Aprile 2018 | www.odic.admin.ch

Strategia nazionale per la protezione della Svizzera contro i cyber-rischi 2018–2022

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Consiglio federale

Colofone

Editore

Organo direzione informatica della Confederazione ODIC
Schwarztorstrasse 59
CH-3003 Berna

info@isb.admin.ch
www.odic.admin.ch
intranet.odic.admin.ch

1 Introduzione

In Svizzera è in atto un processo di digitalizzazione. L'interconnessione digitale globale investe già oggi la società, l'economia e lo Stato e il rapido progresso tecnologico è destinato ad accelerare ulteriormente questa evoluzione. Il processo in corso offre grandi opportunità che la Svizzera è intenzionata a sfruttare per assicurare e consolidare il benessere del Paese a lungo termine.

Occorre tuttavia precisare che la digitalizzazione non cela solo nuove opportunità, ma anche molteplici rischi. La crescente dipendenza dalle tecnologie dell'informazione e della comunicazione (TIC) che scaturisce da questo fenomeno rende il nostro Paese più vulnerabile nei confronti di malfunzionamenti, guasti tecnici e utilizzi impropri delle tecnologie stesse.

La rilevanza di questa vulnerabilità emerge osservando l'evoluzione delle minacce presenti all'interno del cyberspazio. La cyber criminalità dilagante, l'intensificazione delle attività di spionaggio supportate da cyber attacchi, gli episodi di sabotaggio informatico di infrastrutture critiche come ospedali e fornitori di energia, la diffusione di informazioni rubate o manipolate per scopi di disinformazione e propaganda e l'aumento di forme ibride di conflitto che si avvalgono di cyber attacchi per destabilizzare società e Stati illustrano chiaramente la grande varietà di minacce esistenti e l'estrema rapidità con cui si sviluppano.

La crescente dipendenza da TIC funzionanti abbinata all'inasprimento della situazione di minaccia impone la necessità di tenere conto dei conseguenti rischi (detti «cyber-rischi») nello sviluppo della società digitale. A livello di politica di sicurezza occorre adottare una serie di misure volte a tutelare l'indipendenza e la sicurezza del Paese dalle nuove minacce e insidie che si profilano o intensificano all'interno del cyberspazio. Dal punto di vista della politica economica e sociale la Svizzera deve proteggersi dai cyber-rischi per poter sfruttare con coerenza le opportunità offerte dalla digitalizzazione e preservare il vantaggio competitivo di essere un Paese sicuro. Tuttavia, data l'impossibilità di ottenere una protezione completa dai cyber attacchi con misure proporzionate, la Svizzera deve aumentare la propria resilienza nei confronti dei cyber incidenti.

La presente Strategia nazionale per la protezione della Svizzera contro i cyber-rischi (SNPC) illustra le modalità per il raggiungimento di tali obiettivi entro il 2022. Essa si fonda sulla prima SNPC attuata nel periodo 2012–2017 e la sviluppa in funzione delle vulnerabilità del Paese, della situazione di minaccia nettamente mutata e inasprita dal 2012 a oggi e del relativo sviluppo previsto per il futuro, completandola con l'inserimento di ulteriori misure. Tale strategia costituisce così il quadro strategico per il miglioramento della prevenzione, dell'individuazione precoce, della reazione e della resilienza in tutti gli ambiti rilevanti sotto il profilo dei cyber-rischi.

La protezione dai cyber-rischi implica una responsabilità congiunta da parte dell'economia, della società e dello Stato, il che significa innanzitutto che tutti gli attori in gioco rispondono della propria protezione personale. Oltre a sostenere e coordinare questi sforzi individuali, la SNPC formula ulteriori provvedimenti negli ambiti in cui i cyber-rischi hanno delle ripercussioni significative sullo sviluppo e sul benessere della nostra società. Dalla responsabilità comune deriva anche l'attuazione congiunta della SNPC. La Confederazione, i Cantoni, l'economia e la società devono implementare le misure previste dalla SNPC collaborando strettamente tra loro e apportando le competenze acquisite in materia.

Poiché le sfide legate ai cyber-rischi continueranno a restare elevate è fondamentale che tutti i soggetti interessati le affrontino con un approccio coordinato e condiviso. Una collaborazione il più possibile efficace tra tutti gli uffici competenti e un'interconnessione internazionale sistematica sono due elementi fondamentali per la creazione di un ambiente sicuro per la digitalizzazione della società e dell'economia. La SNPC 2018–2022 elaborata congiuntamente da Confederazione, Cantoni ed economia deve fungere da guida operativa e da punto di riferimento in tale percorso. Il piano di attuazione della strategia definisce le competenze e le responsabilità di attuazione delle misure definite all'interno della strategia stessa.

2 Situazione iniziale

Per poter elaborare una strategia di protezione efficace della Svizzera contro i cyber-rischi occorre innanzitutto procedere a una valutazione della situazione di minaccia. Non si tratta di calcolare in modo preciso i rischi a cui è esposto il Paese, bensì di stimare la rilevanza strategica delle varie minacce e di formulare una previsione delle probabili tendenze evolutive di queste ultime.
Oltre alla situazione di minaccia, il secondo punto di partenza fondamentale è costituito dal livello attualmente raggiunto sul fronte della protezione della Svizzera contro i cyber-rischi. Confrontando le minacce e la loro evoluzione futura con il dispositivo esistente per la protezione della Svizzera contro i cyber-rischi si delinea con chiarezza la necessità d'intervento futura.

2.1 Cyber minacce

Per fare chiarezza sull'origine dei cyber-rischi, di seguito vengono descritte le principali minacce informatiche che incombono sulla Svizzera. Occorre precisare che tali minacce evolvono in maniera molto dinamica. Oltre alla digitalizzazione che rende la nostra società e la nostra economia sempre più vulnerabili nei confronti dei malfunzionamenti e guasti dei sistemi TIC, le principali cause di questo sviluppo sono costituite dall'inasprimento della situazione di minaccia, dovuto all'evidente professionalizzazione degli autori di attacchi informatici, e dall'espansione della politica di potenza nel cyberspazio. Dovendo partire dal presupposto che le tendenze in atto non si arresteranno, si deve prevedere un'ulteriore intensificazione della situazione di minaccia.
Ai fini della valutazione della situazione è importante operare una distinzione tra le minacce causate da atti intenzionali illeciti (cyber attacchi) e i pericoli derivanti da eventi causati involontariamente (comportamento umano scorretto e malfunzionamenti tecnici). Questi due elementi vengono descritti in paragrafi separati.

2.1.1 Cyber attacchi

Negli ultimi anni è stato registrato un netto aumento delle minacce perpetrate mediante cyber attacchi. Gli attacchi sferrati con successo in Svizzera e all'estero con conseguenze in parte gravi hanno dimostrato che, oltre diventare sempre più complessi e frequenti, tali attacchi sono rivolti in modo sempre più mirato contro Stati o aziende.
In considerazione della molteplicità dei possibili cyber attacchi, ai fini della valutazione della situazione è importante distinguere vari fenomeni mediante criteri come lo scopo degli attacchi, gli autori che li organizzano e la cerchia dei soggetti colpiti. Su questa base si possono individuare cinque diversi tipi di cyber attacchi, anche se occorre precisare che questi ultimi vengono spesso combinati tra loro e finiscono inevitabilmente per sovrapporsi.

Cyber criminalità: in senso stretto, per cyber criminalità si intendono i reati commessi con l'ausilio delle TIC o quelli che sfruttano le vulnerabilità di queste tecnologie e possono pertanto essere commessi soltanto mediante le TIC. In senso lato, rientrano nella cyber criminalità anche i reati commessi utilizzando le TIC e i supporti di memoria, ma che potrebbero essere commessi anche senza queste tecnologie. In contrapposizione alle minacce descritte di seguito, l'obiettivo principale della criminalità informatica è l'arricchimento. Il cyberspazio risulta particolarmente adatto a tale scopo in quanto presenta un rischio contenuto per i malfattori a fronte della possibilità di realizzare guadagni cospicui grazie al numero elevato di vittime facilmente raggiungibili. Non sorprende quindi che negli ultimi anni sia stato registrato un netto aumento della criminalità informatica, la quale colpisce in egual misura aziende, autorità e cittadini e costituisce la minaccia con la maggiore probabilità di realizzazione. Poiché il vero obiettivo degli aggressori non è quello di compromettere il funzionamento della società, dell'economia o dello Stato, le conseguenze immediate degli attacchi rimangono

spesso circoscritte alle vittime che li subiscono. Tuttavia, i cyber criminali sono pronti a correre rischi collaterali elevati o a sfruttare le conoscenze delle relative conseguenze per estorcere alle vittime somme più elevate. Per questo motivo gli attacchi da parte di criminali informatici celano un potenziale di danno elevato per l'intera società ed economia.
Nell'ambito della cyber criminalità si identificano veri e propri settori di attività in cui è possibile realizzare guadagni cospicui. A causa della forte concorrenza, ma anche del costante potenziamento delle misure difensive, i criminali informatici sono fortemente spronati a innovarsi, motivo per cui sviluppano costantemente nuovi metodi. Di conseguenza, si deve prevedere un ulteriore aumento della frequenza e della specializzazione delle attività criminali all'interno del cyberspazio.

Cyber spionaggio: si tratta di un'attività volta ad accedere illecitamente nel cyberspazio a informazioni protette, a fini politici, militari o economici che viene esercitata da attori sia statali sia non statali. Nel mirino degli autori degli attacchi informatici vi sono sia aziende sia istituzioni statali, sociali o internazionali. L'economia svizzera è una delle più innovative del mondo e molti gruppi internazionali hanno costruito qui la propria sede principale o importanti centri di dati. La Svizzera ospita inoltre numerose organizzazioni internazionali e non di rado importanti trattative internazionali. Tutto questo rende il Paese un bersaglio interessante per il cyber spionaggio. Le conseguenze possono variare notevolmente a seconda della tipologia e dell'entità dei dati a cui gli autori degli attacchi riescono ad accedere. Nella maggior parte dei casi gli effetti non sono immediatamente percettibili in quanto gli svantaggi politici ed economici si manifestano solo nel momento in cui gli hacker utilizzano le informazioni di cui sono entrati in possesso.
L'attrattività del cyber spionaggio è destinata ad aumentare in quanto esso costituisce un canale efficiente per procurarsi informazioni. Gli autori degli attacchi hanno escogitato diversi metodi per riuscire a mantenere il più a lungo possibile l'anonimato dopo essere penetrati all'interno delle reti. Poiché per il settore TIC la Svizzera dipende in larga misura dai produttori esteri, rimane il rischio che questi ultimi, in collaborazione con i servizi di informazione dei rispettivi Paesi, lascino volutamente aperte delle falle di sicurezza a scopo di spionaggio.

Sabotaggio e terrorismo informatico: il cyber sabotaggio è un'attività volta a perturbare o a interrompere il funzionamento affidabile ed efficiente delle TIC nel cyberspazio. A seconda del tipo di sabotaggio, una simile attività può avere anche ripercussioni fisiche. Le motivazioni alla base di tali atti possono essere molto varie. Episodi di sabotaggio informatico possono essere effettuati, per esempio, da collaboratori che, a causa della loro frustrazione, decidono di sabotare le TIC di un'organizzazione. Qualora un'azione di sabotaggio venga eseguita, invece, per motivi terroristici, si parla di cyber terrorismo. Gli atti di sabotaggio e terrorismo informatico non sono finalizzati unicamente a generare danni il più possibile ingenti, ma anche a costituire dimostrazioni di forza e intimidazioni volte a destabilizzare un'organizzazione o addirittura l'intera società. Mentre a livello internazionale si sono verificati vari atti di sabotaggio che hanno colpito anche l'approvvigionamento energetico di Stati, in Svizzera finora non sono stati registrati episodi di particolare rilevanza. Qualora la Svizzera oppure le organizzazioni svizzere o con sede in Svizzera dovessero finire per motivi politici nel mirino di attori statali o non statali in grado di sferrare simili attacchi, la probabilità di dover fronteggiare tali eventi aumenterebbe notevolmente. In questo caso i potenziali danni sarebbero molto ingenti.
La rilevanza di questa minaccia aumenterà ulteriormente con la progressiva digitalizzazione della società e dell'economia. La crescente interconnessione digitale di dispositivi fisici attraverso l'Internet delle cose ammette anche nuove forme di manipolazione digitale che hanno, a loro volta, ripercussioni dirette sull'ambiente fisico.

Disinformazione e propaganda: la minaccia costituita dalla diffusione mirata di informazioni false o acquisite illegalmente attraverso cyber attacchi allo scopo di screditare attori politici, militari e della società civile ha acquisito grande rilevanza. In diversi Paesi sono state riscontrate attività di questo tipo alla vigilia di importanti appuntamenti elettorali. Anche in Svizzera non si può escludere la possibilità che attori statali e non cerchino di minare la fiducia dei cittadini nello Stato e nelle istituzioni.
Poiché l'importanza dei social media come fonte di informazioni continua a crescere, si deve

altresì partire dal presupposto che questi canali vengano usati per la propaganda, mescolando informazioni false, argomentazioni politiche e informazioni rubate molto difficili da smascherare.

Cyber conflitti: mentre al giorno d'oggi l'ipotesi di una guerra condotta esclusivamente nel cyberspazio (*cyber-war*) appare irrealistica, è stato dimostrato che cyber attacchi di ogni genere vengono utilizzati come strumento di strategia militare in vari conflitti. Generalmente si tratta di conflitti ibridi nei quali, accanto agli strumenti militari, vengono impiegati anche mezzi politici, economici e criminali. Uno degli scopi della strategia ibrida è di dissimulare le responsabilità all'interno di un conflitto. I cyber attacchi sono uno strumento collaudato in tal senso in quanto, oltre a essere difficilmente classificabili in modo chiaro, a presentare costi relativamente contenuti e a ottenere un effetto immediato, possono essere utilizzati su grandi distanze e consentono di conseguire un effetto politico-militare nella zona grigia al di sotto della soglia bellica.

I cospicui investimenti effettuati da molti Stati per la protezione e la difesa attiva da cyber minacce sottolineano l'importanza assunta dagli strumenti informatici nei conflitti. Di conseguenza, si prevede che l'importanza degli attacchi informatici mirati a fini strategici aumenterà ulteriormente. La Svizzera deve pertanto includere la cyber difesa e la cyber diplomazia nella prevenzione di tali attività e nei preparativi a un eventuale scenario di questo tipo.

2.1.2 Errori umani e guasti tecnici

Oltre che da cyber attacchi mirati e deliberati, i danni nel cyberspazio o nell'ambiente fisico possono essere provocati anche da azioni non intenzionali o eventi naturali o tecnici, imputabili per esempio a errori umani nella predisposizione e nell'utilizzo delle TIC (p. es. un impiego inappropriato o incauto di sistemi TIC, un'amministrazione o una configurazione carenti, la perdita di supporti ecc.) o a guasti tecnici che possono essere originati, a loro volta, da diverse cause (p. es. infrastrutture obsolete o eventi naturali, sovraccarico, difetto di costruzione, manutenzione insufficiente). Eventi di questo tipo si verificano, in misura diversa, frequentemente e sono all'ordine del giorno nelle divisioni TIC di aziende e autorità. Di conseguenza, gli effetti di questi errori e anomalie sono di solito facilmente controllabili. L'esperienza dimostra, tuttavia, che dietro a molti incidenti informatici di grosse proporzioni non si nascondono attacchi mirati, bensì una concatenazione di vari fattori, come errori umani o guasti tecnici, collegati a una preparazione insufficiente. Nella pianificazione e nell'attuazione di misure di protezione non devono quindi essere trascurate misure preventive contro eventi di questo genere.

I cyber-rischi imputabili a tali problemi continueranno a giocare un ruolo centrale. La crescente complessità causata dall'interconnessione di ambiti svariati complica inoltre la possibilità di stimare e limitare le conseguenze di questi episodi non intenzionali. Una buona preparazione e una pianificazione accurata nei confronti di tali incidenti rimangono pertanto elementi centrali nella gestione dei cyber-rischi.

2.2 Stato della protezione della Svizzera contro i cyber-rischi

I lavori condotti finora si sono basati sulla prima SNPC che è stata approvata nel 2012 e attuata entro la fine del 2017. Occorre tenere conto però anche del contesto strategico della SNPC. La modalità adottata dalla Svizzera per proteggersi dai cyber-rischi viene influenzata in maniera diretta da varie strategie della Confederazione che creano così la base di partenza per gli interventi successivi.

2.2.1 Strategia nazionale per la protezione della Svizzera contro i cyber-rischi 2012–2017

La prima SNPC comprendeva 16 misure che sono state attuate in modo decentralizzato

dalle rispettive unità organizzative dell'Amministrazione federale in collaborazione con associazioni e gestori di infrastrutture critiche. I risultati della SNPC sono descritti in dettaglio nel Rapporto «Verifica dell'efficacia della SNPC»[1]. Gli obiettivi raggiunti della SNPC ed elencati di seguito sono importanti per la valutazione della situazione di partenza della SNPC 2018–2022:

- **acquisizione di competenze, abilità e conoscenze:** una delle priorità della SNPC era costituita dall'acquisizione di competenze, abilità e conoscenze all'interno delle rispettive organizzazioni. Nel 2012 si era constatato che molti settori non disponevano delle risorse e delle conoscenze tecniche necessarie. L'attuazione delle misure SNPC ha consentito un miglioramento della situazione;
- **organizzazione di processi, strutture e basi:** dato che i cyber-rischi riguardano una grande varietà di attori è stato fondamentale organizzare la collaborazione tra i vari uffici, suddividere le responsabilità ed elaborare le basi richieste a tale scopo. I processi, le strutture e le basi sono stati definiti e devono essere ora utilizzati e continuamente perfezionati;
- **particolare attenzione alla protezione delle infrastrutture critiche:** le misure della SNPC si sono concentrate innanzitutto sulla protezione delle infrastrutture critiche. Per i sottosettori critici sono state eseguite analisi dei rischi e della vulnerabilità, sono state identificate le misure da adottare, è stata potenziata l'assistenza in caso di incidenti ed è stata sviluppata una rappresentazione della situazione relativa alle cyber minacce. Questi lavori, che costituivano il fulcro della SNPC, possono essere ora approfonditi e ampliati;
- **rafforzamento della collaborazione con terzi:** oltre a migliorare il coordinamento all'interno dell'amministrazione è importante anche sviluppare la collaborazione con altri partner. La SNPC ha rafforzato la cooperazione con i Cantoni, il mondo economico e vari partner internazionali, il che ha consentito di rafforzare la fiducia reciproca e promuovere lo scambio di informazioni. In questo modo si creano delle valide premesse per un ulteriore approfondimento e ampliamento della collaborazione a tutti i livelli.

2.2.2 Contesto strategico

Le linee guida di riferimento per la tematica dei cyber-rischi si evincono da varie strategie elaborate dalla Confederazione che creano il contesto strategico per la protezione della Svizzera da tali rischi. Le strategie fondamentali a tale scopo sono le seguenti.

- **Rapporto del Consiglio federale sulla politica di sicurezza della Svizzera:** nel rapporto sulla politica di sicurezza stilato nel 2016 il Consiglio federale definisce l'orientamento strategico di fondo della politica di sicurezza della Svizzera. Questo documento illustra l'importanza significativa e crescente delle cyber minacce per la politica di sicurezza e definisce importanti concetti legati a tale tematica. Oltre a rinviare alla SNPC come base per la protezione della Svizzera contro i cyber-rischi, sottolinea che la protezione dei sistemi e delle infrastrutture TIC dovrà acquisire in futuro una rilevanza ancora maggiore.
- **Strategia del Consiglio federale per una Svizzera digitale:** la strategia mostra come la Svizzera intende sfruttare le opportunità offerte dalla digitalizzazione. Uno dei principali obiettivi strategici è creare trasparenza e sicurezza per consentire agli abitanti della Svizzera di esercitare il proprio diritto all'autodeterminazione informativa. A tale scopo è fondamentale che lo Stato assolva il proprio compito di proteggere la società e l'economia anche nell'era digitale. La strategia e il relativo piano d'azione definiscono, inoltre, gli obiettivi e le misure per il posizionamento della Svizzera nel contesto internazionale rispetto a questioni legate alla digitalizzazione e ai conseguenti processi di trasformazione. Nell'ambito della sicurezza informatica tale obiettivo deve essere raggiunto principalmente mediante l'attuazione della SNPC.

[1] https://www.isb.admin.ch/isb/it/home/themen/cyber_risiken_ncs/ncs_strategie-2012/wirksamkeitsueberpruefung.html

- **Strategia nazionale per la protezione delle infrastrutture critiche:** la strategia PIC definisce il concetto di «infrastrutture critiche» e indica i settori e i sottosettori ritenuti critici in Svizzera. Contiene altresì misure finalizzate a migliorare la resilienza della Svizzera in relazione alle infrastrutture critiche. La SNPC copre tutti i rischi per le infrastrutture critiche nel settore informatico.

2.3 Necessità d'intervento: sviluppo necessario della SNPC

Gli obiettivi raggiunti con la prima SNPC e il contesto strategico costituiscono la base per il proseguimento dei lavori. Il confronto tra la situazione di minaccia attuale e l'atteso sviluppo con il dispositivo esistente per la protezione della Svizzera contro i cyber-rischi mostra però chiaramente che il mantenimento dello status quo non basta per garantire un livello di protezione sufficiente. Occorre pertanto intervenire a diversi livelli. Da un lato, occorre rafforzare le capacità e le competenze esistenti e sfruttare i processi, le strutture e le basi creati per attuare le misure, dall'altro servono però anche adeguamenti strategici. La SNPC deve acquisire maggiore efficacia come strategia nazionale al di fuori dell'Amministrazione federale e delle infrastrutture critiche, a conferma del fatto che le cyber minacce investono l'intera economia, società e politica. A tale scopo occorre ampliare il target della SNPC e rafforzare la collaborazione avviata finora, creando dei collegamenti volti a sviluppare una rete per tutelare il Paese dai cyber-rischi. Infine, anche la struttura organizzativa decentralizzata deve essere integrata con una gestione strategica più forte e un servizio centrale di contatto per il pubblico in modo tale che, alla luce dell'elevata dinamicità dei cyber-rischi, si possa reagire in qualsiasi momento a nuovi sviluppi e assicurare che la SNPC possa essere recepita con maggiore chiarezza dal pubblico e dalla politica.

La tabella 1 riassume gli interventi necessari.

Livello	SNPC 2012–2017	Necessità d'intervento
Competenze, abilità e conoscenze	Miglioramento delle competenze e conoscenze rispetto al 2012.	È necessario ampliare ulteriormente le competenze acquisite per far fronte all'intensificarsi della situazione di minaccia.
Obiettivi delle misure SNPC	Creazione di processi, strutture e basi.	Utilizzo produttivo dei processi, delle strutture e delle basi al fine di ridurre i cyber-rischi. Le misure e i prodotti ideati devono essere implementati, perfezionati e, laddove necessario, integrati.
Struttura organizzativa	L'attuazione viene eseguita in modo decentralizzato dai rispettivi uffici.	La maggiore rilevanza politica, economica e sociale e la rapida evoluzione dei cyber-rischi rendono necessario un rafforzamento della gestione strategica della SNPC. La struttura organizzativa decentralizzata deve essere pertanto integrata.
Target	Focalizzazione sulla protezione delle infrastrutture critiche contro i cyber-rischi.	Poiché le minacce informatiche riguardano tutta la Svizzera è necessario ampliare il target della SNPC.
Collaborazione	Avvio della collaborazione con i Cantoni, il mondo economico e i partner internazionali.	L'interconnessione in costante aumento rafforza l'importanza della collaborazione a tutti i livelli. Le cooperazioni esistenti e i partenariati pubblico-privati devono essere rafforzate creando dei collegamenti volti a sviluppare una rete per la protezione della Svizzera contro i cyber-rischi.

La seconda SNPC deve portare avanti gli interventi attuati con la prima SNPC e, laddove necessario, ampliarli e integrarli con nuove misure. Essa deve altresì garantire la continuità con i lavori svolti fino a questo momento e assicurare che gli obiettivi, i principi, i campi d'intervento e i provvedimenti definiti siano in linea con gli sviluppi riscontrati dal 2012 e anticipino in modo ottimale le tendenze future.

3 Orientamento strategico della SNPC 2018–2022

Dalla necessità d'intervento individuata si desume l'orientamento strategico della SNPC 2018–2022. La visione e gli obiettivi strategici stabiliscono i risultati che ci prefigge di raggiungere nell'arco di tempo indicato, mentre i principi strategici descrivono le modalità con cui deve essere eseguito tale intervento. Nel paragrafo «Gruppi di destinatari» vengono definiti, infine, i destinatari a cui è rivolta la strategia.

3.1 Visione e obiettivi strategici

Dato che i cyber-rischi investono contemporaneamente diversi ambiti dell'economia, della politica e della società, è necessario adottare misure d'intervento a diversi livelli. Affinché la strategia resti coerente nella sua diversità, è fondamentale perseguire una visione comune e formulare obiettivi strategici generali.

Visione della SNPC 2018–2022

«Nell'utilizzo delle opportunità offerte dalla digitalizzazione la Svizzera è protetta in maniera adeguata dai cyber-rischi ed è resiliente nei confronti di questi ultimi. La capacità di agire e l'integrità della sua popolazione, dell'economia e dello Stato nei confronti delle minacce informatiche sono garantite».

Obiettivi strategici

La visione sopra descritta si concretizza nel momento in cui vengono raggiunti i sette obiettivi strategici della SNPC 2018–2022 elencati di seguito.

- La Svizzera dispone delle competenze, conoscenze e capacità necessarie per individuare precocemente i cyber-rischi e valutarli.
- La Svizzera sviluppa delle misure efficaci volte a ridurre i cyber-rischi e le attua nell'ambito del programma di prevenzione.
- La Svizzera dispone a tutti i livelli delle capacità e delle strutture organizzative necessarie per individuare tempestivamente i cyber-rischi e per gestirli qualora si protraggano per una certa durata e investano contemporaneamente diversi settori.
- La Svizzera è resiliente ai cyber-rischi. La capacità delle infrastrutture critiche di mettere a disposizione servizi e beni importanti continua a essere garantita anche in caso di incidenti informatici di una certa entità.
- La protezione della Svizzera contro i cyber-rischi viene percepita come un compito comune della società, dell'economia e dello Stato; le responsabilità e le competenze vengono definite chiaramente e assunte da tutti gli attori interessati.
- Oltre a impegnarsi a favore della cooperazione internazionale per aumentare la sicurezza informatica, la Svizzera promuove il dialogo sulla politica estera e di sicurezza informatica, collabora attivamente con gli organi specializzati internazionali e cura lo scambio con altri Stati e organizzazioni internazionali.
- La Svizzera analizza attentamente i cyber attacchi che si sono verificati all'interno e all'esterno del Paese traendone i necessari insegnamenti e definisce misure ad hoc sulla base delle conoscenze acquisite.

3.2 Principi

La visione e gli obiettivi strategici stabiliscono i *risultati* che ci si prefigge di raggiungere con la SNPC 2018–2022, mentre i principi definiscono le *modalità* di tale intervento.

- La SNPC parte da un **approccio globale basato sul rischio**, che considera tutte le vulnerabilità e minacce rilevanti e che ha l'obiettivo di migliorare la resilienza della Svizzera

sul fronte dei cyber-rischi. Implicita in tale approccio è l'idea che, pur non potendo garantire una protezione completa contro i cyber-rischi, sia possibile assicurare una gestione dei rischi fintantoché il rischio residuo sia sostenibile.

- La sicurezza informatica riguarda quasi tutti gli ambiti della vita, dell'economia e dell'amministrazione. Tutti devono agire e contribuire a proteggere la Svizzera contro i cyber-rischi. La SNPC rafforza questa responsabilità comune attribuendo agli attori le competenze richieste e sfruttando le strutture esistenti. Da ciò deriva un'**attuazione** decentralizzata che deve essere tuttavia controllata centralmente dalla gestione strategica della SNPC e prevedere una chiara suddivisione dei compiti e dei ruoli.
- La SNPC si fonda sull'idea di un **ruolo sussidiario dello Stato**, il che significa che l'intervento dello Stato è ammesso solo qualora il benessere della nostra società sia compromesso in maniera significativa e qualora gli attori privati siano impossibilitati o non intenzionati a risolvere autonomamente il problema. In questo caso lo Stato può offrire il proprio supporto, fornire incentivi o intervenire per regolamentare la situazione.
- La SNPC persegue un approccio cooperativo, rafforza e coordina i **partenariati pubblico-privati** esistenti, promuove altre cooperazioni in tale ambito e consolida la collaborazione tra Confederazione, Cantoni e Comuni.
- La SNPC promuove la **collaborazione con i partner internazionali** a livello globale.
- L'attuazione della SNPC avviene in modo trasparente, purché ciò non comporti una diminuzione dell'efficacia delle misure, mediante **una comunicazione attiva della strategia stessa** nei confronti della società, dell'economia e della politica.

3.3 Gruppi di destinatari

La Confederazione si impegna ad attuare le misure descritte nella SNPC in collaborazione con i Cantoni, l'economia e la società civile. L'effetto che si intende raggiungere con la SNPC interessa perciò tutto il Paese. La SNPC si rivolge in maniera esplicita ai gruppi di destinatari indicati di seguito:

- **infrastrutture critiche:** il principale gruppo di destinatari della SNPC è costituito dai gestori di infrastrutture critiche, che garantiscono la disponibilità di beni e prestazioni di servizi fondamentali. Il loro funzionamento è pertanto imprescindibile per la popolazione e l'economia svizzera. La protezione di tali infrastrutture ha la massima priorità ed è al centro di tutte le misure della SNPC;
- **autorità:** tra le infrastrutture critiche rientrano anche le prestazioni delle amministrazioni e delle autorità, la cui protezione compete direttamente alla Confederazione, ai Cantoni e ai Comuni;
- **popolazione:** la protezione della popolazione rappresenta lo scopo ultimo di tutte le misure della SNPC (p. es. la protezione da guasti delle infrastrutture tecniche), ma è collegata in maniera particolare alla cyber criminalità. La SNPC contribuisce, inoltre, a consentire alla popolazione una gestione sicura, informatizzata e affidabile delle TIC attraverso un'informazione trasparente;
- **economia:** la presenza di un contesto sicuro e affidabile costituisce una condizione importante e un vantaggio competitivo per l'economia. I cyber-rischi pongono non solo le infrastrutture critiche, ma anche tutte le restanti aziende e soprattutto le PMI di fronte a grandi sfide. La SNPC crea delle condizioni il più possibile sicure per le aziende della Svizzera e mette a loro disposizione, in via sussidiaria rispetto alle offerte del mercato, un supporto mirato per la gestione dei cyber-rischi.

4 Campi d’azione e misure della SNPC 2018–2022

Per raggiungere gli obiettivi strategici prefissati è necessario attuare misure in ambiti molto diversi. La SNPC distingue dieci campi d’azione che riguardano vari aspetti parziali dei cyber-rischi e all’interno dei quali vengono formulate complessivamente 29 misure.

Nella tabella 2 sono elencati i campi d’azione e le misure della SNPC 2018–2022.

Campo d’azione	Misure
Acquisizione di competenze e conoscenze	1. Individuazione precoce di tendenze e tecnologie e acquisizione delle conoscenze 2. Ampliamento e promozione delle competenze di ricerca e formazione 3. Creazione di condizioni quadro vantaggiose per un’economia della sicurezza delle TIC innovativa in Svizzera
Situazione di minaccia	4. Rafforzamento delle capacità di valutazione e rappresentazione delle cyber minacce
Gestione della resilienza	5. Miglioramento della resilienza delle TIC delle infrastrutture critiche 6. Miglioramento della resilienza delle TIC all’interno dell’Amministrazione federale 7. Scambio di conoscenze e creazione di basi per il miglioramento della resilienza delle TIC nei Cantoni
Standardizzazione / regolamentazione	8. Valutazione e introduzione di standard minimi 9. Verifica dell’obbligo di notifica dei cyber incidenti e decisione in merito alla relativa introduzione 10. Internet governance globale 11. Acquisizione di know-how su aspetti della standardizzazione collegati alla sicurezza informatica
Gestione degli incidenti	12. Potenziamento di MELANI come collaborazione tra settore pubblico e privato per i gestori di infrastrutture critiche 13. Elaborazione di prestazioni per tutte le imprese 14. Collaborazione della Confederazione con uffici e centri di competenza rilevanti 15. Processi e basi della gestione degli incidenti
Gestione delle crisi	16. Integrazione dei servizi deputati del settore cyber sicurezza negli stati maggiori di crisi della Confederazione 17. Esercitazioni comuni sulla gestione delle crisi
Perseguimento penale	18. Rappresentazione della situazione della cyber criminalità 19. Rete di supporto alle indagini per la lotta alla criminalità digitale 20. Formazione 21. Centrale per la cyber criminalità
Cyber difesa	22. Ampliamento delle capacità di acquisizione delle informazioni e di attribuzione degli attacchi informatici 23. Capacità di eseguire misure attive nel cyberspazio secondo SIC e LM 24. Garanzia della prontezza operativa dell’Esercito nel cyberspazio in ogni circostanza e regolamentazione del loro ruolo sussidiario di supporto delle autorità civili.
Posizionamento attivo della Svizzera nella politica di sicurezza informatica internazionale	25. Collaborazione e partecipazione attiva a processi della politica estera di sicurezza informatica 26. Cooperazione internazionale per l’acquisizione e lo sviluppo di competenze nell’ambito della sicurezza informatica 27. Consultazioni politiche bilaterali e dialoghi multilaterali sulla politica estera di sicurezza informatica
Visibilità e sensibilizzazione	28. Creazione e attuazione di un piano di comunicazione sulla SNPC 29. Sensibilizzazione dell’opinione pubblica sui cyber-rischi (consapevolezza)

I campi d’azione e le misure sopra indicati vengono descritti in dettaglio nei paragrafi successivi, mentre le competenze e le basi legali attuative, eventualmente ancora da creare, sono definite nel piano di attuazione separato.

4.1 Acquisizione di competenze e di conoscenze

Tabella sinottica del campo d'azione	
Descrizione	Per poter ridurre i cyber-rischi è fondamentale individuarli il più precocemente possibile e valutarli correttamente. Affinché gli attori dell'economia, della società e del mondo istituzionale possano riuscire in tale compito, è necessario che dispongano, da un lato, di un know-how di base e, dall'altro, di conoscenze tecniche specifiche. Le relative competenze devono essere create, veicolate e sviluppate trasversalmente attraverso gli istituti di formazione e ricerca esistenti. La sfida maggiore in tale ambito è costituita dalla varietà e dalla natura estremamente dinamica dei cyber-rischi.
Premessa	La Svizzera vanta una rete efficiente di istituti di formazione e ricerca a diversi livelli. A causa del rapido sviluppo dei cyber-rischi, la necessità di disporre di adeguate competenze e conoscenze in materia è fortemente aumentata. Attualmente si registra una carenza di conoscenze specifiche e di personale qualificato nei vari settori rilevanti per i cyber-rischi, il che complica lo sviluppo di un'efficace protezione contro i cyber-rischi e limita le possibilità dell'economia di posizionarsi sul mercato in crescita della sicurezza delle TIC. L'individuazione precoce delle tendenze e delle tecnologie importanti continua a rappresentare in generale una grande sfida. Finora non è stato eseguito nessun rilevamento sistematico e coordinato di queste tendenze e tecnologie includendo aspetti internazionali.
Obiettivi e necessità d'intervento	Il settore della formazione e della ricerca svizzero deve attribuire la giusta rilevanza al tema dei cyber-rischi e fornire alla società, all'economia e alle autorità le competenze necessarie e i risultati delle ricerche condotte in materia. Le nuove tendenze e tecnologie nell'ambito della sicurezza informatica devono essere individuate con tempestività in modo da poter reagire prontamente ai possibili rischi e avviare con la massima sollecitudine interventi ad hoc per contrastarli. L'economia deve disporre di sufficiente know-how e personale qualificato per affrontare con competenza i cyber-rischi e riuscire a sfruttare le opportunità offerte dal mercato emergente della sicurezza delle TIC. A tal riguardo è necessario verificare se le soluzioni di sicurezza delle TIC possano essere prodotte sempre più in Svizzera, rafforzando la collaborazione tra l'economia, la ricerca e lo Stato e quindi migliorando le condizioni quadro per la realizzazione, produzione e distribuzione di soluzioni innovative nell'ambito della sicurezza delle TIC. La ricerca nel campo della sicurezza informatica costituisce la base per il raggiungimento di questi obiettivi. Infatti, non solo è importante per lo sviluppo delle conoscenze specialistiche e l'individuazione precoce di tendenze e tecnologie, è anche in grado di creare un contesto attraente per il personale specializzato e le imprese innovative attraverso la condivisione delle conoscenze con il mondo economico. La ricerca deve essere pertanto coordinata al meglio a livello interdisciplinare.

Misure

1) Individuazione precoce di tendenze e tecnologie e acquisizione delle conoscenze

Le tendenze e tecnologie nel settore delle TIC devono essere individuate precocemente e a intervalli regolari, riconoscendo le opportunità e i potenziali rischi che ne derivano. I risultati di questo monitoraggio vengono comunicati agli attori del mondo scientifico, economico, politico e sociale. La ricerca di base e la ricerca applicata vengono promosse in funzione delle necessità e nel limite delle possibilità nell'ambito dei canali e processi esistenti (p.es. con i programmi nazionali di ricerca).

2) Sviluppo e promozione della formazione di competenze Mediante lo scambio tra il mondo economico, gli atenei, la Confederazione e i Cantoni si procede a un'analisi delle esigenze riscontrate a livello della formazione delle competenze sui cyber-rischi, esaminando in particolare la possibilità di integrare maggiormente tale tematica nei cicli di formazione attuali.
3) Creazione di condizioni quadro vantaggiose per un'economia della sicurezza delle TIC innovativa in Svizzera La Svizzera deve diventare una sede interessante per le aziende nel campo della sicurezza delle TIC. Un maggiore scambio tra il mondo dell'economia e della ricerca deve contribuire alla promozione di startup innovative in questo settore. Anche a tale scopo sono disponibili i canali esistenti citati nella misura 1. All'occorrenza vengono vagliate e implementate altre misure in collaborazione con le associazioni e le università per migliorare le condizioni quadro per le aziende che operano nel settore della sicurezza delle TIC.

4.2 Situazione di minaccia

Tabella sinottica del campo d'azione	
Descrizione	Come descritto nel capitolo relativo alla situazione di partenza, lo scenario delle cyber minacce è caratterizzato da vasta gamma di potenziali insidie che variano a seconda dello scopo dell'attacco, degli autori delle minacce e della cerchia dei soggetti colpiti. I confini tra le varie minacce sono spesso labili, in quanto gli hacker possono perseguire contemporaneamente vari scopi e persino combinare tra loro diversi obiettivi e tipologie d'attacco. Tale complessità e nebulosità, sommata all'elevata dinamicità con cui evolvono i cyber-rischi, complica la possibilità di avere un quadro completo delle cyber minacce. Tuttavia, una visione d'insieme di questo tipo è fondamentale per la protezione contro i rischi informatici in quanto, oltre a costituire la base per la scelta e la definizione delle priorità per le misure di prevenzione e reazione, è un elemento imprescindibile per adottare decisioni corrette in caso di incidenti e situazioni di crisi. A tale scopo occorre fare una stima delle minacce esistenti e dei relativi sviluppi futuri (descrizione e valutazione della situazione).
Premessa	Nell'ambito dell'attuazione della SNPC 2013–2017 sono state acquisite le competenze richieste per la descrizione e valutazione della situazione, l'individuazione precoce delle minacce e dei pericoli e l'attribuzione della paternità degli attacchi. Sono stati implementati i processi necessari per fornire una rappresentazione completa della situazione e le informazioni relative alle minacce sono state riassunte e rappresentate con l'aiuto di un grafico radar dinamico, interattivo e messe a disposizione delle autorità e dei gestori di infrastrutture critiche.
Obiettivi e necessità d'intervento	Per proteggersi dai cyber-rischi la Svizzera necessita tuttora di disporre di una rappresentazione della situazione globale. Alla luce dell'inasprimento della situazione di minaccia occorre potenziare le competenze già disponibili e intensificare lo scambio di informazioni con l'economia e i Cantoni. Attualmente non è possibile garantire una valutazione e una registrazione sistematiche dei cyber incidenti, in quanto le risorse esistenti vengono in gran parte assorbite dall'attività quotidiana. Nella valutazione delle minacce rilevanti per la Svizzera si deve raggiungere una maggiore profondità e precisione. Inoltre i risultati relativi alla situazione di minaccia non devono più essere messi a disposizione unicamente delle autorità e dei gestori di infrastrutture critiche, ma devono essere resi accessibili in forma adeguata anche ad altre aziende svizzere e alla popolazione.

Misure

4) Rafforzamento delle capacità di valutazione e rappresentazione delle cyber minacce

Le competenze finalizzate all'acquisizione, alla valutazione e alla verifica delle informazioni sulle cyber minacce all'interno del Servizio delle attività informative devono essere potenziate. A tale scopo è necessario utilizzare sistematicamente l'*Open Source Intelligence* (OSINT) e applicare le conoscenze tecniche a essa collegate, utilizzare strumenti tecnici, aggiornare e ampliare la rete di partner nazionali e internazionali. Le conoscenze acquisite in merito alle minacce informatiche devono essere elaborate in maniera sistematica, regolarmente aggiornate e rappresentate mediante il grafico radar della situazione in funzione dei gruppi di destinatari. Inoltre, è necessario predisporre una versione di tale grafico per il pubblico.

4.3 Gestione della resilienza

Tabella sinottica del campo d'azione	
Descrizione	Le infrastrutture critiche dipendono fortemente dal funzionamento e dalla sicurezza dei sistemi e delle infrastrutture TIC. Le misure volte a ridurre le vulnerabilità delle TIC delle infrastrutture critiche rivestono pertanto una grande importanza per la protezione della Svizzera contro i cyber-rischi. Esse non riguardano solo il potenziamento della difesa, ma includono anche provvedimenti volti a contenere i danni e a diminuire il periodo di inattività in caso di incidenti. L'obiettivo è migliorare la resilienza (capacità di resistenza e ripristino) delle infrastrutture critiche della Svizzera. Gran parte delle infrastrutture critiche della Svizzera viene gestita da aziende private. L'attuazione delle misure di miglioramento della resilienza delle TIC avviene a opera di queste ultime. Tuttavia, nell'ambito del suo mandato costituzionale volto a garantire la sicurezza nazionale, lo Stato è investito della responsabilità di proteggere le infrastrutture critiche e di garantire la disponibilità dei beni e delle prestazioni di vitale importanza per la popolazione e l'economia. Questo compito deve essere attuato in via sussidiaria e in stretta collaborazione con l'economia. Per questo motivo la Confederazione assume un ruolo attivo nella definizione di misure volte al miglioramento della resilienza delle TIC nei sottosettori critici e ne monitora l'applicazione. A seconda della misura, la relativa attuazione può avvenire a diversi livelli, per esempio delle aziende o del settore. Un caso speciale è costituito dalle infrastrutture critiche TIC delle autorità: la responsabilità dell'adozione delle misure compete qui alla Confederazione e ai Cantoni.
Premessa	Tra il 2013 e il 2017 l'UFAE e l'UFPP hanno identificato, in collaborazione con le autorità competenti, le associazioni e i rappresentanti di gestori di infrastrutture critiche, i rischi e le vulnerabilità TIC in 28 sottosettori critici e hanno elaborato insieme delle proposte di misure per migliorare la resilienza delle TIC (in parte già attuate). Per proteggere le proprie infrastrutture TIC, la Confederazione ha elaborato un piano mediante il quale assicura un'analisi periodica delle vulnerabilità dei sistemi TIC all'interno dell'Amministrazione federale. I Cantoni hanno effettuato delle analisi dei rischi nell'ambito di due progetti RSS per le loro amministrazioni.
Obiettivi e necessità d'intervento	Le misure identificate volte a migliorare la resilienza delle TIC nei sottosettori critici e nelle amministrazioni devono essere applicate e sviluppate sulla base di analisi dei rischi e delle vulnerabilità da aggiornare periodicamente. Tale intervento viene eseguito in accordo con le misure del campo d'azione «Standardizzazione e regolamentazione» e sfruttando effetti sinergici con i lavori in corso della Confederazione nell'ambito della protezione delle infrastrutture critiche, della gestione delle crisi, della protezione della popolazione (rete di dati sicura, SDVN+), dell'approvvigionamento economico del Paese, della gestione dei rischi presso la Confederazione, della sicurezza delle TIC e di altri uffici convolti.

Misure
5) Miglioramento della resilienza delle TIC delle infrastrutture critiche Questo intervento è finalizzato ad applicare le misure per migliorare la resilienza delle TIC dei sottosettori critici coinvolgendo le principali autorità di regolamentazione e gli uffici specializzati. Le basi sono costituite dalle analisi dei rischi e delle vulnerabilità esistenti e dalle conseguenti proposte di misure. Oltre all'implementazione delle misure identificate, le analisi e le misure devono essere aggiornate regolarmente e, se necessario, adeguate ai nuovi risultati e sviluppi.
6) Miglioramento della resilienza delle TIC all'interno dell'Amministrazione federale La resilienza delle TIC in questo ambito viene migliorata attuando il piano per l'analisi e la gestione delle vulnerabilità delle TIC all'interno dell'Amministrazione stessa. Il piano prevede di provvedere direttamente a selezionare le misure di sicurezza delle TIC da implementare opportunamente partendo dalle vulnerabilità individuate. Per migliorare la resilienza delle TIC si forma e sensibilizza in modo mirato il personale dei dipartimenti competente per la protezione delle infrastrutture TIC e per il trattamento operativo degli incidenti. Inoltre, la clausola sulla tutela del segreto nei contratti dell'Amministrazione federale con offerenti esterni è formulata in modo da consentire agli uffici competenti per la gestione degli eventi e agli incaricati della sicurezza informatica di trasmettere le informazioni sulle lacune e sugli incidenti di sicurezza ai dipartimenti interessati.
7) Scambio di conoscenze e creazione di basi per migliorare la resilienza delle TIC nei Cantoni Si procede alla creazione di una rete delle autorità (o all'utilizzo delle reti esistenti) al fine di effettuare uno scambio di esperienze e gettare delle basi comuni per rafforzare la resilienza delle TIC all'interno dei Cantoni. L'obiettivo è il supporto reciproco e l'individuazione di una procedura coordinata da parte delle autorità di Confederazione e Cantoni.

4.4 Standardizzazione / regolamentazione

Tabella sinottica del campo d'azione	
Descrizione	Le standardizzazioni e le regolamentazioni delle TIC sono strumenti importanti per la protezione contro i cyber-rischi. I requisiti minimi per i provvedimenti di protezione da adottare rafforzano la prevenzione e le disposizioni per la gestione degli incidenti (p.es. obblighi di notifica) contribuiscono a garantire una reazione più efficace. La standardizzazione e la regolamentazione sono importanti anche nel contesto internazionale, poiché creano più trasparenza e fiducia nella società digitale globalizzata. Introducendo standardizzazioni e regolamentazioni si deve però tenere conto delle grandi differenze esistenti tra i settori economici e le aziende di diverse dimensioni. I settori non sono esposti ai cyber-rischi nella stessa misura e le disponibilità finanziarie e di personale delle aziende divergono notevolmente. Le standardizzazioni e le regolamentazioni devono pertanto essere sviluppate e introdotte prevedendo una stretta collaborazione tra l'economia privata e lo Stato. Inoltre, in ogni caso di deve tenere in considerazione il contesto internazionale. A livello internazionale, gli standard e le norme devono essere possibilmente compatibili nel cyberspazio transfrontaliero. I lavori degli organismi di standardizzazione internazionali e lo sviluppo normativo nel contesto svizzero sono pertanto determinanti. Nell'ambito tematico della standardizzazione e regolamentazione rientrano anche i vari processi relativi all'Internet governance, istituita dal Vertice mondiale dell'ONU sulla società dell'informazione (VMSI), finalizzati all'elaborazione di principi, norme, regole e meccanismi decisionali relativi allo sviluppo e all'uso di Internet a livello internazionale. Nell'attuazione della linea d'azione VMSI C5 (sicurezza e fiducia) l'ITU assume il ruolo di moderatore di diversi progetti e attività. Inoltre, altri attori internazionali come l'OCSE o il Forum economico mondiale (WEF) hanno lanciato processi e attività finalizzati al miglioramento della sicurezza in ambito digitale. La priorità centrale del VMSI di coinvolgere tutti i gruppi d'interesse (approccio multistakeholder) tiene conto della crescente influenza esercitata dagli attori privati globali nella definizione di norme e regole nel mondo digitale e riconosce pertanto l'importanza della cooperazione tra soggetti statali e privati.
Premessa	Sono presenti diversi standard settoriali e alcuni generali per la sicurezza informatica. In collaborazione con l'economia è stato eseguito un primo bilancio della necessità di standardizzazione e regolamentazione nei vari settori. Gli sviluppi all'interno degli organismi di standardizzazione internazionali e nell'ambito della regolamentazione in altri Paesi sono noti. A livello europeo è stata approvata una direttiva sulla sicurezza delle reti e dell'informazione (NSI, *Network and Information Security*), attualmente in fase di attuazione da parte degli Stati membri, che prevede l'introduzione di standard minimi e di un obbligo di notifica dei cyber incidenti. Nell'ambito dell'Internet governance sono stati identificati gli organismi, i processi e gli eventi chiave per la Svizzera, sono state chiarite le competenze all'interno della Confederazione ed è stato garantito il coordinamento con tutti gli attori coinvolti grazie ai processi stabiliti attraverso la SNPC.

Obiettivi e necessità d'intervento	La crescente importanza delle standardizzazioni e regolamentazioni TIC è un aspetto di cui bisogna tenere conto. Standard minimi TIC vincolanti e verificabili sono rilevanti per la sicurezza e la fiducia nell'economia e società digitale e devono essere valutati e, laddove opportuno, introdotti in collaborazione con l'economia privata. Occorre inoltre valutare se e come occorre introdurre l'obbligo di notifica di cyber incidenti. Il contesto internazionale viene preso in considerazione nell'ambito delle misure che vengono influenzate in maniera significativa da quest'ultimo; i relativi sviluppi devono pertanto continuare a essere seguiti. La Svizzera partecipa ai processi principali apportando i propri interessi e valori.

Misure

8) Sviluppo e introduzione di standard minimi

Sulla base delle analisi dei rischi e delle vulnerabilità condotte si procede alla valutazione e all'introduzione di standard minimi TIC verificabili in stretta collaborazione con le autorità specializzate, l'economia privata e le associazioni. Laddove disponibili, gli standard esistenti vengono applicati e all'occorrenza adeguati. Le autorità competenti verificano le organizzazioni e le attività per cui è richiesta l'applicazione vincolante degli standard sulla base dei risultati delle analisi della vulnerabilità effettuate.

9) Verifica dell'obbligo di notifica dei cyber incidenti e decisione in merito alla relativa introduzione

Per migliorare la rappresentazione della situazione delle cyber minacce si deve valutare la possibilità di introdurre un obbligo di notifica per i cyber incidenti. Tra i vari aspetti da chiarire vi sono innanzitutto il target a cui deve essere applicato tale obbligo, gli incidenti che deve riguardare e l'organo a cui deve essere effettuata la notifica. Occorre altresì verificare se l'introduzione di un obbligo di notifica consente di migliorare in maniera sostanziale la rappresentazione della situazione rispetto a oggi. Vengono elaborate diverse varianti per l'attuazione di obblighi di notifica nei vari settori e vengono illustrate le basi giuridiche richieste a tale scopo. Tale intervento viene effettuato con il coinvolgimento delle rispettive autorità, dell'economia privata e delle associazioni, in coordinamento con la strategia nazionale per la protezione delle infrastrutture critiche e tenendo conto degli sviluppi internazionali. Sulla base di questi chiarimenti verrà presa in seguito una decisione in merito all'eventuale introduzione dell'obbligo in oggetto e, all'occorrenza, saranno adottate le misure necessarie.

10) Internet governance globale

La Svizzera deve impegnarsi in modo attivo e coordinato per creare un regolamento internazionale relativo all'utilizzo e allo sviluppo di Internet che sia conciliabile con gli ideali svizzeri di libertà, democrazia e responsabilità (individuale), servizio di base, pari opportunità, sicurezza, diritti umani e stato di diritto. A tale proposito devono essere coinvolti i soggetti portatori di interessi nazionali cui devono essere illustrati i principali sviluppi.

11) Acquisizione di know-how su aspetti della standardizzazione collegati alla sicurezza informatica

La Confederazione istituisce un pool di esperti per questioni in materia di standardizzazione legate all'ambito della sicurezza informatica. Questo pool di esperti consiglia i regolatori nello sviluppo e nell'attuazione di normative, linee guida o standard specifici sull'argomento. Tale organo assiste all'occorrenza i Cantoni, monitora lo sviluppo internazionale a livello di standardizzazione e regolamentazione e procede a uno scambio in merito con l'economia, contribuendo così alla creazione di una procedura coordinata e in linea con gli sviluppi internazionali.

4.5 Gestione degli incidenti

Tabella sinottica del campo d'azione	
Descrizione	Poiché non esiste un modo per proteggersi totalmente dai cyber attacchi e poiché dobbiamo aspettarci un aumento del numero di attacchi mirati, la creazione e il mantenimento di un'organizzazione incaricata della gestione degli incidenti (*incident management*) costituiscono un compito fondamentale della gestione dei rischi informatici. Il concetto di gestione degli incidenti copre una serie di attività che vanno dal riconoscimento tempestivo degli stessi, all'identificazione e alla messa in atto delle contromisure adeguate fino all'analisi degli incidenti da cui trarre informazioni utili a migliorare la prevenzione. Per far fronte a questo compito servono competenze specialistiche, strumenti di analisi, un'organizzazione ben funzionante e una stretta collaborazione tra tutti gli uffici interessati. È fondamentale lo scambio di informazioni su incidenti e possibili contromisure tra partner affidabili, perché spesso gli incidenti coinvolgono più uffici contemporaneamente e quindi possono essere gestiti con maggiore rapidità ed efficacia se le informazioni pertinenti vengono condivise da tutte le parti in causa. La condivisione e la valutazione delle informazioni richiede un coordinamento a livello centrale, affinché la portata strategica e per la politica di sicurezza di un incidente possa essere identificata il prima possibile e gli organismi competenti possano essere informati. Per la Confederazione si tratta, tra l'altro e a seconda del genere e della portata degli eventi, del Comitato ristretto Sicurezza e della Giunta del Consiglio federale in materia di sicurezza (GSic).
Situazione iniziale	Per gestire i cyber attacchi, in Svizzera molte organizzazioni si sono dotate internamente di team specializzati oppure hanno affidato l'incarico a società esterne. Questi team hanno denominazioni diverse (p. es. *response teams, computer security incident response teams*) e competenze specifiche nel settore in cui si trovano a operare. Anche la Confederazione e molti Cantoni dispongono di analoghi team, ed è a loro che è affidata in primo luogo la gestione degli incidenti. A sostegno dei gestori di infrastrutture critiche, la Confederazione ha istituito la Centrale d'annuncio e d'analisi per la sicurezza dell'informazione (MELANI), un organo che funge da punto di contatto a livello nazionale e offre supporto per l'analisi tecnica e informativa degli incidenti, mettendo a disposizione anche la relativa piattaforma per lo scambio di informazioni. MELANI assume un ruolo coordinativo nella gestione degli incidenti anche all'interno dell'Amministrazione federale. Gli uffici interessati generalmente informano MELANI, che valuta le segnalazioni ricevute, inoltrandole ai servizi preposti. Tuttavia i processi non sono standardizzati e non è ancora dato sapere a partire da quale momento MELANI informi il Comitato ristretto Sicurezza e/o la GSic. Nel quadro della SNPC 2012–2017 sono state rafforzate le capacità di MELANI in termini di personale, ed è stata ulteriormente ampliata la collaborazione con i team specializzati interni ed esterni all'Amministrazione federale. In conseguenza di ciò, è cresciuto anche il numero delle aziende che hanno accesso alla piattaforma per lo scambio di informazioni e al supporto tecnico. Anche dopo questo ampliamento, i servizi di MELANI rivolti all'economia restano però focalizzati sui gestori di infrastrutture critiche.

Obiettivi e necessità di intervento	Con l'allargamento del gruppo di destinatari della SNPC, il supporto alle attività di riconoscimento, gestione e analisi degli incidenti deve essere esteso anche ad altre realtà, mantenendone invariato l'attuale livello qualitativo e continuando a garantire l'affidabilità dello scambio di informazioni con i gestori di infrastrutture critiche. La già stretta collaborazione con i rispettivi centri di competenze deve essere intensificata in maniera mirata, in modo da sfruttare quanto più efficientemente ed efficacemente possibile le limitate risorse specializzate di cui dispone la Svizzera. Oltre ad estendere e intensificare la collaborazione con terzi, la gestione degli incidenti richiede anche un miglioramento dei processi interni all'Amministrazione. Mentre ogni dipartimento deve disporre sostanzialmente della capacità di risolvere gli incidenti informatici in modo adeguato, MELANI deve essere pronta a fornire il necessario supporto sotto la guida dell'Organo direzione informatica della Confederazione (ODIC). Nel caso di incidenti che coinvolgono contemporaneamente più dipartimenti e/o che secondo la valutazione di MELANI rappresentano una minaccia alla sicurezza interna o esterna, gli eventi sono gestiti centralmente e unitariamente sotto l'egida dell'ODIC e con il coinvolgimento dei dipartimenti interessati. L'ODIC valuta immediatamente le conseguenze di un incidente informatico sul piano strategico e della politica di sicurezza coinvolgendo i dipartimenti interessati.

Misure

12) Potenziamento di MELANI come partenariato pubblico-privato (PPP) per i gestori di infrastrutture critiche

Si deve ampliare ulteriormente il supporto ai gestori di infrastrutture critiche. L'obiettivo è quello di coinvolgere tutti i settori critici nello scambio di informazioni, facendo in modo che avvenga sempre più anche a livello intersettoriale. Il potenziamento del PPP non deve in ogni caso prescindere dal mantenimento del livello qualitativo dei servizi attualmente forniti. Si deve definire con chiarezza quali sono i servizi cui hanno diritto i singoli membri della cerchia chiusa di clienti.

13) Creazione di servizi per tutte le imprese

MELANI allarga il gruppo di destinatari e sviluppa servizi nel campo della prevenzione e della gestione degli incidenti per un gruppo di destinatari più ampio e non limitato solo ai gestori di infrastrutture critiche. L'economia svizzera, e soprattutto le piccole e medie industrie, devono poter beneficiare del supporto di MELANI, fornito in via sussidiaria alle offerte disponibili sul mercato nel campo della protezione e della gestione degli incidenti.

14) Collaborazione della Confederazione con gli uffici competenti e i centri di competenze

Si deve rafforzare ulteriormente la già stretta collaborazione tra MELANI e altri uffici competenti a livello federale e cantonale. In considerazione del numero limitato di specialisti disponibili in Svizzera, si deve intensificare in maniera mirata la collaborazione con centri di competenze selezionati e migliorare il coordinamento, in modo da sfruttare quanto più efficientemente ed efficacemente possibile le risorse limitate.

15) Processi e basi della gestione degli incidenti nell'Amministrazione federale
Al fine di standardizzare la gestione degli incidenti nell'Amministrazione federale, viene elaborato un processo che indica i percorsi per le segnalazioni e le competenze e attraverso il quale viene garantito il coinvolgimento delle autorità di perseguimento penale e, in caso di incidenti rilevanti sotto il profilo strategico o della politica di sicurezza, la gestione degli incidenti da parte del Comitato ristretto Sicurezza e della (GSic). I dipartimenti definiscono un interlocutore preposto al coordinamento della gestione degli incidenti e all'ODIC viene conferita la facoltà di impartire istruzioni nella gestione degli incidenti. La comunicazione riguardo agli incidenti informatici è di competenza della Cancelleria federale. La coordinazione della comunicazione in caso di incidenti informatici riguardanti più dipartimenti avviene tramite la Cancelleria federale.

4.6 Gestione delle crisi

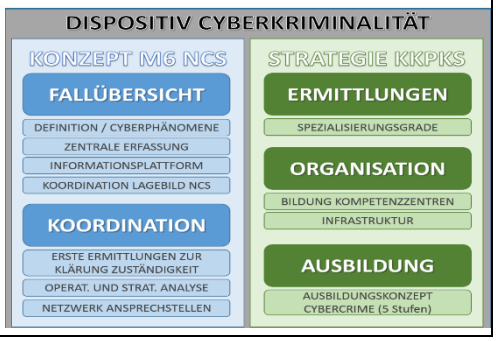
Tabella sinottica del campo d'azione	
Descrizione	Gli incidenti informatici possono avere gravi conseguenze e possono determinare un'escalation tale per cui diventa necessario gestire la crisi a livello nazionale. Ai fini della gestione delle crisi è determinante avere un quadro aggiornato, unitario e completo della situazione e disporre di processi decisionali efficaci oltre che di una strategia di comunicazione. La gestione delle crisi è per lo più indipendente dallo scenario specifico. Ciò significa che le procedure e i processi di condotta adottati dai Cantoni e dalla Confederazione per la gestione delle crisi in generale sono validi anche nel caso di crisi che presentano aspetti inerenti al cyberspazio. Tuttavia, in queste crisi è importante riuscire a supportare gli stati maggiori con conoscenze specifiche e ad assicurare un'intensa collaborazione tra tutti gli uffici competenti a livello federale e cantonale e il mondo dell'economia. Solo così si può arrivare a disporre in maniera chiara e tempestiva di tutte le informazioni importanti ai fini della gestione della crisi. Poiché la gestione di una qualsiasi crisi non consente alcuna perdita di tempo, è necessario elaborare dei piani di condotta e di comunicazione e imparare anticipatamente a conoscere i processi applicabili ricorrendo a esercitazioni pratiche.
Situazione iniziale	Per la gestione delle crisi che coinvolgono rischi informatici, partendo dai risultati dell'Esercizio di condotta strategica 2013 la Confederazione ha predisposto un piano per la gestione delle crisi che presentano aspetti inerenti al cyberspazio che, in collaborazione con i Cantoni e i rappresentanti dell'economia, è stato esteso diventando un piano per la gestione nazionale delle crisi del settore. Il piano è stato testato e gli esercizi fatti oggetto di analisi e valutazione, arrivando a concludere come l'elemento cruciale oltre che la principale sfida da affrontare quando si tratta di gestire crisi che presentano aspetti inerenti al cyberspazio sia la disponibilità di un quadro della situazione quanto più preciso e aggiornato possibile.
Obiettivi e necessità di intervento	Gli esercizi hanno evidenziato la necessità di potenziare le capacità di coordinamento a livello operativo e di rappresentazione della situazione. È necessario coinvolgere direttamente i servizi deputati del settore cyber sicurezza nella gestione delle crisi a livello di Confederazione, gestione che viene attuata dagli stati maggiori esistenti o creati ad hoc. Inoltre, si deve mantenere una collaborazione regolare con i Cantoni e il mondo dell'economia, affinché i partecipanti conoscano le rispettive competenze e i servizi che fungono da interlocutori.

Misure
16) Integrazione dei servizi deputati per la cyber sicurezza negli stati maggiori di crisi della Confederazione Per la gestione delle cyber crisi vengono impiegati gli stati maggiori di crisi già esistenti (Stato maggiore federale Protezione della popolazione e Stato maggiore di crisi dell'UFAE) o vengono creati degli stati maggiori ad hoc. Il settore cyber sicurezza, in quanto unione di organizzazioni specializzate, deve diventare parte integrante degli stati maggiori e deve disporre delle capacità che, in presenza di una crisi caratterizzata da aspetti legati alle tecnologie informatiche, le consentano di farsi carico del coordinamento tecnico e di formulare raccomandazioni all'indirizzo dello Stato maggiore di crisi. A tale proposito va inoltre chiarito quali facoltà di emanare istruzioni debbano avere le singole organizzazioni specializzate in caso di crisi.
17) Esercizi congiunti di gestione delle crisi Nel corso degli esercizi congiunti fatti da Confederazione, Cantoni e rappresentanti delle infrastrutture critiche viene messa alla prova la gestione delle crisi con particolare riferimento agli aspetti legati alle tecnologie informatiche. In tali occasioni, non solo si devono includere gli aspetti legati alle tecnologie informatiche negli esercizi generali, ma si devono anche effettuare esercizi specifici di gestione di crisi che presentano aspetti inerenti al cyberspazio. Gli esercizi vengono poi analizzati e concorrono a ottimizzare le procedure e i processi di condotta.

4.7 Perseguimento penale

Tabella sinottica del campo d'azione	
Descrizione	L'infrastruttura digitale che Internet ci mette a disposizione offre ai potenziali criminali nuove opportunità di commettere reati che possono arrecare enormi danni alla società e all'economia. Le restrizioni temporali e geografiche associate ai reati sono ormai pressoché inesistenti. La criminalità informatica oltrepassa qualsiasi limite territoriale, e lo fa nell'ambito di un processo estremamente dinamico con cicli d'innovazione brevi. Quanto più è forte l'interconnessione digitale tanto maggiore è il rischio che gli incidenti informatici, pur prendendo avvio nel mondo virtuale, possano sortire i loro effetti dannosi nel mondo reale. Alla luce di questi sviluppi, è opportuno trovare urgentemente nuove soluzioni anche per quanto riguarda il perseguimento penale. Le cose da fare su tutto il territorio nazionale e in collaborazione con partner internazionali sono migliorare l'interoperabilità e la capacità di reazione come pure coordinare efficacemente le competenze specialistiche, tecniche e personali senza per questo modificare l'attribuzione di poteri tra le diverse autorità e livelli statali.

Situazione iniziale	Un passo importante nella lotta contro la criminalità informatica è la predisposizione di una tabella sinottica nazionale dei casi. A tal fine è disponibile un programma consolidato, elaborato in collaborazione con i Cantoni. Inoltre, sono state definite misure finalizzate all'acquisizione centralizzata, al coordinamento e alla diffusione di informazioni sulla situazione in corso, misure di polizia per determinare le competenze territoriali e materiali ed è stato introdotto un processo di rilevamento e analisi della criminalità informatica. La tabella sinottica nazionale e il coordinamento intercantonale dei casi sono però soltanto due degli aspetti da affrontare nella sfida alla criminalità informatica. Altri aspetti, altrettanto importanti, dovranno ancora essere chiariti: tra questi, le indagini vere e proprie, le strutture nazionali e l'adeguata formazione a ogni singolo livello. È per questo che la Conferenza dei comandanti delle polizie cantonali (CCPCS) sta lavorando a un dispositivo nazionale denominato «Cybercrime e informatica forense», in cui si affrontano tutte queste questioni organizzative e infrastrutturali nel loro complesso e si procede all'attribuzione delle risorse necessarie.
Obiettivi e necessità di intervento	Il dispositivo nazionale per la lotta alla criminalità informatica della CCPCS e il relativo piano di attuazione devono comprendere tutti gli aspetti della lotta alla criminalità informatica, partendo dalla panoramica e dal coordinamento dei casi, passando per la formazione fino ad arrivare alle attività di indagine, e devono dimostrare quali passi compiere per adottare misure e piani.



Misure

18) Rappresentazione della situazione della criminalità informatica
La Confederazione (fedpol) e i Cantoni (CCPCS) analizzano e predispongono le condizioni quadro tecniche per l'elaborazione di un quadro nazionale di polizia che rifletta in tempo reale la situazione della criminalità informatica. Questi lavori vengono svolti congiuntamente al programma di armonizzazione dell'informatica della polizia.

19) Rete di supporto alle indagini nella lotta alla criminalità digitale
La Confederazione (fedpol) e i Cantoni (CDDGP) preparano un accordo amministrativo di collaborazione e coordinamento tra il centro di competenza informatico nazionale (National Cyber Competence Center, NC3) e i centri di competenza informatici regionali (Regional Cyber Competence Center, RC3) facenti parte della rete di supporto alle indagini nella lotta alla criminalità digitale.

20) Formazione sulla lotta contro la criminalità informatica
Nel quadro della collaborazione tra la Conferenza dei direttori delle polizie cantonali (CCPCS) e la Conferenza dei procuratori della Svizzera (CPS) vengono creati specificatamente programmi di formazione per lo sviluppo continuo delle competenze necessarie nell'ambito dei procedimenti penali.

21) Ufficio centrale per la criminalità informatica
Fedpol predispone la modifica della legge sugli Uffici centrali (LUC) al fine di creare un ufficio centrale per la criminalità informatica e le basi necessarie alla collaborazione con i Cantoni nella lotta contro la criminalità informatica.

4.8 Cyber difesa

Tabella sinottica del campo d'azione	
Descrizione	Attacchi informatici su vasta scala o mirati alle infrastrutture critiche della Svizzera possono compromettere la sicurezza della popolazione e dell'economia. Oltre a un'ampia serie di misure, che rafforzano la protezione dai cyber-rischi, sono perciò necessarie delle capacità e delle risorse sfruttabili in ogni circostanza per impedire attacchi in corso e per identificare gli attori responsabili degli stessi. Nel caso di attacchi che pregiudicano il funzionamento delle infrastrutture critiche, devono poter essere adottate le necessarie contromisure attive per assicurarne il funzionamento. La cyber difesa comprende pertanto tutte le misure che servono alla difesa generale dei sistemi critici e alla difesa da attacchi nel cyberspazio in ogni circostanza e cioè anche in caso di conflitto o di guerra.
Situazione di partenza	Con la legge federale sulle attività informative (LAIn) e la riveduta legge militare (LM) la Confederazione dispone delle basi legali necessarie per implementare e adottare misure e contromisure attive nell'ambito della cyber difesa. L'aumento degli attacchi informatici negli ultimi anni e la loro crescente complessità richiedono tuttavia un numero maggiore di risorse per lunghi periodi. Ciò espone al rischio di non riuscire a individuare tempestivamente più attacchi svolti contemporaneamente, in quanto i pochi specialisti a disposizione saranno occupati a risolvere gli altri casi che devono seguire. La scarsità di risorse intralcia la necessaria rielaborazione continua dei casi. Con il suo Piano d'azione per la cyber difesa (PACD) il DDPS ha rilevato una necessità d'intervento e di risorse nell'ambito della difesa informatica, ha definito i compiti dei differenti organi (in particolare l'Esercito) e ha descritto le misure che saranno adottate per adempierli.
Obiettivi e necessità di intervento	Il Servizio delle attività informative deve essere in grado, tramite l'acquisizione sistematica di informazioni e la successiva analisi, di scoprire il più rapidamente possibile nuovi modelli d'attacco. Inoltre deve poter effettuare un'identificazione dei responsabili di attacchi avvenuti (attribuzione della paternità) il più possibile precisa, in modo da tutelare la libertà d'azione delle autorità politiche e delle autorità di perseguimento penale. Nel caso di attacchi contro i gestori di infrastrutture critiche, il Servizio delle attività informative deve essere in grado, con il coinvolgimento di unità di supporto, di adempiere al proprio compito nel quadro della LAIn. L'Esercito ricopre un ruolo decisivo quale riserva strategica per l'appoggio sussidiario delle unità civili dell'amministrazione e nel caso di mobilitazione. A questo scopo deve poter assicurare la prontezza operativa nell'ambito della cyber difesa in ogni circostanza.

Misure

22) Ampliamento delle capacità di acquisizione delle informazioni e di attribuzione degli attacchi informatici

Le attuali conoscenze specifiche e le capacità di acquisizione delle informazioni per il riconoscimento precoce di attacchi informatici e per la loro attribuzione saranno ulteriormente sviluppate. Inoltre, sarà intensificata la collaborazione tra la Confederazione e i Cantoni in quest'ambito specifico e sarà ampliato lo scambio di informazioni con l'economia. Il Servizio delle attività informative della Confederazione conduce approfondite analisi degli attori e dell'ambiente, utilizza e sviluppa strumenti tecnici, la sorveglianza delle telecomunicazioni e metodi della *Human Intelligence (HUMINT)*. In questo modo gli attacchi informatici che sono stati perpetrati vengono sistematicamente trattati e seguiti.

23) Capacità di attuazione di misure attive nel cyberspazio secondo LAIn e LM
Il DDPS (SIC ed Esercito) ha competenze e capacità qualitativamente e quantitativamente sufficienti per arrestare o rallentare eventuali attacchi contro le infrastrutture critiche. L'impiego di tali misure avviene in conformità alle disposizioni della LAIn e della LM.

24) Garanzia della prontezza operativa dell'Esercito nel cyberspazio in ogni circostanza e regolamentazione del suo ruolo sussidiario di supporto delle autorità civili
Nell'ambito dell'ulteriore sviluppo dell'esercito (USEs), quest'ultimo garantisce la disponibilità di mezzi, risorse e competenze sufficienti per adempiere al proprio compito in situazioni straordinarie nel cyberspazio conformemente alla legge militare. Inoltre, l'Esercito deve assicurare la prontezza operativa per supportare sussidiariamente quale riserva strategica le autorità civili. A tal fine istruisce i propri quadri e militi e definisce insieme alle autorità civili federali e cantonali le condizioni quadro in base alle quali deve fornire un supporto sussidiario nel caso di incidenti informatici, quali compiti svolgere e quali casi concreti determinano un tale intervento.

4.9 Posizionamento attivo della Svizzera nella politica internazionale sulla sicurezza informatica

Tabella sinottica del campo d'azione	
Descrizione	Il cyberspazio ha creato una nuova dimensione della politica sulla sicurezza esterna. Il cyberspazio viene sempre più utilizzato dagli attori statali come luogo di proiezione di potere e per il raggiungimento di obiettivi politici, la realizzazione di progetti informativi e per scopi militari. Oltre all'utilizzo di mezzi informatici in conflitti armati tradizionali, sempre più spesso i conflitti si combattono anche nello spazio digitale. Per ridurre i cyber-rischi è quindi essenziale la collaborazione internazionale a livello sia diplomatico che tecnico-operativo. La tutela degli interessi della Svizzera in materia di politica estera e di sicurezza deve essere garantita anche nel cyberspazio. Pertanto, sia a livello diplomatico che a livello tecnico-operativo, la Svizzera si impegna in favore del rafforzamento della cooperazione internazionale per ridurre al minimo i cyber-rischi.
Situazione iniziale	L'importanza della cooperazione internazionale era già stata messa in evidenza nella SNPC del 2012. I processi e le strutture per una politica sulla sicurezza esterna in ambito informatico coordinata e coerente sono stati creati. Considerazioni riguardanti la politica della sicurezza sono presenti anche nella strategia «Svizzera digitale» varata dal Consiglio federale nel 2016. Nei processi internazionali importanti la Svizzera viene considerata un partner attivo, affidabile e meritevole di fiducia e la sua voce viene ascoltata. Per quanto concerne il cyberspazio, il nostro Paese si è molto impegnato a favore dello sviluppo e dell'attuazione delle prime misure per rafforzare la fiducia tra gli Stati. La Svizzera partecipa attivamente alla definizione dei processi multilaterali inerenti alla sicurezza informatica e si impegna per intensificare la cooperazione con Paesi e organizzazioni selezionati.

Obiettivi e necessità di intervento	Per ridurre al minimo i cyber-rischi è fondamentale avere una politica coerente in materia di sicurezza esterna in ambito informatico, che persegua l'obiettivo supremo di garantire un cyberspazio libero, aperto e sicuro. Per tutelare i propri interessi nei confronti di altri Stati e delle organizzazioni internazionali e per promuovere la pace, la stabilità e la sicurezza internazionale la Svizzera si avvale di diversi strumenti. *In primo luogo,* si impegna a favore del riconoscimento, del rispetto e dell'applicazione del diritto internazionale pubblico nel settore della sicurezza informatica e contribuisce a fare chiarezza su come si debba applicare il diritto internazionale esistente nel cyberspazio. *In secondo luogo,* si impegna attivamente affinché si consolidi il clima di fiducia tra gli Stati e *in terzo luogo,* supporta e sviluppa iniziative per accrescere le capacità nazionali e sviluppare le capacità degli Stati terzi. Per quanto riguarda quest'ultimo punto, occorre anche fare in modo che tutti o quantomeno il maggior numero possibile di attori interessati possano partecipare alle discussioni internazionali a sostegno della sicurezza informatica. In tutte le attività non viene tralasciata neanche la valorizzazione della Svizzera e della piazza internazionale ginevrina come piattaforma di discussione sulla politica in materia di sicurezza esterna in ambito informatico.

Misure

25) Ruolo attivo nella definizione e partecipazione ai processi di politica in materia di sicurezza esterna in ambito informatico

Per quanto riguarda la politica in materia di sicurezza esterna in ambito informatico, la Svizzera si impegna affinché venga sviluppato un dispositivo normativo, finalizzato all'utilizzo responsabile delle tecnologie dell'informazione e della comunicazione. Il suo impegno in tal senso si esplica nell'ambito dell'ONU, dell'OCSE e di altri importanti forum internazionali.
La sua azione va anche nella direzione di un'estensione del riconoscimento del diritto internazionale pubblico e contribuisce a chiarire questioni specifiche sulla sua applicazione (p. es. gruppo di esperti ONU e seguito dei processi, processo di Tallinn e altri).
Per la Svizzera vale il principio secondo cui i diritti dell'uomo sono gli stessi, sia nel mondo offline che nel mondo online. Per questo si impegna affinché sia garantita la tutela dei diritti dell'uomo anche nell'ambito delle interazioni della politica di sicurezza nel cyberspazio.
In seno all'OCSE e ad altri importanti forum la Svizzera si adopera a favore dell'attuazione e dello sviluppo di misure per consolidare la fiducia.
Infine partecipa attivamente alle discussioni in merito all'interfaccia tra sicurezza informatica e controllo degli armamenti e promuove lo sviluppo di know-how e di capacità in questo settore tematico.

26) Cooperazione internazionale per la crescita e lo sviluppo delle capacità nel settore della sicurezza informatica

Attraverso la collaborazione e lo scambio con altri Stati, organizzazioni internazionali o centri di ricerca specializzati (p. es. il Cooperative Cyber Defence Centre of Excellence) la Svizzera intende avvalersi del know-how estero e utilizzarlo per accrescere le capacità nazionali di minimizzazione dei rischi.
La Svizzera sostiene progetti e iniziative in altri Stati volti a sviluppare le capacità nell'ambito della sicurezza informatica (p. es. scambio di esperti per la creazione di istituzioni e infrastrutture per la sicurezza esterna in ambito informatico, organizzazione di workshop sui processi internazionali, supporto al Global Forum on Cyber Expertise).

27) Consultazioni politiche bilaterali e dialoghi multilaterali sulla politica in materia di sicurezza esterna in ambito informatico

Con determinati Paesi la Svizzera intrattiene consultazioni sulla politica in materia di sicurezza esterna in ambito informatico, in particolare sulle minacce informatiche e le tendenze. Partecipa inoltre attivamente alla promozione di dialoghi multilaterali (p. es. Sino-European Cyber Dialogue).

4.10 Effetti all'esterno e sensibilizzazione

Tabella sinottica del campo d'azione	
Descrizione	Il rapido sviluppo e l'aumento dei rischi informatici genera insicurezza nella popolazione e nell'economia. Sia le persone che le imprese difficilmente riescono a valutare i rischi informatici a cui sono esposti e le opportune misure di protezione da adottare. Oltre alla difficoltà di riuscire a valutare i rischi informatici, spesso non è neanche chiaro quale sostegno potersi aspettare dallo Stato. L'ampia gamma di misure previste dalla SNPC e la loro attuazione decentralizzata rendono difficile, per chi osserva la situazione dall'esterno, capire quali misure lo Stato adotti per garantire alla Svizzera una migliore protezione contro i rischi informatici. Le attività di attuazione della strategia prevedono quindi anche la comunicazione attiva delle misure adottate e dei progressi fatti. Oltre a comunicare la SNPC, la Confederazione deve anche contribuire a sensibilizzare la popolazione sui rischi informatici. Informare la popolazione su quali siano i rischi informatici e quali le possibili misure di protezione permette di prevenire e migliorare la resilienza e aiuta a ridurre il senso di incertezza.
Situazione iniziale	Finora gli strumenti utilizzati per divulgare i risultati ottenuti nell'ambito della SNPC sono stati i rapporti annuali, gli incontri annuali (riunioni SNPC e «Cyber-Landsgemeinde») e il sito Internet. I feedback forniti dalla popolazione e dal mondo dell'economia e della politica hanno però evidenziato che gli strumenti disponibili non sono sufficienti a soddisfare il bisogno di informazioni. Nuovi incidenti hanno altresì evidenziato che perdura la necessità di sensibilizzare la collettività sui rischi informatici e di attirare l'attenzione sulle possibilità basilari di protezione.
Obiettivi e necessità di intervento	In futuro il pubblico dovrà essere informato ancora più attivamente sullo stato di attuazione della SNPC, in modo che non solo gli addetti ai lavori siano a conoscenza delle misure che la Confederazione adotta per proteggere la Svizzera dai rischi informatici. Nell'ottica della prevenzione, la Confederazione dovrà inoltre attivarsi maggiormente per sensibilizzare sia la popolazione che il mondo dell'economia e della politica sui rischi informatici e per informarli sulle possibili misure di protezione.

Misure
28) Creazione e attuazione di un piano per la comunicazione di informazioni sulla SNPC Le linee guida, le competenze e i processi di comunicazione sono stabiliti in un apposito piano. Un aspetto da considerare a questo proposito è anche quello dell'equilibrio tra la confidenzialità e il bisogno di informazioni. Il piano deve essere attuato in maniera adeguata ai destinatari attraverso attività nel settore mediatico e delle relazioni pubbliche e deve essere portato avanti attivamente.
29) Sensibilizzazione del pubblico sui rischi informatici (*awareness*) La Confederazione contribuirà all'opera di sensibilizzazione del pubblico sui rischi informatici, intensificando la comunicazione al riguardo e sfruttando le capacità di cui dispongono le federazioni, le associazioni e le autorità che già operano attivamente in questo settore.

5 Attuazione della strategia

Le misure descritte nei dieci campi d'azione riportati sopra saranno attuate entro il 2022. A tal fine si devono definire chiaramente i responsabili per l'adozione delle singole misure, le basi legali su cui l'attuazione dovrà poggiare e i termini entro i quali devono essere raggiunti gli obiettivi. Questo presuppone, in primo luogo, che la Confederazione stabilisca chiaramente le competenze delle unità amministrative coinvolte e chi assume la responsabilità globale della SNPC. In secondo luogo, si devono chiarire le basi legali; in terzo luogo si deve definire come la Confederazione collabora con i Cantoni, l'economia e la società e che ruoli svolgono questi attori nell'adozione delle singole misure; in quarto luogo, deve essere possibile seguire lo stato di avanzamento dell'attuazione della SNPC. A tal fine si devono definire gli obiettivi prestazionali quantificabili per tutte le misure e in quanto tempo devono essere raggiunti. Infine, è necessario indicare come e da chi viene aggiornata la SNPC, se si verificassero nuovi sviluppi o fosse necessario apportare integrazioni o modifiche prima della fine del 2022.
Poiché questi punti riguardano la questione dell'attuazione e non interessano direttamente il suo orientamento strategico, vengono descritti in un piano di attuazione separato. Esso deve essere considerato una parte complementare della SNPC in cui vengono integrati gli obiettivi strategici con quelli operativi e vengono descritte le responsabilità e le competenze. Di seguito vengono spiegati gli elementi principali dei punti precedenti in modo da chiarire come si procede all'attuazione della SNPC.

5.1 Compiti e competenze nell'Amministrazione federale

Con l'approvazione della SNPC la Confederazione si impegna direttamente ad adottare le misure ivi contenute. Poiché la SNPC comprende un'ampia gamma di misure e considerato l'approccio decentrato della SNPC, diversi uffici federali partecipano direttamente alla sua attuazione. I compiti della Confederazione possono essere suddivisi sommariamente in tre ambiti.

- **Cyber sicurezza**: comprende tutte le misure volte a prevenire e ad affrontare incidenti informatici nonché a migliorare la resilienza ai cyber-rischi e che servono a intensificare la collaborazione internazionale a tale scopo. La Confederazione adotta le misure necessarie per rafforzare la propria protezione informatica e, tenuto conto del principio di sussidiarietà, contribuisce a migliorare la sicurezza informatica dell'economia e della società, ponderando opportunamente l'importanza cruciale delle infrastrutture critiche. Tra le misure rientra anche la promozione della collaborazione internazionale nell'ambito della sicurezza informatica.

- **Cyber difesa:** comprende tutte le misure relative alle attività informative e militari che servono a proteggere i sistemi critici, a respingere gli attacchi informatici, a garantire la prontezza operativa dell'Esercito in ogni circostanza e a creare le capacità e le competenze per fornire un supporto sussidiario alle autorità civili. Il settore della cyber difesa comprende, in particolare, le misure attive da adottare per individuare le minacce informatiche, identificare gli autori, far fronte a perturbazioni e far cessare gli attacchi.

- **Perseguimento penale della criminalità informatica:** comprende le misure della polizia e del Ministero pubblico per la lotta contro la criminalità informatica.

5.2 Collaborazione con terzi

Un obiettivo strategico della SNPC è garantire una collaborazione comune per proteggere la Svizzera dai cyber-rischi. Di conseguenza, è particolarmente importante che i Cantoni, l'economia e la società siano direttamente coinvolti nei lavori di attuazione. Mentre la Confederazione stabilisce in modo vincolante le competenze e gli obblighi degli uffici federali nel piano di attuazione, deve essere definito anche quali compiti devono essere assunti dai Cantoni e dalle organizzazioni dell'economia e della società. I Cantoni e le organizzazioni dell'economia e della società vengono quindi coinvolti nella predisposizione del piano di attuazione.

5.2.1 Partecipazione dei Cantoni all'attuazione

Per garantire la partecipazione diretta dei Cantoni all'attuazione delle misure relative alla SNPC 2018−2022, il CDDGP insieme alla RSS sta elaborando un piano di attuazione cantonale. Su questa base, nel piano di attuazione della NSPC vengono definiti le misure in cui i Cantoni sono direttamente coinvolti e gli obiettivi da conseguire.

5.2.2 Partecipazione dell'economia e della società

Nell'ottica di un'autoregolamentazione, nel piano di attuazione della SNPC vengono definite le organizzazioni dell'economia e della società che intendono impegnarsi ad adottare determinate misure. L'elenco delle organizzazioni dell'economia e della società non deve essere considerato esaustivo; infatti altre organizzazioni possono sempre partecipare.

5.2.3 Coordinamento dell'attuazione

Sotto la direzione generale del progetto, tutti i partecipanti coordinano le loro attività, concertano periodicamente i lavori di attuazione e verificano se sono necessarie misure aggiuntive per conseguire gli obiettivi della SNPC. A tal fine viene istituito un comitato di coordinamento, costituito da rappresentanti della Confederazione, dei Cantoni e dell'economia.

5.3 Obiettivi prestazionali per l'adozione delle misure

Affinché si possa valutare lo stato di avanzamento nell'adozione delle misure, per tutte devono essere definiti obiettivi prestazionali quantificabili. Partendo dallo stato attuale nei settori interessati dalle misure, vengono indicati gli obiettivi da conseguire e i termini entro i quali raggiungerli. Gli obiettivi prestazionali indicano, per esempio, il lasso di tempo entro il quale devono essere elaborati prodotti concreti, quali progetti o relative fasi devono essere completati e quali processi devono essere consolidati ed eventualmente sviluppati.

5.4 Aggiornamento della SNPC

La presente Strategia verrà aggiornata alla fine del 2022. La SNPC viene verificata regolarmente durante l'attuazione e, se necessario, modificata. Un aggiornamento anticipato è previsto solo se si manifestano delle minacce informatiche inaspettate o subentrano altri fattori, precedentemente descritti nel capitolo «Situazione iniziale», che mettono in discussione le ipotesi iniziali. In caso di aggiornamento anticipato, la nuova versione della SNPC viene presentata al Consiglio federale, agli uffici federali, ai Cantoni e ai rappresentanti dell'economia.

6 Elenco delle abbreviazioni

CCPCS		Conferenza dei comandanti delle polizie cantonali della Svizzera
CDDGP		Conferenza dei direttori cantonali di giustizia e polizia
CERT		Computer Emergency Response Team
DDPS		Dipartimento federale della difesa, della protezione della popolazione e dello sport
DFF		Dipartimento federale delle finanze
Direttiva NIS		Direttiva UE sulla sicurezza delle reti e dei sistemi informativi (Network and Information Security)
Fedpol		Ufficio federale di polizia
GSic		Giunta del Consiglio federale in materia di sicurezza
HUMINT		Human Intelligence
ITU		International Telecommunication Union / Unione internazionale delle telecomunicazioni
LAIn		Legge federale sulle attività informative
LM		Legge militare
LUC		Legge federale sugli Uffici centrali di polizia giudiziaria della Confederazione e i centri comuni di cooperazione di polizia e doganale con altri Stati
MELANI		Centrale d’annuncio e d’analisi per la sicurezza dell’informazione
OCSE		Organizzazione per la cooperazione e lo sviluppo economico
ODIC		Organo direzione informatica della Confederazione
ONU		Organizzazione delle Nazioni Unite
OSCE		Organizzazione per la sicurezza e la cooperazione in Europa
OSINT		Open Source Intelligence
PACD		Piano d’azione per la cyber difesa
PIC		Protezione delle infrastrutture critiche
PNR		Programmi nazionali di ricerca
PPP		Partenariato pubblico-privato
RC3		Centri regionali di competenza informatica
RSS		Rete integrata Svizzera per la sicurezza
RTN		Reti tematiche nazionali
SDVN+		Rete di dati sicura
SNPC		Strategia nazionale per la protezione della Svizzera contro i cyber-rischi
SOC		Security Operations Centers / Centri operativi di sicurezza
TIC		Tecnologie dell’informazione e della comunicazione
UE		Unione europea
UFAE		Ufficio federale per l’approvvigionamento economico del Paese
UFPP		Ufficio federale della protezione della popolazione
USEs		Ulteriore sviluppo dell’esercito
WEF		World Economic Forum
WSIS		World Summit on the Information Society

7 Glossario

Cyber attacco	Atto illecito intenzionale compiuto da una persona o da un gruppo di persone nel cyberspazio per compromettere l'integrità, la confidenzialità o l'accessibilità di informazioni e dati. A seconda del tipo di attacco, può anche avere ripercussioni fisiche.
Cyber criminalità (Criminalità informatica)	Cyber criminalità in senso stretto: riguarda i reati commessi con l'ausilio delle tecnologie dell'informazione e della comunicazione (TIC) o che sfruttano le vulnerabilità di queste tecnologie. Queste attività criminali sono nuove e possono essere compiute soltanto mediante le TIC. Cyber criminalità in senso lato: utilizza Internet come mezzo di comunicazione, usando impropriamente le funzionalità disponibili come per esempio il traffico delle e-mail, lo scambio o la predisposizione di file per scopi illeciti. Queste attività criminali non sono nuove, ma i mezzi utilizzati per compierle o per memorizzare i dati (Whatsapp, Snapchat, Instagram, Telegram e supporti dati elettronici invece della carta, servizi cloud ecc.) sono recenti.
Cyber difesa	Comprende tutte le misure dei servizi d'informazione e militari che servono a interferire, bloccare o rallentare gli attacchi informatici, a identificare gli autori, a garantire la prontezza operativa dell'Esercito in ogni circostanza e a creare le capacità e le competenze per fornire un supporto sussidiario alle autorità civili.
Cyber sabotaggio (Sabotaggio informatico)	Attività mirata a perturbare il buon funzionamento delle infrastrutture informatiche e delle comunicazioni o a distruggerle. A seconda del tipo di sabotaggio, tale attività può avere anche ripercussioni fisiche.
Cyber sicurezza	Stato auspicabile nel cyberspazio in cui le comunicazioni e lo scambio di dati tra le infrastrutture TIC funzionano come previsto originariamente. Questo stato si consegue adottando misure di sicurezza delle informazioni e di cyber difesa.
Cyber spionaggio	Attività compiuta nel cyberspazio a scopi politici, militari o economici per accedere illecitamente a informazioni protette.
Cyber-rischi	Sono il prodotto della probabilità che si verifichi un incidente informatico e dell'impatto di tale incidente qualora si verificasse. .
Cyberspazio	Comprende tutte le infrastrutture informatiche e per le comunicazioni (hardware e software) che consentono di scambiare, rilevare, memorizzare, elaborare dati oppure di convertirli in azioni (fisiche) e tutte le possibili interazioni che ne derivano tra persone, organizzazioni e Stati.
Incidente informatico	Evento intenzionale o fortuito che causa un processo nel cyberspazio che può compromettere l'integrità, l'accessibilità o la confidenzialità di dati e informazioni e può causare malfunzionamenti.
Infrastrutture critiche	Processi, sistemi e dispositivi essenziali per il funzionamento dell'economia e il benessere della popolazione.

Minaccia informatica	Operazione che può causare un incidente informatico.
Resilienza	Capacità di un sistema, di un'organizzazione o di una società di resistere a interferenze e di mantenere o ripristinare rapidamente la funzionalità.
Sicurezza delle informazioni/ Sicurezza delle TIC	La sicurezza delle informazioni (o sicurezza delle TIC) è data dalla garanzia dell'autenticità, della confidenzialità, dell'integrità e della accessibilità di un sistema TIC e dei dati che vengono elaborati e salvati in questo sistema.