militare e della protezione civile.

Incendi nel Canton Grigioni

Grandi operazioni contro le fiamme e i focolai

Dal 27 dicembre 2016 al 12 gennaio 2017, un centinaio di squadre d'intervento sono entrate in azione per spegnere gli incendi divampati nei boschi della Mesolcina e della Val Calanca (GR) con il supporto di elicotteri militari e civili. La collaborazione tra i comuni colpiti, la polizia cantonale, i pompieri, il servizio forestale, le organizzazioni sanitarie, la protezione civile e l'esercito svizzero è stata molto efficiente e basata sulla fiducia reciproca.

La siccità protrattasi da metà novembre ha dato origine a diversi incendi boschivi, il 27 dicembre 2016 a Mesocco e Soazza in Mesolcina e il giorno successivo a Braggio in Val Calanca. A Mesocco sono state evacuate quattro persone da due case, mentre non è stato possibile raggiungere una terza abitazione per il pericolo di caduta massi. L'autostrada A13 e la strada cantonale H13 sono state temporaneamente chiuse per il pericolo di caduta massi. A Braggio le fiamme si sono avvicinate alle case fino a cinquanta metri. Gli incendi hanno distrutto oltre un centinaio di ettari di bosco di protezione, ma per fortuna non hanno fatto vittime. La linea ad alta tensione di Sils-Soazza, molto importante per il trasporto di elettricità attraverso l'Europa, non ha subito danni grazie al rapido intervento delle squadre antincendio.

La condotta è rimasta nelle mani delle forze di condotta locali per tutta la durata dell'intervento.

I pompieri e gli elicotteri di spegnimento sono riusciti a domare le fiamme in poco tempo. Nei giorni successivi, i pendii impervi sono stati battuti palmo a palmo per rintracciare e spegnere i numerosi focolai rimasti.

Forze congiunte

Alle operazioni hanno partecipato l'esercito svizzero, la polizia cantonale dei Grigioni, pompieri provenienti da tutto il cantone, il servizio forestale, il servizio regionale di soccorso, le aziende tecniche comunali e cantonale e la protezione civile. Per salvare i boschi colpiti sono stati complessivamente prestati più di mille giorni di servizio.
I lavori di spegnimento dei focali sono stati un'impressionante dimostrazione della collaborazione tra i partner coinvolti nelle operazioni. Grazie alle immagini delle termocamere impiegate dalle truppe militari di ricognizione e sull'elicottero FLIR, i forestali locali hanno potuto, insieme ai pompieri e ai militi della protezione civile, controllare metro per metro la superficie dei boschi bruciati. Gli elicotteri dell'esercito hanno irrorato i margini dei boschi di protezione, mentre quelli civili sono stati impiegati per spegnimenti mirati e soprattutto per il trasporto di personale e materiale. Oltre che a collaborare alle operazioni di spegnimento, i militi della protezione civile si sono occupati del vitto e dell'alloggio per le squadre d'intervento. I soldati, i militi della protezione civile e i pompieri si sono cameratescamente divisi il rifugio di protezione civile del comune di Soazza.

Responsabilità regionale – coordinamento cantonale

La direzione delle operazioni è rimasta per tutta la durata dell'intervento nelle mani degli organi di condotta locali. Nelle prime 48 ore, l'intervento è stato diretto dal capo della polizia regionale della Mesolcina. Dopo la riapertura degli assi stradali e la riattivazione delle linee ad alta tensione, egli ha ceduto la direzione all'ispettore locale dei pompieri.
Sia in Mesolcina che in Val Calanca, l'ingegnere forestale regionale è stato coinvolto nella definizione dei compiti prioritari sin dall'inizio delle operazioni di spegnimento. I membri dello stato maggiore cantonale di condotta responsabili per i pompieri, l'esercito e per la protezione civile erano sul posto per assistere e fornire consulenza alla direzione dell'intervento. Hanno presentato le richieste di aiuto all'esercito e si sono occupati di garantire il rinforzo con ulteriori forze d'intervento dei pompieri e della protezione civile dei Grigioni settentrionali.

Primi risultati e prime conclusioni

Il successo di queste operazioni di spegnimento dimostra che la collaborazione tra le organizzazioni di pronto intervento, il servizio forestale, la protezione civile e l'esercito funziona bene ed è valida. Nei prossimi mesi, i partecipanti valuteranno più in dettaglio l'intervento per trarre gli insegnamenti necessari per migliorare le procedure. I primi risultati e le prime conclusioni sono però già disponibili:

- Le prime reazioni e misure delle squadre d'intervento locali e regionali della polizia, dei pompieri, dei servizi di soccorso nonché degli ingegneri forestali regionali e delle guardie forestali locali sono state decisive per la continuazione delle operazioni. Si tratta ora di perfezionarle in previsione di altri grossi incendi. I responsabili delle regioni di tutto il Cantone devono infatti essere in grado di adottare autonomamente le prime misure e di preparare rapidamente l'infrastruttura di condotta necessaria.
- La protezione civile grigionese ha dimostrato di essere in grado di sostenere in modo tempestivo e polivalen-

I pionieri della compagnia di protezione civile Surselva spengono i focolai su un pendio ripido sopra il paese di Mesocco.

Sulla base delle informazioni fornite dall'esercito, l'ingegnere forestale regionale traccia le mappe per le squadre d'intervento dei pompieri e della protezione civile.

I pompieri della Val Calanca lavorano tutta la notte per impedire che le fiamme si propaghino al villaggio di Braggio. Sono stati danneggiati circa dodici ettari di bosco.

Senza l'intervento degli elicotteri di spegnimento dell'esercito, i boschi di protezione sopra Soazza e Mesocco sarebbero stati distrutti. Le Forze aeree hanno versato più di 2'400 tonnellate d'acqua sui boschi in fiamme.

te i pompieri e il servizio forestale. Ha garantito la capacità di resistenza per tutta la durata dell'intervento. Occorre però sviluppare e perfezionare le possibilità per accelerare e finalizzare la mobilitazione.

– Senza l'intervento degli elicotteri di spegnimento dell'esercito non sarebbe stato possibile salvare i boschi di protezione sopra Soazza e Mesocco. Per l'esercito svizzero è stata la più grande operazione antincendio da vent'anni a questa parte. Ha nuovamente dimostrato di essere un partner semplice, affidabile e indispensabile. L'ottima collaborazione con l'esercito, non solo in caso di sinistro, è un presupposto molto importante soprattutto a Grigioni.

Martin Bühler
Capo dello Stato maggiore cantonale di condotta Grigioni

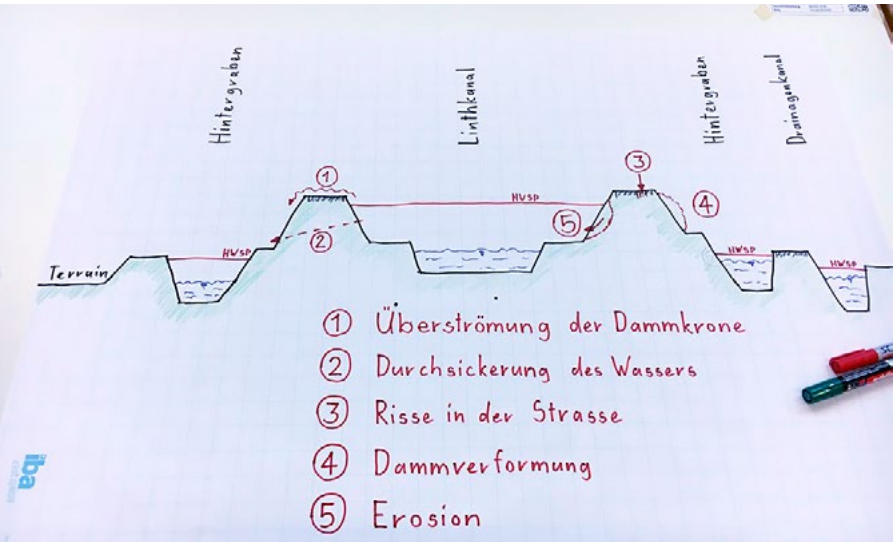
Esercitazione di stato maggiore SMCI Linth 16

Gestione congiunta di eventi sovracantonali

Affrontare in modo coordinato le conseguenze di un'ondata di maltempo e delle successive piene: questo il compito dello stato maggiore di coordinamento incercantonale Linth (SMCI Linth) nell'ambito dell'esercitazione di stato maggiore SMCI LINTH 16.

Il Canale della Linth collega il Walensee con il Lago di Zurigo. Lungo questo percorso traccia il confine tra i Cantoni di Glarona, Svitto e San Gallo. Considerato l'elevato pericolo di piene in caso di maltempo nella zona di deflusso del canale della Linth e del Canale Escher, i tre cantoni hanno allestito delle pianificazioni d'emergenza e istituito lo stato maggiore di coordinamento intercantonale Linth (SMCI Linth), cui hanno affidato il compito di gestire le piene nella pianura della Linth. L'ubicazione di condotta equipaggiata della più moderna infrastruttura si trova a Kaltbrunn (SG).

Per gestire le piene nella pianura della Linth, i Cantoni di Glarona, Svitto e San Gallo hanno creato lo «stato maggiore di coordinamento intercantonale Linth».



La situazione è stata rappresentata sia elettronicamente, sia con i mezzi convenzionali.

Sostegno dell'UFPP e dell'UFAM

L'esercitazione di stato maggiore SMCI Linth 16 svolta nel 2016 ha dimostrato che lo SMCI Linth è pronto a gestire un evento e che la collaborazione con i tre stati maggiori di condotta cantonali (SMC) funziona. L'esercitazione è stata diretta dall'Ufficio federale della protezione della popolazione (UFPP) e ha coinvolto specialisti dei tre cantoni e dell'Ufficio federale dell'ambiente (UFAM).
Lo scenario dell'esercitazione prevedeva una piena straordinaria della Linth, causata da piogge intense e persistenti e temperature sempre più miti, che hanno portato allo scioglimento delle nevi. Oltre alle perturbazioni e ai danni ingenti causati dalle piene nei cantoni colpiti, le organizzazioni di condotta cantonali hanno dovuto gestire anche numerosi altri eventi.

Scambio di informazioni

L'esercitazione, durata un giorno, ha permesso di addestrare il personale nello svolgimento di numerose attività: garantire i collegamenti tra gli stati maggiori cantonali di condotta (presso le loro ubicazioni) e lo SMCI, scambiare le valutazioni e le informazioni sulla situazione, pianificare l'impiego dei mezzi, consultarsi con il servizio di sorveglianza della Linth e applicare i processi di condotta conformemente alla situazione. Si è trattato in particolare di impiegare il sistema radio di sicurezza Polycom e il sistema d'informazione e d'intervento (IES). L'esercitazione è inoltre servita a verificare la sorveglianza degli argini.

La protezione civile e il sistema IES hanno dimostrato il loro valore

La valutazione dell'esercitazione è stata positiva: l'aiuto alla condotta della protezione civile ha contribuito in modo significativo ad assicurare la capacità di condotta dello stato maggiore, e l'impiego della presentazione elettronica della situazione tramite IES si è dimostrata valido. La direzione dello SMCI Linth ha potuto ricorrere in qualsiasi momento a un quadro attuale della situazione nei tre cantoni e ai risultati della sorveglianza degli argini. La protezione civile ha assicurato la sorveglianza degli argini in modo ottimale.
La direzione dell'esercitazione ha costatato che la collaborazione tra i tre cantoni è ottimale e che lo SMCI Linth è in grado di gestire queste situazioni con successo. La discussione dell'esercitazione è stata trasmessa in diretta via skype nelle tre ubicazioni di condotta degli SMC di Glarona, Svitto e San Gallo.

Esercitazione militare-civile in caso di catastrofe nel Canton Appenzello

Palestra d'addestramento per le organizzazioni civili

Durante l'esercitazione con truppe al completo «Technico 16», svoltasi dal 25 al 28 ottobre 2016, un migliaio di forze d'intervento civili e militari hanno lavorato fianco a fianco. L'esercitazione, concepita dall'esercito, è stata preparata in collaborazione con i partner civili.

Una pioggia di meteoriti causa danni ingenti in tutto il cantone: edifici in fiamme, strade danneggiate, numerose vittime e senzatetto, danni a boschi e colture. Era questo lo scenario dell'esercitazione «Technico 16», concepita come addestramento militare della Regione territoriale 4 ed essenzialmente svolta dal battaglione d'aiuto in caso di catastrofe 4 con il sostegno della protezione civile.

L'unione fa la forza

Una cosa era chiara sin dai primi preparativi, iniziati un anno prima dell'esercitazione: per sfruttare appieno il potenziale d'apprendimento bisognava coinvolgere le autorità, gli stati maggiori e le organizzazioni d'intervento civili già nella fase di pianificazione. I partner civili hanno quindi preparato e seguito dall'inizio alla fine le singole parti dell'esercitazione.
Di regola, i primi ad entrare in azione in caso di catastrofe sono le organizzazioni di primo intervento. L'esercito viene impiegato solo a titolo sussidiario, quando le forze d'intervento civili non sono più sufficienti e il Cantone è costretto a chiedere rinforzi alla Confederazione. Questo iter doveva essere rispettato anche nel copione dell'esercitazione. L'esercitazione è iniziata con una chiamata alle centrali operative. Una regia ha fornito gli input relativi alla situazione. Gli organi di condotta civili con le loro unità di aiuto alla condotta hanno effettuato una ricognizione e una valutazione delle piazze sinistrate e deciso in merito agli interventi necessari. L'impiego sussidiario dell'esercito ha fatto seguito a una richiesta d'aiuto del Cantone pervenuta al Comando della regione territoriale. Quando sono giunte sul posto, le truppe hanno concordato gli incarichi da svolgere e preso in consegna le piazze sinistrate dalle forze d'intervento civili.

Numerose sinergie

Sulla piazza sinistrata, la competenza delle forze d'intervento assume un ruolo centrale. Questa potrebbe essere addestrata singolarmente da ogni organizzazione. Tuttavia un addestramento unilaterale non costituisce solo uno spreco di risorse, ma anche una simulazione poco realistica delle operazioni. Il successo di un intervento in caso di catastrofe dipende dall'efficienza e dalla qualità della collaborazione delle organizzazioni coinvolte a tutti i livelli. I processi di questa cooperazione devono essere addestrati in modo particolarmente attento e consapevole. Questo è possibile solo se le sinergie vengono definite e preparate di comune accordo. Ciò vale in particolare per la comunicazione relativa all'esercitazione, che in caso di reale emergenza viene sempre gestita dalle autorità civili.

I militi della protezione civile del Canton Appenzello esterno preparano l'ex-deposito delle munizioni di Teufen per l'esercitazione «Technico 16».

L'esercito impegnato nell'esercitazione di un'operazione di salvataggio presso la piazza delle macerie preparata dalla protezione civile.

Una grande opportunità per i partner civili

Il Canton Appenzello esterno ha colto questa opportunità di scambio e di collaborazione, partecipando attivamente e con molto impegno alla pianificazione, allo svolgimento e alla discussione finale. Grazie alla disponibilità dell'esercito, il successo è stato grande quanto l'esercitazione stessa!

Gunnar Henning, coordinatore delle zone della Federazione svizzera della protezione civile FSPC

Un meritato congedo

Ora che nel nuovo organigramma della Federazione svizzera della protezione civile (FSPC) tutte le posizioni di responsabile di zona sono state occupate, «Mister protezione civile» Gunnar Henning ha deciso di ritirarsi: nel 2018 non lavorerà più per la Federazione.

Dopo tre anni, Gunnar Henning può finalmente esultare: «Evviva, tutte le zone sono occupate!». Non è stato sempre facile trovare persone interessate e competenti, disposte ad assumersi questa responsabilità. Per fortuna, all'inizio della riorganizzazione erano già disponibili quattro persone: tre delegati di zona e lui stesso, già membro del comitato della FSPC. «Ciò ha reso le cose molto più semplici».

Argomenti validi

Il coordinatore delle zone ha sempre da parte validi argomenti per convincere i potenziali candidati che sono attivi nella protezione della popolazione a livello cantonale. «Chi s'impegna in una zona della FSPC, riceve tutte le informazioni più attuali dall'Amministrazione federale». Secondo Henning, infatti, molti cantoni sarebbero restii a diffondere integralmente tutte le novità provenienti da Berna. Egli difende gli interessi delle zone e porta le loro richieste e proposte fino alle cerchie più alte.
Rimangono vacanti solo alcuni posti di rappresentanti al terzo livello gerarchico. Nel nuovo organigramma saltano però all'occhio due caselle ancora colorate di rosso: Grigioni e Sciaffusa non si sono ancora decise a diventare membri. «Questo è un loro diritto», dice Henning, «ma è un gran peccato. Nella protezione civile occorrono maggiore dialogo e cooperazione».
Secondo Henning, per un investimento di soli tre centesimi per abitante i vantaggi sono notevoli. Gli argomenti da lui addotti a favore dell'adesione alla Federazione sono, oltre a informazioni di prima mano, l'accesso alle reti dei partner, la grande offerta di manifestazioni, congressi e seminari, e il diritto di voto in base al numero abitanti.
Henning si impegna tenacemente per la protezione civile da diversi decenni. «Mister protezione civile», come è stato benevolmente definito da un giornale della sua regione nella Svizzera Orientale, ha lanciato e seguito molte riforme. In particolare si è impegnato a favore di un'istruzione più intensiva e orientata alla pratica, di materiale migliore e di istruttori più professionali. Non c'era nulla che odiasse di più dei tempi morti.

Gunnar Henning, da anni al servizio della protezione civile e della protezione della popolazione.

Grande consenso

Quando Henning parla dei primi tempi in cui lavorava nella protezione civile sembra che sia stato ieri. «Sembravamo un esercito di dilettanti», racconta. Ma la truppa schernita e derisa di allora, che si ritrovava per montare letti di fortuna, è ormai morta e sepolta. «Oggi percepisco un grande consenso. Non siamo veloci come i pompieri, ma in caso di catastrofe naturale possiamo intervenire con più personale e più a lungo. La popolazione apprezza molto questo aspetto. Anche la motivazione dei militi è notevolmente migliorata nel corso del tempo».
Essendo pensionato dal 2013, professionalmente il 66enne non ha più niente a che fare con la protezione della popolazione. Ma anche l'impegno profuso a titolo onorifico nella protezione civile sta per finire per Gunnar Henning. In occasione dell'Assemblea generale del 2018 a Lucerna vuole essere congedato da tutte le sue funzioni di membro del comitato, capo zona e coordinatore delle zone. D'un canto ha già trovato il suo successore per la funzione di coordinatore delle zone, d'altro canto sostiene di non voler più essere attivo al fronte per paura di parlare solo del passato e perdere così credibilità.

Impiego di droni civili

Supporto dal cielo per la REDOG

I cani da salvataggio della REDOG ricevono supporto anche dal cielo. In futuro, i droni della Federazione svizzera dei droni civili (FSDC) supporteranno le squadre cinofile della REDOG per agevolare le ricerche di persone disperse in Svizzera, specialmente nelle zone estese, impervie e difficili.

Per una volta una joint-venture che non ha lo scopo di realizzare utili, ma di salvare vite umane. Per cercare i dispersi, le squadre della Società svizzera per cani da ricerca e salvataggio REDOG si avvalgono di telecamere termiche e visori notturni. Ma in zone estese o impervie l'aiuto fornito da questi ausili tecnologici è limitato. La collaborazione con la Federazione svizzera dei droni civili (FSDC) permette di colmare questa lacuna. I droni, equipaggiati di telecamere termiche, supporteranno le ricerche dal cielo.

In futuro, le squadre cinofile di REDOG potranno contare anche su un supporto dal cielo.

L'unione fa la forza

Due associazioni volontarie con scopi diversi uniscono i loro sforzi per uno scopo comune. REDOG è un'organizzazione umanitaria della Croce Rossa Svizzera (CRS) che si occupa dell'addestramento di squadre cinofile per la ricerca e il salvataggio di persone disperse o sepolte dalle macerie. L'organizzazione conta circa 240 membri volontari e offre aiuto sia in Svizzera che all'estero. La FSDC rappresenta i piloti, gli operatori, i commercianti e i produttori dei droni in Svizzera e si adopera per la sicurezza, l'accettazione da parte della popolazione e l'integrazione nello spazio aereo dei droni.
La FSDC porta con sé la tecnologia e l'esperienza dei piloti dei droni, REDOG mette a disposizione la sua struttura d'allarme collaudata e raggiungibile al numero d'emergenza 0844 441 144, la sua direzione tecnica d'intervento e le sue squadre cinofile sempre pronte all'impiego. L'istruzione e l'addestramento degli specialisti della localizzazione tecnica di REDOG e della FSDC saranno adattati in vista delle operazioni congiunte. Durante gli interventi, i piloti dei droni e il personale di REDOG formeranno un'unica squadra.

«Collaborazione senza scopo di lucro»

Romaine Kuonen, presidente centrale di REDOG, afferma con soddisfazione: «Due importanti organizzazioni su base volontaria uniscono i loro sforzi per cercare in modo più efficiente i dispersi quando ogni minuto conta». E precisa: «Si tratta di una collaborazione umanitaria senza scopo di lucro».

Ueli Sager, presidente della FSDC, aggiunge che «in futuro si impiegheranno sempre più droni per la ricerca e il salvataggio di persone. La collaborazione tra REDOG e FSDC permetterà di unire l'esperienza di REDOG nel campo della ricerca di persone con la competenza tecnica e operativa della FSDC. Siamo convinti che questa collaborazione darà risultati importanti anche fuori dai confini nazionali».
«Up in the air». In futuro REDOG sarà supportata dal cielo, anche se i droni non saranno mai in grado di sostituire l'olfatto dei cani da salvataggio che operano a terra.

Per maggiori in formazioni:
www.redog.ch
www.drohnenverband.ch

Forum PBC 27/2016

Un Forum PBC «bestiale»

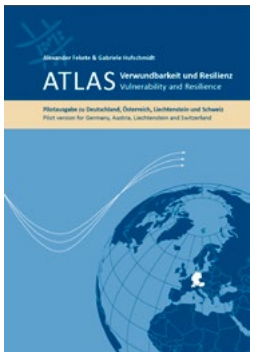
Animali e beni culturali, un accoppiamento dalle infinte sfaccettature, tutte da scoprire. Sin dall'antichità l'animale riveste una grande importanza per l'uomo, come minaccia, animale da reddito, fonte di cibo, vettore di significati religiosi e simbolici, cavia o compagno fidato nella vita quotidiana. Rimaniamo affascinati dagli animali che vediamo negli zoo, nei musei o in libertà. Questo stretto rapporto si riflette anche nei beni culturali che rappresentano animali su dipinti, sculture e statuette di diversi materiali. I musei, gli archivi e le biblioteche sono pieni di simili esempi. Oltre che sulle facciate di case, gli animali sono presenti su stemmi, mobili e mezzi di trasporto, nella letteratura, nelle favole, nei toponimi, nei cognomi, nel vocabolario corrente e anche in psicologia. Motivo più che sufficiente per dedicargli il numero 27/2016 di «Forum PBC».

Congresso internazionale sull'assistenza psicosociale d'urgenza 2017

«Dalla pratica – per la pratica»

L'Associazione svizzera per l'assistenza psicosociale d'urgenza (AS-APSU) organizza il 3° congresso internazionale sull'assistenza psicosociale d'urgenza, che si terrà Il 20 maggio 2017 presso il Campus di Sursee (LU). Il motto del congresso sarà: «Dalla pratica – per la pratica». Destinato ai membri delle forze d'intervento che prestano assistenza psicosociale d'emergenza e delle organizzazioni di crisi e di salvataggio, il congresso non offrirà solo un programma di conferenze su temi pratici, ma sarà anche un'ottima occasione per stringere contatti e scambiarsi esperienze.

Per maggiori informazioni: www.sv-psnv.ch



Pubblicazione

Atlante della vulnerabilità e della resilienza

Con i termini «vulnerabilità» e «resilienza» si descrive in che misura i pericoli hanno conseguenze sulla società. La scuola tecnica di Colonia e l'Università di Bonn hanno raccolto nell'Atlante VR («Atlas VR») vari progetti ed esempi in cui vengono applicati i due termini. Il volume bilingue (tedesco e inglese) contiene 46 studi modello compiuti in Germania, Austria, Liechtenstein e Svizzera.

Disponibile gratuitamente qui: www.atlasvr.de

IMPRESSUM

Protezione della popolazione 27 / Marzo 2017 (anno 10)

La rivista *Protezione della popolazione* in Svizzera è gratuita e disponibile in italiano, francese e tedesco.

Editore: Ufficio federale della protezione della popolazione UFPP

Coordinamento e redazione: P. Aebischer

Redazione: A. Bucher, Ch. Fuchs, D. Häfliger, M. Haller, K. Münger, N. Wenger

Traduzioni e revisione redazionale: Servizi linguistici UFPP

Contatto: Ufficio federale della protezione della popolazione UFPP, Informazione, Monbijoustr. 51A, CH-3003 Berna, telefono +41 58 462 51 85, e-mail info@babs.admin.ch

Fotografie: p. 1, 7, 9 e 11 Fotolia, p. 17 Protezione & Salvataggio Zurigo; altro UFPP/a disp.

Layout: Centro dei media elettronici CME, Berna

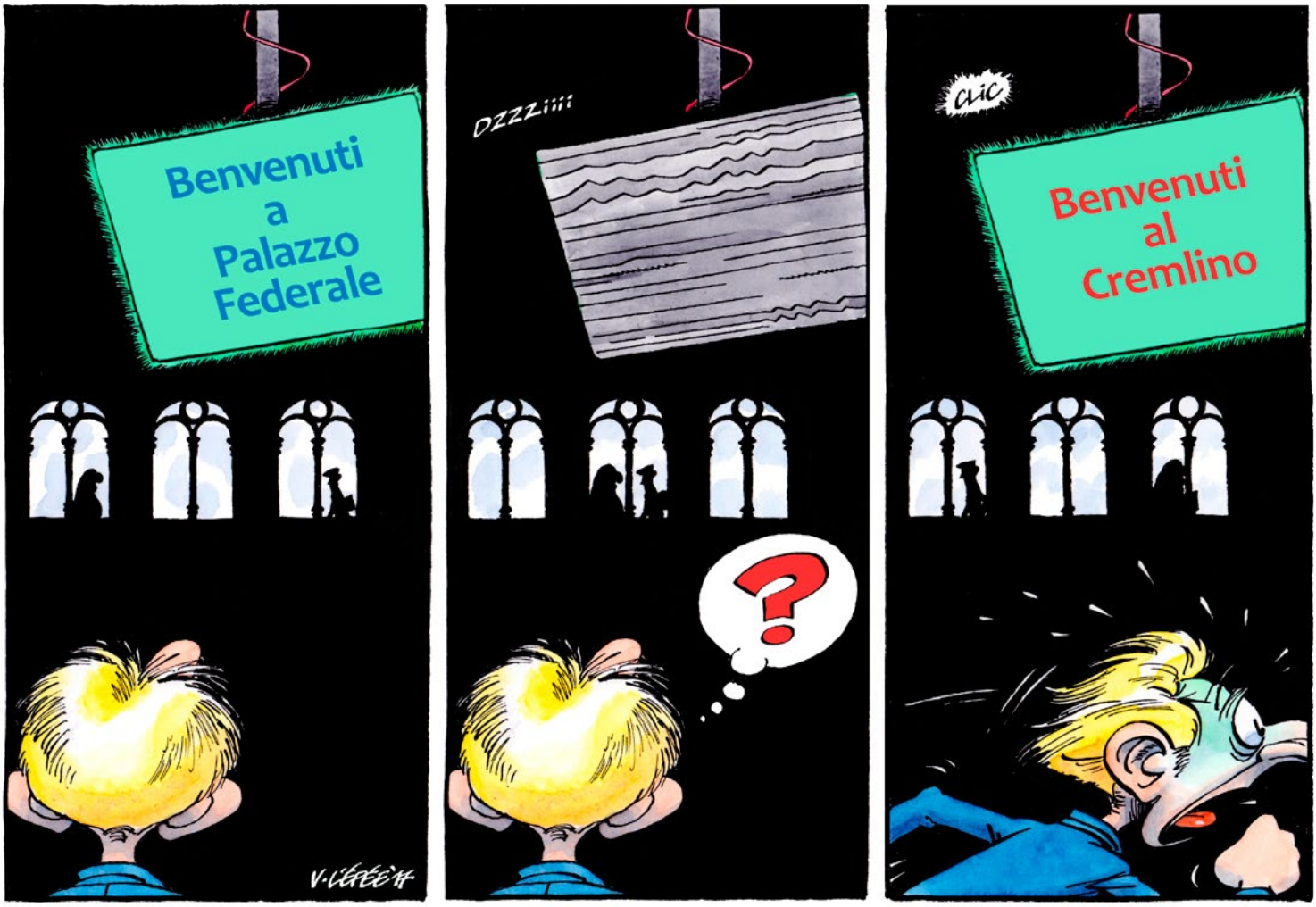
Tiratura: tedesco 8100 copie, francese 3100 copie, italiano 800 copie.

La rivista «Protezione della popolazione» è edita dall'Ufficio federale della protezione della popolazione (UFPP). Non è una pubblicazione ufficiale in senso stretto, bensì una piattaforma. Pertanto gli articoli non rispecchiano sempre il punto di vista dell'UFPP.

Cyber-rischi

Il punto di vista di V. L'Épeé

Vincent L'Epée lavora come vignettista per i quotidiani romandi «L'Express», «L'Impartial» e «Le Journal du Jura». I suoi lavori sono pubblicati anche sulla rivista bimestrale «Edito+Klartext» e saltuariamente nel settimanale «Courrier international». Risiede a Neuchâtel.



Prospettive N° 28, luglio 2017

Dossier

Organizzazione partner Sanità pubblica

Che cosa ne pensate?

Vi siamo grati per qualsiasi giudizio e suggerimento per i prossimi numeri.

info@babs.admin.ch

Ordinazione

La rivista dell'Ufficio federale della protezione della popolazione UFPP esce 3 volte all'anno in italiano, francese e tedesco.

Potete ordinare le riviste e gli abbonamenti gratuiti nel sito www.protpop.ch o all'indirizzo e-mail info@babs.admin.ch.

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Ufficio federale della protezione della popolazione UFPP

«La sfida consiste nel portare sotto lo stesso tetto la protezione delle informazioni e l'usabilità»

Nicoletta della Valle, direttrice di fedpol
Pagina 6

«Possiamo continuare a rallegrarci per le numerose innovazioni; ma dobbiamo anche accettare il fatto che bisogna proteggersi nel miglior modo possibile contro le minacce»

Max Klaus, vicecapo della Centrale d'annuncio e d'analisi per la sicurezza dell'informazione MELANI
Pagina 12

«Sembravamo un esercito di dilettanti»

Gunnar Henning, coordinatore delle zone della Federazione svizzera della protezione civile FSPC
Pagina 36

Ufficio federale della protezione della popolazione UFPP
Monbijoustrasse 51A
CH-3003 Berna
Telefono +41 58 462 51 85
E-mail: info@babs.admin.ch
www.protpop.ch