Ciberstrategia nazionale (CSN)

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Consiglio federale

Colofone

Editore
Centro nazionale per la cibersicurezza (NCSC)
Schwarztorstrasse 59
CH-3003 Berna

info@ncsc.admin.ch
www.ncsc.admin.ch

Panoramica

1 Introduzione

La cibersicurezza è diventata un aspetto cruciale a tutti i livelli. Si tratta di un elemento chiave della politica di sicurezza, un presupposto indispensabile per la digitalizzazione, un fattore centrale per la protezione dei dati, un'opportunità per la Svizzera come piazza economica e di ricerca e un aspetto sempre più importante della politica estera. Tuttavia, non riguarda solo tali questioni di politica statale, ma è diventata da tempo un aspetto che concerne l'utilizzo quotidiano delle tecnologie digitali da parte di tutti i cittadini. Ne consegue che una ciberstrategia nazionale deve prendere in considerazione svariati argomenti e misure. Allo stesso tempo, occorre che tale strategia organizzi questo ampio ventaglio di argomenti, che li ponderi e li metta in relazione tra loro. A tale scopo, questo capitolo introduttivo descrive in primo luogo le diverse minacce da contrastare e, in secondo luogo, le basi su cui si fonda la strategia. Il tema della cibersicurezza non è più una novità e in Svizzera sono già state elaborate delle basi. È importante partire dal lavoro già svolto come pure mettere in discussione tale operato e integrarlo laddove necessario. In terzo luogo viene affrontata la ripartizione delle varie responsabilità, una questione che si è più volte rivelata una delle sfide principali nell'ambito trasversale della cibersicurezza.

1.1 Ciberminacce

In questa strategia, si definisce ciberminaccia una circostanza che ha il potenziale di causare un incidente informatico. Un ciberincidente è a sua volta definito come un evento che, nell'ambito dell'utilizzo delle tecnologie dell'informazione e della comunicazione (TIC), compromette la confidenzialità, l'accessibilità o l'integrità delle informazioni o la tracciabilità del loro trattamento. Sulla base di queste definizioni è possibile individuare un'ampia gamma di potenziali ciberminacce, le quali vengono descritte qui di seguito. Per identificare le contromisure adeguate, si rende inoltre necessaria una panoramica sistematica dei fattori che influenzano direttamente le minacce informatiche.

1.1.1 Minaccia di ciberattacchi

Per ciberattacchi si intendono incidenti informatici causati intenzionalmente. La protezione da tali minacce rappresenta l'elemento centrale delle misure di cibersicurezza. Si tratta di una questione importante in ragione delle persistenti minacce di ciberattacchi e della dipendenza sempre più forte dell'economia e della società da ambienti TIC funzionanti.
In considerazione della molteplicità dei possibili ciberattacchi, ai fini della valutazione della situazione e dei possibili meccanismi di gestione, è importante distinguere i 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 ciberattacchi, anche se occorre precisare che gli attacchi perpetrati sono spesso il risultato di una loro combinazione o sovrapposizione.

Cibercriminalità: in contrapposizione alle minacce descritte di seguito, la cibercriminalità comprende soprattutto reati contro il patrimonio. La criminalità informatica costituisce l'insieme dei reati e delle omissioni punibili commessi nel ciberspazio. Si distingue tra «cibercrime» e «criminalità digitale». Il primo concetto designa reati perpetrati ai danni della rete, dei sistemi o dei dati informatici che rendono necessario l'utilizzo di strumenti tecnici per il lavoro d'indagine svolto dalle autorità di perseguimento penale. Il secondo si riferisce a reati finora commessi prevalentemente al di fuori dell'infrastruttura informatica. A causa della crescente digitalizzazione, i classici tipi di reati vengono commessi sempre più spesso con l'ausilio delle tecnologie informatiche.

La criminalità informatica 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 solitamente circoscritte alle vittime che li subiscono. Tuttavia, i cibercriminali sono pronti a correre rischi collaterali elevati o sfruttano tali 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 cibercriminalità si identificano veri e propri settori di attività in cui gruppi organizzati agiscono secondo metodi di ripartizione del lavoro. A causa della forte concorrenza, i criminali informatici sono fortemente spronati a innovarsi, motivo per cui sviluppano o acquisiscono costantemente nuovi metodi e si professionalizzano sempre di più. Di conseguenza, si deve continuare a prevedere un crescente aumento della frequenza e della specializzazione delle attività criminali all'interno del ciberspazio.

Ciberspionaggio: si tratta di un'attività in cui i ciberattacchi vengono utilizzati per scopi politici, militari o economici per accedere illecitamente a informazioni o per osservare i movimenti della vittima. Spesso gli autori degli attacchi cercano di mantenere il più a lungo possibile l'anonimato dopo essere penetrati con successo all'interno delle reti. Tipici di queste attività sono gli attacchi sofisticati e persistenti, i cosiddetti «Advanced Persistent Threat» (APT). Il ciberspionaggio è spesso svolto da attori statali, ma anche semi-statali o 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 e conferenze. Tutto questo rende il Paese un bersaglio interessante per il ciberspionaggio. Le conseguenze possono variare notevolmente a seconda della tipologia e dell'entità dei dati a cui gli autori degli attacchi riescono ad accedere. Tuttavia, per le PMI che dipendono fortemente dalla loro capacità d'innovazione, tali conseguenze possono assumere rapidamente proporzioni che minacciano la loro stessa esistenza. 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. Inoltre, in seguito a tali operazioni, si registrano spesso danni collaterali, poiché i cibercriminali utilizzano in seconda battuta i loro vettori di attacco.
Con l'aumento delle tensioni geopolitiche, anche il ciberspionaggio sta acquisendo sempre maggiore importanza. La minaccia è ulteriormente accresciuta dall'influenza esercitata dai governi sui produttori di prodotti TIC, aumentando la probabilità che le lacune di sicurezza dei prodotti non vengano volutamente colmate. Poiché le catene di fornitura dei prodotti TIC sono molto complesse e la Svizzera dipende in larga misura da produttori esteri, affrontare tale minaccia in modo adeguato costituisce un compito impegnativo.

Cibersabotaggio: il sabotaggio informatico è un'attività volta a manipolare, perturbare o a interrompere il funzionamento affidabile ed efficiente delle TIC tramite ciberattacchi. A seconda del tipo di sabotaggio, una simile attività può avere anche ripercussioni fisiche. Le motivazioni alla base di tali attacchi possono essere molto varie. Possono essere compiuti da singoli malfattori, per esempio per convinzioni ideologiche o frustrazioni personali, oppure essere perpetrati da attori statali per raggiungere obiettivi politici o militari. In ogni caso, l'obiettivo è costituire dimostrazioni di forza e intimidazioni volte a destabilizzare un'organizzazione o addirittura la società.

Mentre a livello internazionale si sono verificati atti di sabotaggio di particolare rilevanza che hanno colpito anche l'approvvigionamento energetico di Stati, in Svizzera finora non ne sono stati registrati. Tuttavia, la probabilità che vengano effettuati tali atti è aumentata anche per la Svizzera con l'acuirsi delle tensioni geopolitiche. In questo caso i potenziali danni sarebbero molto ingenti.

Cibersovversione: si parla di sovversione informatica quando attori statali, parastatali o animati da motivi politici utilizzano ciberattacchi in modo mirato per minare il sistema politico di un altro Stato. Tali attacchi prendono di mira, per esempio, le procedure dei processi democratici, le istituzioni politiche o le organizzazioni di grande interesse pubblico. I criminali informatici cercano di minare la fiducia nello Stato e combinano spesso questi attacchi con

campagne di disinformazione.

Ciberoperazioni nei conflitti armati: L'impiego di mezzi illegali, oltre a quelli regolari, nei conflitti armati è oggi prassi comune. Le ciberoperazioni sono uno strumento particolarmente adatto in tal senso in quanto, oltre a essere difficilmente classificabili in modo chiaro e a presentare costi relativamente contenuti, possono essere utilizzati su grandi distanze senza essere fisicamente presenti e consentono di produrre degli effetti anche senza dover ricorrere direttamente a operazioni militari.
I cospicui investimenti effettuati da molti Stati per la protezione e la difesa attiva da ciberminacce sottolineano l'importanza assunta dagli strumenti informatici nei conflitti armati. Di conseguenza, si prevede che l'importanza delle ciberoperazioni a fini politici aumenterà ulteriormente. La Svizzera deve pertanto includere la ciberdifesa e la ciberdiplomazia nella prevenzione di tali attività e nei preparativi a un eventuale scenario di questo tipo.

1.1.2 Errori umani e guasti tecnici

Oltre che da ciberattacchi mirati e deliberati, gli incidenti informatici possono essere provocati anche da azioni non intenzionali o eventi naturali o tecnici. Essi sono 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, approvvigionamento energetico 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. Tuttavia, è importante notare che dietro a molti ciberincidenti 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 ciberincidenti imputabili a errori umani o a guasti tecnici continueranno a verificarsi frequentemente. La crescente complessità causata dall'interconnessione di ambiti svariati complica inoltre la possibilità di stimare e limitare le conseguenze di questi episodi non intenzionali. La formazione del personale nonché in generale una buona preparazione e una pianificazione accurata nei confronti di tali incidenti rimangono pertanto elementi centrali nella protezione contro le ciberminacce.

1.1.3 Fattori che influenzano la situazione di minaccia

Gli sviluppi tecnologici, politici e sociali influenzano notevolmente la situazione di minaccia, che in linea di principio può cambiare molto rapidamente in qualsiasi momento. Tuttavia, è possibile identificare i fattori che molto probabilmente influenzeranno lo sviluppo futuro di ciberminacce, motivo per cui nel contesto strategico è importante considerarli. Allo stesso tempo, si deve sempre tenere conto che l'elenco dei possibili fattori non deve assolutamente essere inteso come esaustivo e che fa parte della valutazione continua della situazione riconoscere tempestivamente ulteriori possibili influenze e rivalutare costantemente i fattori già identificati.
L'evoluzione dello scenario delle ciberminacce è essenzialmente influenzato da innovazioni geopolitiche e tecnologiche. In termini di geopolitica, si può semplicisticamente affermare che un acuirsi delle tensioni geopolitiche comporta un peggioramento della situazione delle ciberminacce. Poiché Internet collega globalmente Stati, aziende e persone, le tensioni internazionali hanno ripercussioni dirette su queste interazioni. È dunque possibile prevedere un aumento dei ciberattacchi reciproci in tutte le modalità precedentemente descritte. Al contempo, con l'aumento delle tensioni tra Paesi che figurano tra i più importanti produttori di prodotti hardware e software, ci si può aspettare anche blocchi reciproci. Ciò complica

l'approvvigionamento di tali strumenti e rende ancora più importante per i beneficiari di prestazioni soppesare i rischi con estrema attenzione al momento dell'acquisto.
Per quanto riguarda gli sviluppi tecnologici, va notato che le innovazioni tecnologiche possono sia migliorare che peggiorare la situazione e che a volte ciò accade contemporaneamente. Se da un lato le nuove tecnologie spesso contribuiscono a migliorare la sicurezza, dall'altro comportano nuove dipendenze, aumentano la complessità o addirittura portano direttamente a nuove minacce, essendo utilizzate dai criminali informatici. Per la protezione dalle ciberminacce è dunque fondamentale confrontarsi tempestivamente con i nuovi sviluppi tecnologici e anticipare le possibili minacce.
Nei prossimi anni occorrerà prestare particolare attenzione agli sviluppi delle tre seguenti tecnologie di base della digitalizzazione:

- **cloud computing**: tale sistema consente lo sviluppo di nuove applicazioni e innovazioni tecnologiche e può aumentare la cibersicurezza, per esempio garantendo un'elevata disponibilità di informazioni. Allo stesso tempo, il cloud computing comporta rischi. Le informazioni di grande importanza per la Svizzera possono essere trattate al di fuori del Paese, il che significa che la protezione legale relativa all'accesso e all'utilizzo di questi dati non è disciplinata unicamente dalla legislazione svizzera. Inoltre, il cloud computing può potenzialmente portare a un'elevata dipendenza da un numero limitato di fornitori di servizi. Le conseguenze derivanti da questo tipo di sistema possono compromettere la cibersicurezza in assenza di adeguate contromisure;
- **Internet of Things (IoT)**: l'Internet delle cose, ovvero l'interconnessione di oggetti fisici (things) attraverso Internet continua ad avanzare velocemente e riguarda il controllo, il monitoraggio e l'interconnessione sia dei sistemi dell'industria (Operational Technology) che dei beni di consumo. In riferimento allo scenario delle ciberminacce, l'enorme diffusione dell'IoT riveste in primo luogo un ruolo di grande importanza. Il collegamento di migliaia di dispositivi porta ad ambienti di sistema molto complessi e a una massiccia espansione della potenziale superficie di attacco. In secondo luogo, questa interconnessione aumenta anche la minaccia di cibersabotaggio, in quanto diventa sempre più facile ottenere conseguenze fisiche dirette attraverso i ciberattacchi. In terzo luogo, va notato che spesso la sicurezza non viene presa sufficientemente in considerazione nei dispositivi IoT, né durante la produzione né nel corso dell'ulteriore ciclo di vita degli apparecchi, al fine di mantenere bassi i costi. Per contrastare tale situazione sia a livello nazionale che europeo, vengono attualmente introdotte disposizioni relative alla sicurezza dei dispositivi IoT (p. es con l'ordinanza dell'UFCOM sugli impianti di telecomunicazione);
- **intelligenza artificiale**: la disponibilità di un'elevata potenza di calcolo e di un cospicuo numero di dati consente oggi un uso molto più ampio dell'intelligenza artificiale. Grazie all'apprendimento automatico parzialmente o completamente autonomo, le applicazioni IA sono in grado di eseguire analisi molto complesse in breve tempo. Tali possibilità possono essere utilizzate per proteggere meglio i sistemi, ma al contrario anche per sferrare attacchi con conseguenze di più ampia portata e un dispendio inferiore di risorse. Dal momento che molte organizzazioni si affidano sempre di più alle analisi delle applicazioni AI per prendere decisioni, anche gli attacchi a tali strumenti rappresentano uno scenario di minaccia rilevante. Inoltre, le applicazioni AI possono rappresentare un rischio per la sicurezza anche in assenza di fattori esterni, se un'applicazione difettosa causa una perturbazione o una fuga di dati.

Oltre agli sviluppi delle tecnologie di base della digitalizzazione, è importante considerare gli sviluppi tecnologici non ancora ampiamente utilizzati, ma il cui uso può avere un impatto diretto sulla cibersicurezza. Un esempio di questo tipo di tecnologia sono i computer quantistici, che sono in grado di risolvere alcuni problemi matematici in modo molto più efficiente rispetto a quelli odierni. I diffusi metodi di crittografia asimmetrica potrebbero così essere violati da questa tecnologia, motivo per cui è necessario sviluppare e utilizzare algoritmi post-quantistici. Occorre dunque prendere in considerazione tali progressi tecnologici nell'attuazione delle misure della strategia.

1.2 Stato della protezione della Svizzera contro le ciberminacce

La presente strategia si basa sui lavori svolti nel quadro delle prime due strategie per la protezione della Svizzera contro i ciber-rischi, attuate dal 2012 al 2017 e dal 2018 al 2022. Inoltre, si inserisce nel contesto strategico dato dall'orientamento della Svizzera in materia di digitalizzazione e politica di sicurezza. Lo stato di protezione contro le ciberminacce in Svizzera si riflette a livello istituzionale nell'organizzazione della Confederazione e negli organi creati per promuovere la collaborazione tra Confederazione, Cantoni, mondo economico e scuole universitarie.

1.2.1 Le prime due strategie nazionali

Le prime due strategie nazionali per la protezione contro i ciber-rischi si sono concentrate sull'acquisizione e lo sviluppo di capacità, strutture e processi. La loro attuazione ha posto le basi necessarie per una politica coerente di cibersicurezza in Svizzera. Nell'ambito di queste strategie, sono state prese anche decisioni fondamentali sulle strutture organizzative della politica di sicurezza informatica. In seno alla Confederazione è stato creato un centro di competenza, il Centro nazionale per la cibersicurezza (NCSC), e sono stati definiti gli organi necessari per la collaborazione all'interno dell'Amministrazione federale e al di fuori di essa con i Cantoni, il mondo economico e le scuole universitarie. I lavori condotti finora hanno quindi gettato le basi necessarie e la presente strategia può ora definire gli obiettivi prioritari del lavoro esistente o futuro.

1.2.2 Contesto strategico della strategia

Le linee guida di riferimento per la protezione della Svizzera dalle ciberminacce si evincono da varie strategie elaborate dalla Confederazione che creano il contesto per la presente strategia.

- **Strategia Svizzera digitale**: la strategia mostra come la Svizzera intenda sfruttare, per il benessere di tutti, le opportunità che la trasformazione digitale crea per la società e l'economia. «Sicurezza e fiducia» è uno dei cinque settori d'impatto.
- **Strategia nazionale per la protezione delle infrastrutture critiche (PIC):** 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.
- **Rapporto del Consiglio federale sulla politica di sicurezza della Svizzera:** nel rapporto sulla politica di sicurezza il Consiglio federale definisce l'orientamento strategico di fondo della politica di sicurezza della Svizzera. Il rapporto e il rapporto complementare del 2022 illustrano l'importanza delle ciberminacce per la politica di sicurezza e definiscono importanti concetti relativi a tale tematica.
- **Concetto generale ciber dell'Esercito svizzero:** il CG Ciber illustra le sfide nell'ambito del ciberspazio, dello spazio elettromagnetico nonché delle TIC e descrive le capacità che l'Esercito svizzero dovrà sviluppare entro la metà degli anni 2030 per essere in grado di affrontare anche le minacce future.
- **Strategia di politica estera digitale:** la strategia definisce i campi d'azione della politica estera digitale della Svizzera. Nell'ambito della cibersicurezza, la Svizzera si impegna a favore di norme di diritto internazionale relative al ciberspazio, del coinvolgimento di attori privati nella politica di cibersicurezza e di misure per rafforzare la fiducia. Offre inoltre buoni uffici anche riguardo a questioni di cibersicurezza.

1.3 Organizzazione per la protezione della Svizzera dalle ciberminacce

La cibersicurezza è un tema trasversale che non può essere attribuito a un'unica autorità. Questo vale tanto più per la Svizzera, dove l'assegnazione dei compiti è comunque caratterizzata dal federalismo. Sebbene le interazioni digitali siano difficilmente individuabili a livello territoriale, il principio costituzionale della competenza federale riguarda anche il ciberspazio.
Su questa base, la Confederazione e i Cantoni hanno sviluppato le rispettive ciberorganizzazioni. Sebbene le strutture di base della Confederazione e dei Cantoni siano state definite, almeno a grandi linee, è importante che vengano continuamente valutate e, se necessario, ulteriormente sviluppate.
Oltre alla ripartizione dei compiti tra i diversi livelli statali, è fondamentale l'aspetto della collaborazione tra attori pubblici e privati nella cibersicurezza. Tale cooperazione è organizzata in diversi modi e si realizza attraverso organizzazioni composte da attori pubblici e privati, tramite il coinvolgimento diretto di associazioni e aziende nell'attuazione delle misure della CSN o anche nella collaborazione quotidiana e nello scambio di conoscenze tra team addetti alla sicurezza privati e pubblici.
Quanto segue non intende elencare tutte le organizzazioni e le forme di collaborazione rilevanti per la cibersicurezza, ma presentare gli elementi principali dell'organizzazione della Confederazione e dei Cantoni e illustrare i meccanismi per gestire l'attuazione della strategia.

1.3.1 Organizzazione e competenze in seno alla Confederazione

All'interno della Confederazione si distingue tra i seguenti tre settori di compiti:
- **cibersicurezza:** comprende tutte le misure volte a prevenire e gestire i ciberincidenti nonché a migliorare la resilienza ai ciber-rischi e a intensificare la collaborazione internazionale a tale scopo;
- **ciberdifesa:** comprende tutte le misure militari e del Servizio delle attività informative che servono a proteggere i sistemi critici per la difesa nazionale, a respingere i ciberattacchi, a garantire l'efficienza operativa dell'esercito in ogni situazione e a creare le capacità e le competenze per fornire un supporto sussidiario alle autorità civili. Tra queste rientrano anche le misure attive volte a individuare le minacce, identificare gli aggressori nonché ostacolare e bloccare gli attacchi;
- **perseguimento penale della cibercriminalità:** comprende tutte le misure adottate dalla polizia e dai ministeri pubblici di Confederazione e Cantoni nella lotta contro la cibercriminalità.

Il Centro nazionale per la cibersicurezza (NCSC) è responsabile dei compiti principali nel campo della cibersicurezza nonché del coordinamento con tutti gli altri uffici coinvolti. In base alla decisione presa il 2 dicembre 2022 dal Consiglio federale, l'NCSC diventerà un Ufficio federale. Tale organo espleterà compiti concepiti esclusivamente per la cibersicurezza civile e quindi chiaramente delimitati da quelli del Servizio delle attività informative e dell'esercito nell'ambito della ciberdifesa. Il nuovo Ufficio federale non assumerà inoltre i compiti di vigilanza e regolamentazione svolti dalle autorità specializzate nei loro settori. Queste ultime continueranno a essere responsabili delle attività di autorizzazione e di vigilanza operativa continua, esercitate sull'industria e sulle imprese concessionarie riguardanti prescrizioni relative alla cibersicurezza specifiche del loro settore. L'NCSC collabora direttamente con gli Uffici specializzati mettendo a loro disposizione tutte le conoscenze di carattere specialistico relative alla cibersicurezza.
Il settore del perseguimento penale della cibercriminalità è principalmente di competenza dei Cantoni. Da parte della Confederazione sono competenti l'Ufficio federale di polizia (fedpol) e il Ministero pubblico della Confederazione (MPC).

Le basi legali delle organizzazioni precisano le competenze dei relativi uffici. Allo stesso tempo, le unità amministrative assicurano tra loro un coordinamento ottimale e l'utilizzo di sinergie, nel quadro stabilito dalla legge, attraverso un continuo scambio di informazioni e conoscenze.

1.3.2 Organizzazione e competenze nei Cantoni

I Cantoni definiscono la propria organizzazione di cibersicurezza in modo indipendente e adeguato alle proprie esigenze. A tale scopo, possono basarsi sulle «Raccomandazioni per l'attuazione della ciberorganizzazione cantonale» messe a punto dalla Rete integrata Svizzera per la sicurezza (RSS) e adottate dalla Conferenza delle direttrici e dei direttori dei dipartimenti cantonali di giustizia e polizia (CDDGP) nel 2020. La struttura organizzativa raccomandata prevede la nomina di una persona per il coordinamento dei compiti relativi alla cibersicurezza (cibercoordinatore/trice) e di una Delegazione del governo cantonale a livello del Consiglio di Stato. Queste strutture permettono di tenere conto del carattere trasversale della cibersicurezza.
Il coordinamento intercantonale su questioni globali in materia di cibersicurezza viene svolto dalla CDDGP; tuttavia, ciò non impedisce ad altre conferenze governative di occuparsi degli aspetti ciber rientranti nei loro ambiti di competenza. La collaborazione con la Confederazione viene coordinata e promossa dalla RSS.

1.3.3 Gestione congiunta della CSN da parte di Confederazione, Cantoni, mondo economico e scuole universitarie

Il Consiglio federale nomina un comitato direttivo che gestisce l'attuazione della CSN coordinando il lavoro svolto dalle parti coinvolte e valutandone lo stato di avanzamento. Il comitato direttivo è composto da esperti dei vari settori della cibersicurezza e ha il compito di integrare le richieste dei Cantoni, del mondo economico, della società, delle scuole universitarie e della Confederazione. Ai fini del coordinamento del lavoro, il comitato elabora un piano di attuazione in accordo con gli attori centrali. Lo scopo è uniformare le priorità delle parti coinvolte in modo da garantire uno svolgimento mirato e coordinato dei lavori relativi all'attuazione.
Per valutare l'avanzamento del processo di attuazione, il comitato direttivo definisce alcuni indicatori di prestazione per le singole misure. Grazie a questi indicatori è possibile determinare se l'attuazione di tali misure permette di raggiungere gli obiettivi della strategia nella misura richiesta.
Il comitato direttivo informa regolarmente il Consiglio federale e i Cantoni sullo stato di attuazione della strategia e sulle valutazioni espresse in merito al grado di attuazione. In quanto segretariato del comitato direttivo, l'NCSC funge da tramite per comunicare le informazioni di tale organo al Consiglio federale e ai Cantoni per mezzo del DDPS. Mediante lo stesso iter di comunicazione, il comitato direttivo può proporre ai Cantoni e al Consiglio federale di integrare, modificare o annullare determinate misure oppure di completare la strategia con ulteriori obiettivi o provvedimenti.

2 Orientamento della CSN

2.1 Visione e obiettivi strategici

2.1.1 Visione

«La Svizzera sfrutta le opportunità offerte dalla digitalizzazione e riduce le ciberminacce e le relative conseguenze attraverso misure di protezione adeguate. La Svizzera figura tra i Paesi più importanti al mondo sul piano delle conoscenze, della formazione e delle innovazioni in materia di cibersicurezza. È uno dei principali produttori di prodotti e servizi digitali sicuri. La capacità di agire e l'integrità della sua popolazione, dell'economia, delle sue autorità e delle organizzazioni internazionali con sede in Svizzera nei confronti delle minacce informatiche sono garantite».

2.1.2 Obiettivi strategici

- **Autodeterminazione digitale:** la Svizzera espande la sua posizione come uno dei luoghi più importanti al mondo per la conoscenza, la formazione e l'innovazione anche nel campo della cibersicurezza. Sfrutta queste capacità per valutare in modo indipendente i ciber-rischi lungo le catene di fornitura, anticipare gli sviluppi tecnologici e rispondere ad essi in modo agile. La popolazione è informata sui rischi informatici e quindi acquista fiducia nell'utilizzo dei servizi digitali.
- **Servizi e infrastrutture digitali sicuri:** la Svizzera attua misure in modo capillare volte a rafforzare la ciber-resilienza. La Confederazione e i Cantoni creano le condizioni quadro necessarie per garantire un elevato livello di protezione, l'utilizzo di infrastrutture, prodotti e servizi digitali sicuri e la gestione consapevole della propensione al rischio.
- **Riconoscimento, prevenzione, gestione e difesa efficaci in materia di ciberincidenti:** in ogni circostanza, la Svizzera dispone delle capacità e delle strutture organizzative necessarie per individuare rapidamente le ciberminacce e gli incidenti informatici e ridurne al minimo i danni. Gli incidenti vengono gestiti anche quando si protraggono nel tempo e interessano contemporaneamente diversi settori.
- **Lotta e perseguimento penale efficaci in materia di cibercriminalità:** la Svizzera amplia le proprie competenze finalizzate a identificare gli autori di ciberattacchi, perseguirli in collaborazione secondo la legislazione penale e condannarli nei limiti di quanto previsto dalla legge.
- **Ruolo centrale nella cooperazione internazionale:** a livello operativo e strategico, la Svizzera si impegna a favore di un ciberspazio aperto, libero e sicuro nel quale il diritto internazionale venga pienamente riconosciuto, rispettato e attuato. La Ginevra internazionale è una delle sedi principali per i dibattiti sulla cibersicurezza. In caso di divergenze nell'ambito di ciberoperazioni, la Svizzera può svolgere il ruolo di mediatrice.

2.2 Principi

La visione e gli obiettivi strategici stabiliscono *i risultati* che la CSN si prefigge di raggiungere, mentre i principi definiscono *le modalità* con cui deve essere eseguito tale intervento.

- La CSN parte da un **approccio globale basato sul rischio**, che considera tutte le vulnerabilità e tutti i rischi rilevanti e che ha l'obiettivo di migliorare la resilienza della Svizzera sul fronte delle ciberminacce. Implicita in tale approccio «basato sul rischio» è l'idea che, pur non potendo garantire una protezione completa contro le ciberminacce, sia possibile affrontarle in modo che il rischio residuo sia sostenibile.

- La protezione della Svizzera contro le ciberminacce è 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. La CSN viene quindi attuata sulla base dei principi del federalismo, in modo decentralizzato e in responsabilità congiunta.
- La CSN si fonda sull'idea di un **ruolo sussidiario e collaborativo dello Stato**, il che significa che l'intervento dello Stato è ammesso solo qualora il benessere della nostra società sia minacciato 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, determinando misure ad hoc in stretto scambio con gli attori interessati e impegnandosi a favore di una serrata collaborazione con loro.
- L'attuazione della CSN 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, del mondo scientifico e della politica nonché un diretto coinvolgimento dei partner fondamentali dell'amministrazione, della società e del settore privato.

2.3 Gruppi di destinatari

Con la CSN la Confederazione e i Cantoni stabiliscono quali obiettivi si propongono di attuare in collaborazione con l'economia, il mondo scientifico e la società. L'effetto che si intende raggiungere con la CSN interessa tutto il Paese. La strategia si rivolge in maniera esplicita ai gruppi di destinatari indicati di seguito:

- **popolazione:** la protezione della popolazione rappresenta lo scopo di tutte le misure della CSN. La popolazione è direttamente interessata dai ciberincidenti, soprattutto in caso di attacchi ad opera di cibercriminali o di compromissione dei dati personali. La CSN contribuisce inoltre a sensibilizzare la popolazione in merito a minacce di questo genere, a metterla in guardia e a consentirle una gestione sicura delle tecnologie digitali. La strategia assicura una migliore protezione dei dati permettendo alle persone interessate di tenere sotto controllo i propri dati personali e impedendo ai criminali di accedervi.
- **economia:** la presenza di un contesto sicuro costituisce una condizione importante e un vantaggio competitivo per l'economia. Le ciberminacce pongono tutte le aziende, soprattutto le PMI, di fronte a grandi sfide. L'attuazione della CSN serve ad aumentare la sicurezza per le aziende della Svizzera. Al suo interno viene definito il supporto che le aziende ricevono in via sussidiaria rispetto alle offerte del mercato per la gestione delle ciberminacce. La responsabilità dell'autoprotezione spetta alle aziende stesse;
- **infrastrutture critiche:** garantiscono la disponibilità di beni e prestazioni di servizi fondamentali. Il loro funzionamento è imprescindibile per la popolazione e l'economia svizzera. La protezione di tali infrastrutture ha un'elevata priorità ed è al centro di tutte le misure della CSN, tenendo conto delle diverse condizioni relative alla loro esposizione al rischio;
- **autorità:** la Confederazione, i Cantoni e i Comuni sono responsabili della protezione nell'ambito delle prestazioni di servizi fornite. Le autorità devono avere un'elevata disponibilità nell'adempimento al proprio compito. Inoltre, le autorità a tutti i livelli statali trattano informazioni sensibili e offrono sempre più servizi online. L'attuazione della CSN consente di migliorare la resilienza delle autorità;
- **organizzazioni internazionali e organizzazioni non governative:** la Svizzera sostiene le organizzazioni internazionali nella protezione dalle ciberminacce e crea condizioni quadro sicure per le attività delle organizzazioni internazionali e delle organizzazioni non governative in materia di cibersicurezza.

3 Misure della CSN

Per raggiungere i cinque obiettivi strategici prefissati, vengono attuate le misure descritte in questo capitolo. I provvedimenti si basano sulle attività precedenti e specificano come queste debbano essere ampliate, ulteriormente sviluppate e integrate per raggiungere gli obiettivi strategici. Esse illustrano, inoltre, quali aspetti più importanti vengano stabiliti nell'attuazione delle misure e quali attori siano coinvolti. L'elenco delle priorità riflette lo stato al momento dell'elaborazione della strategia e viene esaminato dal comitato direttivo della CSN su base continua e integrato all'occorrenza.
L'elenco degli attori non deve essere inteso come esaustivo, ma ha lo scopo di indicare al comitato direttivo gli attori a cui rivolgersi per la valutazione e l'ulteriore sviluppo della misura. Nell'elenco vengono dapprima citate in corsivo le principali unità responsabili all'interno dell'Amministrazione federale, successivamente vengono poi riportati in ordine alfabetico gli ulteriori attori rilevanti. Le organizzazioni dei Cantoni, delle scuole universitarie, dell'economia e della società vengono menzionate separatamente. Per tutte le organizzazioni vengono utilizzati degli acronimi, il cui significato viene spiegato nell'elenco delle abbreviazioni.
Prima di attuare qualsiasi misura occorre verificare la presenza delle opportune basi giuridiche o la necessità di far adeguare la legislazione da parte delle autorità statali competenti. Quanto descritto si applica, per esempio, in relazione allo scambio di dati, che va disciplinato di volta in volta nelle relative leggi e ordinanze applicabili, soprattutto per quanto concerne i dati personali.

3.1 Misure per l'obiettivo «autodeterminazione digitale»

Per rafforzare l'autodeterminazione digitale della Svizzera nella protezione contro le ciberminacce, vengono adottate misure nei settori della formazione, della ricerca, dell'innovazione nonché finalizzate alla sensibilizzazione, a migliorare la valutazione della situazione di minaccia e ad ampliare le capacità di analisi delle dipendenze e dei rischi.

M1 Formazione, ricerca e innovazione nella cibersicurezza

Tabella sinottica della misura	
Descrizione	Per proteggersi dalle ciberminacce, la Svizzera ha bisogno di personale formato da un numero sufficiente di membri con conoscenze specifiche. Allo stesso tempo, è necessario garantire che la popolazione sia in possesso delle competenze di base per gestire le tecnologie e i servizi digitali. Le relative competenze devono essere create, veicolate e sviluppate trasversalmente attraverso gli istituti di formazione e ricerca esistenti. La formazione, la ricerca e l'innovazione non sono solo necessarie per rafforzare la protezione contro le ciberminacce, ma dovrebbero piuttosto contribuire direttamente al successo della piazza economica svizzera. La Svizzera intende sfruttare la sua buona posizione di partenza come Paese neutrale, con un elevato livello d'istruzione e un efficiente sistema di innovazione, per diventare una delle sedi principali a livello mondiale per i servizi e i prodotti in materia di cibersicurezza.

Situazione di partenza e necessità d'intervento	La Svizzera vanta una rete efficiente di istituti di formazione e ricerca a diversi livelli. Negli ultimi anni sono state istituite diverse opportunità di formazione in materia di ciber-rischi. Tuttavia, l'elevata domanda da parte dell'economia di esperti in cibersicurezza non può ancora essere soddisfatta adeguatamente e l'insegnamento delle competenze relative a tale ambito non avviene ancora in modo costante a tutti i livelli di formazione (scuola dell'obbligo, livello secondario II, livello terziario, formazione continua). In Svizzera, negli ultimi anni il panorama delle start-up attive nel campo della cibersicurezza si è sviluppato in maniera considerevole e diversi attori importanti hanno aperto filiali nel nostro Paese. Nonostante ciò, un confronto con le regioni leader a livello internazionale e con la capacità d'innovazione della Svizzera in altri settori rende evidente che le condizioni quadro per le innovazioni in materia di cibersicurezza devono essere ulteriormente migliorate.
Temi principali	- Formazione: la formazione e la formazione continua in materia di cibersicurezza devono essere promosse a tutti i livelli. Mentre la scuola dell'obbligo deve insegnare principalmente le competenze di base, la formazione professionale (di base e superiore), quella universitaria e quella continua necessitano di offerte mirate e adeguate alle esigenze del mercato del lavoro. Per promuovere la formazione in materia di cibersicurezza, vengono utilizzati gli strumenti collaudati della politica formativa svizzera. Il personale docente viene supportato da materiali didattici adeguati e da specialisti della materia nell'insegnamento delle competenze in materia di cibersicurezza e viene promosso il coordinamento tra gli istituti di formazione. Per quanto riguarda il personale specializzato (p. es. nel caso delle infrastrutture critiche), si intende ampliare l'offerta di formazioni e training specifici sul territorio nazionale. - Ricerca: la ricerca sulla cibersicurezza è finanziata attraverso i mezzi esistenti della politica di ricerca. Occorre che la ricerca di rilievo nazionale abbia un impatto maggiore sulla politica, sull'economia e sulla società. A questo scopo è necessario un maggiore coordinamento tra i ricercatori dei vari ambiti della cibersicurezza, in modo da poter sviluppare e comunicare raccomandazioni comuni. - Innovazione: un ambiente ideale per l'innovazione si crea attraverso l'interconnessione degli attori. Lo scambio tra scuole universitarie, aziende e autorità deve essere ulteriormente ampliato. Nei limiti delle possibilità consentite dalla legge, gli Uffici federali competenti promuovono il coinvolgimento di esperti in materia di cibersicurezza attraverso programmi di «fellowship» per l'innovazione già esistenti e simili.
Attori centrali	- Amministrazione federale: *CYD Campus, NCSC, SEFRI* - Cantoni: CDDGP, ISP, CDPE, CSSU - Scuole universitarie: tutte le scuole universitarie svizzere, SSCC, swissuniversities, consiglio dei PF - Economia/società: Formazione Professionale Svizzera, associazioni TIC, Innosuisse, SATW

M2 Sensibilizzazione

Tabella sinottica della misura	
Descrizione	Affinché la popolazione svizzera possa utilizzare prodotti e servizi elettronici e digitali essendo consapevole dei rischi, sono necessarie misure di sensibilizzazione. L'obiettivo è creare un alto livello di consapevolezza in materia di cibersicurezza in tutti i settori e fornire strumenti che promuovano un utilizzo responsabile delle tecnologie e dei servizi digitali. In tal senso vengono anche perseguiti determinati obiettivi sul piano della protezione dei dati: da un lato si cerca di garantire che i singoli individui possano tenere sotto controllo i propri dati personali e, dall'altro, che le imprese e le organizzazioni dispongano di metodi trasparenti per il loro trattamento. Nel complesso, l'attività di sensibilizzazione intende rafforzare la resilienza della società ai ciber-rischi.
Situazione di partenza e necessità d'intervento	La sensibilizzazione rispetto alla cibersicurezza è all'ordine del giorno di numerose istituzioni, aziende e organizzazioni svizzere, sempre con l'obiettivo di rendere le aziende e i privati resilienti ai ciber-rischi. Tuttavia, sono necessari un maggiore coordinamento e un'unione degli sforzi attuali e pianificati, perché è importante sensibilizzare il più possibile in funzione dei gruppi di destinatari e delle parti interessate. Per questo motivo, occorre definire i gruppi di destinatari e accertare la necessità di misure dove vi è maggiore vicinanza ai gruppi di destinatari. I messaggi devono essere coordinati tra i mittenti per favorire, attraverso una comunicazione allineata, la comprensione da parte dei destinatari di un argomento talvolta complesso. Esistono già molte competenze per comunicare con gruppi di destinatari specifici. Per questo motivo, gli organi e le organizzazioni esistenti e i relativi canali di comunicazione delle misure dovrebbero continuare a essere utilizzati come avveniva in precedenza (p. es. attraverso eventi e riviste di settore di associazioni, gruppi d'interesse, organizzazioni ombrello).
Temi principali	- Rilevazione del fabbisogno: la necessità di sensibilizzazione e prevenzione nei diversi settori viene continuamente riesaminata. A fungere da base sono gli incidenti attuali e l'evoluzione delle situazioni di minaccia, nonché le valutazioni delle autorità, delle aziende e delle associazioni dell'economia in merito alla necessità di sensibilizzare i rispettivi ambiti. - Sintesi e coordinamento: gli attori coinvolti nella sensibilizzazione sono noti e lo scambio tra loro viene promosso in modo specifico. - Valutazione: gli oneri e gli effetti delle misure di sensibilizzazione vengono rilevati per determinarne il successo e poterli ottimizzare.
Attori centrali	- Amministrazione federale: *NCSC,* UFPP, UFCOM, UFT, UFAC, UFE, UFAS, UFAE, IFPDT, SIC - Cantoni: Comuni e città, centri di competenza cantonali per la cibersicurezza, corpi di polizia cantonali, CDDGP, PSC - Economia/società: tutte le associazioni di categoria e dell'economia interessate, le federazioni, le ONG e le singole aziende saranno coinvolte nelle campagne, laddove opportuno.

M3 Situazione di minaccia

Tabella sinottica della misura	
Descrizione	Per valutare la situazione di minaccia, è necessario determinare quali attori sfruttano o potrebbero sfruttare quali vettori di attacco e vulnerabilità. Inoltre, viene effettuata una ponderazione delle minacce. Ne consegue una valutazione della situazione di minaccia, sulla base della quale l'economia, la società e l'amministrazione possono identificare e attuare le misure di minimizzazione dei rischi nel modo più efficace e mirato possibile. La situazione di minaccia, pertanto, non illustra solo le minacce fondamentali e di ampia portata, ma anche quelle specifiche dell'azienda e del processo.
Situazione di partenza e necessità d'intervento	La Svizzera dispone già di rappresentazioni tattiche, operative e strategiche periodicamente aggiornate della situazione di minaccia nel ciberspazio. Queste vengono alimentate dall'osservazione degli attori artefici delle minacce e delle loro capacità effettive e potenziali, nonché dalle informazioni sui danni o sui guasti causati dai ciberincidenti. Data la crescente digitalizzazione dei processi in vari settori dell'economia, aumenta l'esigenza di valutazioni delle minacce specifiche per questi ambiti. Tale fabbisogno deve essere soddisfatto elaborando le informazioni rilevanti per le minacce in modo appropriato per il gruppo di destinatari. Le suddette informazioni devono essere comunicate alle aziende e alle altre organizzazioni in base alle loro esigenze.
Temi principali	- Ulteriore sviluppo del monitoraggio della situazione con particolare attenzione agli attori che rappresentano una minaccia per la Svizzera a livello tattico, operativo e strategico. - Ulteriore sviluppo della valutazione e dell'approntamento delle informazioni rilevanti per la situazione. Messa a disposizione adeguata a ogni singolo livello dell'economia, della società e dell'amministrazione. - Supporto alla creazione di centri di condivisione e analisi delle informazioni (ISAC) specifici dei singoli settori e avvio di una stretta collaborazione per valutare le situazioni di minaccia specifiche.
Attori centrali	- Confederazione: *SIC*, NCSC, - Cantoni: corpi di polizia cantonali, centri di competenza cantonali per la cibersicurezza, uffici IT, NEDIK - Economia/società: CERT/SOC dell'economia, ISAC, fornitori di servizi di sicurezza, SWITCH

M4 Analisi di tendenze, rischi e dipendenze

Tabella sinottica della misura	
Descrizione	Per la Svizzera è essenziale capire quale sia l'entità della dipendenza dalle tecnologie digitali, come si stia sviluppando e quali rischi comporti. Poiché le tecnologie digitali si sviluppano in maniera dinamica, è importante riconoscere tempestivamente i nuovi sviluppi e comprenderne l'impatto sulla sicurezza. Ciò dovrebbe contribuire a rafforzare la piazza economica svizzera, un Paese in cui vengono utilizzate tecnologie e servizi digitali sicuri sviluppati autonomamente. Un'ulteriore necessità di analisi deriva dal fatto che la maggior parte delle tecnologie digitali chiave vengono attualmente prodotte all'estero. Per la Svizzera è fondamentale capire quali dipendenze esistano da questi produttori e quali rischi vi siano associati. La Svizzera deve essere in grado di prendere decisioni sull'utilizzo delle tecnologie e dei servizi digitali sulla base di analisi e valutazioni indipendenti.

Situazione di partenza e necessità d'intervento	Il monitoraggio delle tecnologie in materia di cibersicurezza viene effettuato dal Cyber-Defence Campus in stretta collaborazione con le scuole universitarie e l'economia. Le Accademie svizzere delle scienze hanno il compito di valutare le opportunità e i rischi delle nuove tecnologie. L'analisi sistematica delle dipendenze e dei rischi legati ai prodotti TIC è decisamente meno sviluppata in Svizzera. Con l'Istituto Nazionale di Test per la Cibersicurezza (NTC), si sta creando un centro capace di esaminare a fondo i prodotti TIC per verificarne la potenziale superficie di attacco. La costituzione di questo centro permetterà ai collaboratori del CYD Campus, ma sempre più anche ad altri fornitori di servizi di sicurezza privati, di ampliare e rafforzare ulteriormente le capacità di cui già dispongono. Tali competenze sono necessarie per una valutazione indipendente della sicurezza dei prodotti utilizzati per esempio nelle infrastrutture critiche. Un ulteriore potenziale risiede nella valutazione sistematica degli incidenti, in quanto possono contribuire a capire meglio quali sono i bersagli di determinati attacchi e le modalità per prevenirli. Ciò richiede uno scambio di informazioni consolidato tra le autorità, i fornitori di servizi di sicurezza e le scuole universitarie, nonché la disponibilità delle aziende interessate a fornire informazioni trasparenti sugli incidenti e le relative conseguenze.
Temi principali	- Monitoraggio delle nuove tecnologie: insieme alle scuole universitarie, il CYD Campus anticipa gli sviluppi tecnologici nel settore della cibersicurezza e mette a disposizione i risultati dell'attività di monitoraggio a tutti gli attori rilevanti. - Ampliamento delle competenze per l'analisi dei ciberincidenti: le cause e i processi degli incidenti informatici devono essere analizzati più nel dettaglio e i risultati di queste indagini devono essere sistematicamente elaborati e precisati. A tale scopo, lo scambio di dati tra autorità, assicuratori e fornitori di servizi di sicurezza viene promosso nei limiti di quanto previsto dalla legge. Le analisi sono volontarie per le persone coinvolte e hanno lo scopo di aiutare a imparare dai ciberincidenti. - Per l'analisi di prodotti TIC e delle reti digitali è possibile rivolgersi ai centri di test sul territorio nazionale, come l'Istituto nazionale di Test per la Cibersicurezza, nonché ad altri fornitori di analisi di vulnerabilità e test di penetrazione. Con la realizzazione dell'NTC vengono così rafforzate le capacità di coloro che effettuano in Svizzera analisi indipendenti dei rischi in relazione ai prodotti TIC. In tale contesto l'NTC può contare sulla collaborazione delle scuole universitarie, degli attori dell'economia privata e di diversi partner a livello internazionale. Il CYD Campus continua a puntare sul rafforzamento delle proprie capacità analitiche nel quadro degli acquisti effettuati per la Confederazione e delle relative attività preparatorie relative a prodotti TIC critici sotto il profilo della sicurezza. - La realizzazione dell'Istituto Nazionale di Test per la Cibersicurezza è in corso di attuazione. In collaborazione con le scuole universitarie e il settore privato, si creeranno capacità per l'analisi indipendente dei rischi relative ai prodotti TIC. - Dipendenze: si analizza quanto siano pronunciate in Svizzera quali dipendenze da quali prodotti e quali fornitori. Le aziende, le scuole universitarie e le autorità stabiliscono congiuntamente le modalità di esecuzione e di aggiornamento continuo di queste analisi. - Monitoraggio delle applicazioni AI nelle infrastrutture critiche: al fine di comprendere meglio le capacità di queste applicazioni e le ripercussioni sulla società, il loro utilizzo sarà regolarmente verificato per conto della Confederazione e dei Cantoni. - Potenziamento dello scambio tra i centri di ricerca: la condivisione esistente nell'ambito del CYD Campus, delle scuole universitarie e del SATW viene ulteriormente ampliata e reciprocamente coordinata.

Attori centrali	- Amministrazione federale: *CYD Campus, NCSC*, TDT, SIC - Scuole universitarie: SSCC - Economia/società: NTC, SATW, fornitori di servizi di sicurezza

3.2 Misure per l'obiettivo «Servizi e infrastrutture digitali sicuri»

Per garantire la sicurezza dei servizi e delle infrastrutture digitali, sono necessarie misure a diversi livelli. È importante che le vulnerabilità dei servizi e delle infrastrutture siano identificate e affrontate tempestivamente e che i nuovi servizi e le nuove infrastrutture siano sviluppati in modo da avere il minor numero possibile di vulnerabilità sin dall'inizio. Oltre all'identificazione e al rilevamento delle vulnerabilità, un altro aspetto di decisiva importanza è la gestione della resilienza. L'obiettivo è determinare, sulla base delle analisi dei rischi e delle vulnerabilità, quali misure a livello tecnico e organizzativo occorre implementare per aumentare la resilienza delle prestazioni di servizi e delle infrastrutture. Occorre anche verificare in quali settori debbano essere introdotte disposizioni mediante standardizzazioni e regolamentazioni. Infine, è importante che le autorità proteggano i propri servizi dalle ciberminacce.

M5 Identificare e prevenire le vulnerabilità

Tabella sinottica della misura	
Descrizione	L'impiego delle tecnologie digitali porta all'automazione dei processi e all'interconnessione. Ne conseguono sistemi complessi che potenzialmente presentano un'ampia superficie di attacco. Tale complessità, unita ai costi spesso elevati e ai tempi stretti dello sviluppo e dell'applicazione di tali tecnologie, aumenta il rischio di vulnerabilità dei sistemi. Per la cibersicurezza, è essenziale prevenire l'insorgere di tali vulnerabilità laddove possibile e riconoscere tempestivamente quelle esistenti, nonché porvi rapidamente rimedio. È importante che le vulnerabilità vengano pubblicate solo dopo l'identificazione e l'attuazione delle contromisure («Coordinated Vulnerability Disclosure»), altrimenti la pubblicazione rafforza la posizione degli autori degli attacchi.
Situazione di partenza e necessità d'intervento	La Svizzera dispone di elevate conoscenze tecniche necessarie per identificare le vulnerabilità e analizzarne le cause, tuttavia, tale potenziale non è ancora sfruttato a sufficienza. I ricercatori nel campo della sicurezza sono poco incentivati a cercare e segnalare i punti deboli e manca un coordinamento nazionale nell'analisi delle vulnerabilità. Inoltre, è essenziale anche la stretta collaborazione con gli uffici specializzati di altri Paesi e le organizzazioni internazionali. Un presupposto per una gestione più efficace delle vulnerabilità è la creazione di basi legali per l'analisi, la segnalazione e la pubblicazione delle vulnerabilità. Infine, è necessario impegnarsi per garantire che le lacune di sicurezza vengano comunicate rapidamente e anche colmate. Troppe aziende e organizzazioni restano vulnerabili perché non risolvono le vulnerabilità, anche se le soluzioni (patch) sarebbero già disponibili da tempo.
Temi principali	- Istituzionalizzare l'hackeraggio etico: vengono condotti programmi di «bug bounty» e «public trust». L'hackeraggio etico viene promosso migliorando la certezza del diritto per gli hacker etici. - Coordinated Vulnerability Disclosure: per creare sicurezza e fiducia attraverso la trasparenza, si incoraggia un approccio coordinato al rilevamento delle vulnerabilità. A tal fine, vengono definite e diffuse direttive e creati incentivi per la segnalazione delle vulnerabilità. - Centralizzare la comunicazione delle vulnerabilità: l'NCSC si posiziona come fulcro del coordinamento e della pubblicazione delle segnalazioni di vulnerabilità e diffonde informazioni e avvisi sulle nuove vulnerabilità e sulle soluzioni tecniche e organizzative per correggerle. - Rilevamento automatico delle vulnerabilità: vengono sviluppate e distribuite soluzioni per il rilevamento automatico delle vulnerabilità e la relativa correzione. - Ecosistema software: lo sviluppo di software sicuri (soprattutto nel campo dei software open source) è supportato dalla collaborazione con organizzazioni e iniziative in questo campo. L'obiettivo è creare incentivi, affinché la sicurezza nello sviluppo di software venga presa tempestivamente in considerazione. Per quanto concerne lo sviluppo di componenti TIC, occorre definire caratteristiche di sicurezza verificabili a livello formale. - Cibersicurezza per i dispositivi senza filo collegati a Internet: i requisiti della riveduta ordinanza sugli impianti di telecomunicazione devono essere applicati attraverso un'efficace sorveglianza del mercato.
Attori centrali	- Confederazione: *UFCOM*, *CYD Campus, NCSC* - Cantoni: uffici IT, centri di competenza cantonali per la cibersicurezza - Scuole universitarie: istituti di ricerca sulla sicurezza TIC - Economia/società: Alleanza Sicurezza Digitale Svizzera, NTC, società di sicurezza

M6 Resilienza, standardizzazione e regolamentazione

Tabella sinottica della misura	
Descrizione	Per proteggersi dalle ciberminacce esistono numerose misure tecniche e organizzative. Resta il fatto che la maggior parte dei ciberincidenti potrebbe essere evitata attraverso l'attuazione coerente di misure basilari (protezione di base). Per scegliere misure adeguate, risultano fondamentali analisi approfondite sull'esposizione ai rischi delle ciberminacce. Una volta determinate le modalità con cui tali rischi si manifestano nei singoli settori, è possibile stabilire misure volte a aumentare la resilienza. Le misure adottate si orientano agli standard internazionali, i quali rappresentano uno strumento importante per l'attuazione di misure di protezione. Il rispetto di tali standard può essere promosso in modi diversi. Oltre alla possibilità di dichiarare gli standard vincolanti attraverso misure regolatorie, occorre soprattutto creare incentivi per la loro attuazione. Un forte incentivo può essere creato mediante la trasparenza, utilizzando marchi che indichino chi è conforme a quali standard. Grazie a questa trasparenza, gli investimenti nella cibersicurezza si traducono in una maggiore fiducia da parte della clientela.
Situazione di partenza e necessità d'intervento	Le analisi dei rischi e delle vulnerabilità dei settori critici facevano già parte delle prime due strategie per la protezione contro i ciber-rischi. Le valutazioni espresse e le misure identificate relative alla resilienza vanno esaminate e adattate periodicamente in tutti i settori critici. Esistono già standard internazionali consolidati per la cibersicurezza che vengono applicati anche in Svizzera. In collaborazione con il mondo dell'economia e gli uffici specializzati, l'UFAE ha elaborato uno standard TIC minimo e ulteriori standard minimi per i diversi settori. Nella maggior parte dei casi, l'osservanza di tali standard non è disciplinata in maniera vincolante. Con la nuova legge sulla protezione dei dati, la cui entrata in vigore avverrà nel settembre del 2023, verranno introdotti alcuni requisiti minimi relativi alla sicurezza dei dati nell'ambito del trattamento dei dati personali. In diversi settori si sta inoltre verificando quali standard dovrebbero essere introdotti come vincolanti per quali organizzazioni. Oltre agli standard specifici del settore sono importanti anche quelli legati alla tecnologia. Gli standard di sicurezza per l'applicazione del cloud computing o dell'IoT svolgono un ruolo rilevante nel garantire la sicurezza delle nuove applicazioni tecnologiche. Con l'ordinanza dell'UFCOM sugli impianti di telecomunicazione, la Svizzera ha già emanato disposizioni in materia di sicurezza dei dispositivi senza filo collegati a Internet e sta ora verificando quali prescrizioni siano necessarie nel settore del cloud computing. Tuttavia, la necessità di esaminare e sviluppare basi legali non si limita alla questione dell'introduzione di standard in modo vincolante. Ne è un esempio la proposta già approvata di introdurre l'obbligo di notifica dei ciberattacchi. È necessario valutare costantemente dove sussista un eventuale ulteriore fabbisogno di basi legali.

Temi principali	- Le attuali analisi dei rischi e delle vulnerabilità nei sottosettori critici vengono aggiornate, all'occorrenza, dall'UFPP e dagli uffici specializzati competenti. I rischi identificati vengono affrontati nell'ambito della gestione della resilienza con la definizione di settori d'intervento e di misure adeguate volte a migliorare la resilienza stessa. L'attuazione delle misure viene costantemente verificata; viene altresì promosso lo scambio, tra la Confederazione e i Cantoni, di informazioni riguardanti i rischi, le vulnerabilità e le misure in materia di resilienza. - L'osservanza degli standard viene incoraggiata nei vari settori. In particolare, l'applicazione degli standard tra le PMI e i Comuni deve essere rafforzata mettendo a disposizione strumenti semplici. Nel caso degli appalti pubblici, deve essere richiesta e verificata anche l'osservanza degli standard di sicurezza delle TIC. - Promuovere la diffusione dei marchi esistenti: in Svizzera sono stati introdotti con successo marchi di cibersicurezza. È importante che questi siano coordinati tra loro a livello nazionale e internazionale. L'utilizzo dei marchi esistenti dovrebbe quindi essere sostenuto attraverso lo scambio di conoscenze tra i marchi stessi. - Si sta valutando se e come la responsabilità delle aziende per la propria protezione contro i ciberincidenti possa essere rafforzata attraverso disposizioni legali. L'obiettivo è quello di avere regolamentazioni efficienti piuttosto che disposizioni operative dettagliate. Le normative devono inoltre essere armonizzate a livello intersettoriale per ridurre al minimo le disparità tra le eventuali disposizioni. - Verrà esaminata la necessità di regolamentazioni specifiche per il settore e, se del caso, verranno preparati i relativi modelli. - L'obbligo di notifica dei ciberattacchi alle infrastrutture critiche è già in fase di valutazione. Nel caso si giunga a una decisione, l'attuazione sarà affrontata in stretta collaborazione con le persone interessate.
Attori centrali	- Confederazione: *UFPP, UFCOM, UFT, UFAC, UFE, NCSC,* UFAE, IFPDT - Cantoni: centri di competenza cantonali per la cibersicurezza - Scuole universitarie: SSCC - Economia/società: cyber-safe.ch, ITSec4KMU, organizzazioni di normazione, NTC, fornitori di servizi di sicurezza, associazioni dei settori economici interessati, istituti assicurativi

M7 Intensificazione della collaborazione tra le autorità

Tabella sinottica della misura	
Descrizione	La cibersicurezza è diventata una sfida di prioritaria importanza per le autorità a tutti i livelli statali. I servizi digitali delle autorità devono disporre di un elevato livello di sicurezza. Mentre per anni gli attacchi a scopo di spionaggio sono stati tra le ciberminacce più rilevanti, negli ultimi tempi sono aumentati anche gli attacchi alle autorità da parte dei criminali informatici. Questi le ricattano, per esempio, con la crittografia e la pubblicazione di dati che le riguardano. È necessario che tali problematiche vengano affrontate a tutti i livelli statali.
Situazione di partenza e necessità d'intervento	Ogni autorità è responsabile della propria cibersicurezza. La legge sulla sicurezza delle informazioni (LSIn) definisce il quadro e le procedure per le misure di sicurezza in seno alla Confederazione e si applica ai Cantoni quando accedono alle risorse informatiche della Confederazione o trattano informazioni classificate della Confederazione. Garantire la cibersicurezza in tutte le strutture federali rappresenta una sfida importante. A causa della mancanza di personale specializzato e spesso anche di risorse finanziarie, la collaborazione tra le autorità a tutti i livelli è essenziale. I canali necessari per la cooperazione esistono, ma vi è ancora molto potenziale per una collaborazione operativa più efficace. Va inoltre chiarito in che misura la Confederazione possa sostenere i Cantoni, le città e i Comuni e in quali casi.
Temi principali	- Applicazione della legge sulla sicurezza delle informazioni all'interno dell'Amministrazione federale. - Promozione dello scambio di informazioni relative alla cibersicurezza all'interno dell'Amministrazione federale, in particolare tra l'NCSC e gli uffici specializzati. - Intensificazione della collaborazione tra la Confederazione e i Cantoni. - Chiarimento sull'entità del supporto che la Confederazione può offrire a Cantoni, città e Comuni. - Chiarimenti sull'entità del supporto dei Cantoni ai Comuni. - Promozione dello scambio con le autorità internazionali.
Attori centrali	- Confederazione e Cantoni: *RSS*, TDT, ADS, centri di competenza cantonali per la cibersicurezza, esercito, organizzazioni comunali (p.es. Associazione dei Comuni Svizzeri, Unione delle città svizzere), NCSC

3.3 Misure per l’obiettivo «Riconoscimento, prevenzione, gestione e difesa efficaci in materia di ciberincidenti»

Riconoscere, prevenire, gestire e difendersi in modo efficace dai ciberattacchi sono i fattori chiave della cibersicurezza. Per determinare misure di protezione adeguate, deve essere chiaro contro quali minacce devono agire. Se si verifica un incidente, sono necessari strumenti, dati e processi adeguati per la gestione degli incidenti. Il passo successivo consiste nell’identificare i responsabili dell’attacco nel modo più preciso possibile (attribuzione). Questo a sua volta aiuta a valutare con maggiore precisione la situazione di minaccia e a prevenire i futuri attacchi. Se i ciberincidenti hanno ripercussioni sul funzionamento delle infrastrutture critiche o sulla sicurezza della Svizzera, diventa necessaria una gestione della crisi. Affinché funzioni, è necessario ricorrere regolarmente a esercitazioni pratiche.
Infine, le possibilità di difesa dai ciberattacchi non si limitano alle misure di protezione dei propri sistemi. È importante che i dati tecnici sugli autori degli attacchi, le loro infrastrutture e il loro modus operandi siano raccolti e resi disponibili alle potenziali vittime. Sono possibili anche misure attive volte a individuare le ciberminacce, identificare gli autori, ostacolare e bloccare gli attacchi.

M8 Gestione degli incidenti

Tabella sinottica della misura	
Descrizione	Poiché non esiste un modo per proteggersi totalmente dai ciberincidenti, la creazione e il mantenimento di un’organizzazione incaricata della gestione degli incidenti costituiscono un compito fondamentale della cibersicurezza. 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 con competenze decisionali definite in modo chiaro 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.

Situazione di partenza e necessità d'intervento	Per gestire i ciberincidenti in Svizzera molte organizzazioni, ma non ancora tutte le infrastrutture critiche, si sono dotate internamente di team specializzati oppure hanno affidato l'incarico a società esterne. Questi team hanno denominazioni diverse (p.es. Security Operations Center, Computer Emergency Response Team, Computer Security Incident Response Team) e competenze specifiche nel proprio settore di compiti. Anche la Confederazione e molti Cantoni dispongono di analoghi team, ed è a loro che è affidata in primo luogo la gestione degli incidenti. Attraverso l'NCSC, la Confederazione supporta sussidiariamente i team dei Cantoni, dei Comuni e delle città, nonché dei gestori di infrastrutture critiche e dei loro fornitori di servizi di sicurezza nell'analisi tecnica degli incidenti e sostiene lo scambio di informazioni tra loro. Anche il pubblico può segnalare all'NCSC incidenti informatici e ciberminacce e, se necessario, ricevere le prime valutazioni specialistiche e raccomandazioni su come procedere. Tali notifiche sono importanti per la valutazione delle ciberminacce. Finora, queste prestazioni da parte della Confederazione non si fondano su basi legali e anche il quadro giuridico dello scambio di informazioni deve essere disciplinato. Le proposte per i necessari adeguamenti legali sono state elaborate, ma non sono ancora state prese decisioni in merito. Una sfida nella gestione degli incidenti è rappresentata dalla scalabilità. Se si verificano contemporaneamente diversi eventi di grande rilevanza, le risorse esistenti si esauriscono rapidamente. Occorre valutare come aumentare rapidamente le capacità attraverso il coinvolgimento di esperti, se necessario.
Temi principali	- Rafforzamento delle capacità delle infrastrutture critiche di rilevare e gestire i ciberincidenti attraverso l'istituzione, la creazione e l'utilizzo comune di SOC. - Ampliamento delle notifiche di ciberincidenti: dovrebbe essere segnalato il maggior numero possibile di incidenti informatici, in modo che emerga un buon quadro dell'attuale situazione di minaccia. - Scambio di informazioni: l'attuale piattaforma dell'NCSC per lo scambio di informazioni tra i gestori di infrastrutture critiche sarà rivista e ampliata con l'obiettivo di semplificarla e renderla gradualmente accessibile a un pubblico più ampio. - Ampliamento della capacità attraverso la collaborazione: ulteriore intensificazione della cooperazione operativa e miglioramento del coordinamento tra GovCERT, SWITCH-CERT e altri team di sicurezza informatica. Si sta inoltre valutando come e quando i pool di esperti volontari possano supportare la gestione degli incidenti, tenendo in considerazione le organizzazioni esistenti. - Intensificazione della collaborazione con gli uffici specializzati: affinché gli uffici specializzati competenti siano in grado di valutare le minacce nel loro settore, vengono informati dall'NCSC sugli incidenti che si verificano nel loro ambito. Sono escluse le informazioni che consentono di risalire alle persone interessate, a meno che queste ultime non acconsentano a fornire informazioni agli uffici specializzati.
Attori centrali	- Confederazione: *NCSC,* UFCOM, UFT, UFAC, UFE, UFIT, milCERT - Cantoni: CERT cantonali, CSIRT, SOC (o organizzazioni simili), servizi di segnalazione delle polizie cantonali - Economia/società: CERT, CSIRT, SOC (o organizzazioni simili) di aziende e organizzazioni, SWITCH

M9 Attribuzione

Tabella sinottica della misura	
Descrizione	Il concetto di attribuzione consiste nell'identificare la paternità degli attacchi nel modo più preciso possibile. Tale aspetto svolge un ruolo importante nella scelta dei mezzi per le azioni successive. Le autorità svizzere devono essere in grado di attribuire una paternità ai ciberattacchi diretti contro il nostro Paese rilevanti per la politica di sicurezza. Può trattarsi di attacchi informatici perpetrati contro vittime sul territorio nazionale o dell'utilizzo improprio di infrastrutture svizzere per attacchi all'estero. L'attribuzione costituisce la base per la formulazione di opzioni d'intervento politiche e legali.
Situazione di partenza e necessità d'intervento	Per fare in modo che gli autori di un ciberattacco rispondano delle loro azioni, occorre innanzitutto identificarli. Si tratta di una grande sfida nel ciberspazio, perché gli autori non si trovano fisicamente sul luogo dell'attacco. L'identificazione può essere realizzata solo se gli attacchi vengono riconosciuti tempestivamente e se è possibile analizzarne il contesto tecnico, operativo e strategico. L'attribuzione dei ciberattacchi è un compito del Servizio delle attività informative della Confederazione (SIC). Per assolverlo, ha bisogno dei risultati delle proprie ricerche, ma si affida anche alla collaborazione con altri uffici della Confederazione e agli scambi di informazioni con i servizi partner, che necessita di essere disciplinata. L'attribuzione dei ciberattacchi è importante per i responsabili politici ai fini della valutazione della situazione di minaccia. In tale contesto viene valutato anche se l'attribuzione possa avvenire sul piano del diritto internazionale e come sia possibile reagire nel quadro delle possibilità contemplate da tale diritto. Il processo di attribuzione costituisce inoltre il presupposto per decisioni prese su misure di carattere tecnico, politico o penale.
Temi principali	- Verifica e integrazione delle basi legali per l'analisi dei ciberattacchi alla Svizzera. - Collaborazione tra il SIC e altri uffici. - Rafforzamento delle competenze del SIC di analizzare gli attacchi informatici rilevanti sotto il profilo della politica. - Definizione delle priorità strategiche: è necessario stabilire quali attacchi verranno analizzati in modo approfondito.
Attori centrali	- Confederazione: *SIC,* DFAE, fedpol, NCSC, SG-DDPS - Cantoni: Corpi di polizia cantonale, NEDIK

M10 Gestione delle crisi

Tabella sinottica della misura	
Descrizione	I ciberincidenti possono avere gravi conseguenze rendendo persino necessaria una gestione della 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. Le capacità e le strutture corrispondenti devono essere regolarmente esercitate, verificate e adeguate.
Situazione di partenza e necessità d'intervento	La collaborazione intersettoriale è fondamentale in caso di crisi. In situazioni di crisi, l'NCSC deve essere in grado di instaurare rapidamente la collaborazione con tutte le parti rilevanti contattando le rispettive organizzazioni interne ed esterne all'Amministrazione federale. L'NCSC è stato inoltre integrato negli stati maggiori di crisi della Confederazione. In ogni ulteriore sviluppo o riorganizzazione della gestione delle crisi nella Confederazione, occorre inoltre garantire che la cibersicurezza sia direttamente integrata nelle strutture di gestione delle crisi. La collaborazione tra gli attori centrali della Confederazione, dei Cantoni e dell'economia per la gestione di una crisi con tempi ristretti è impegnativa. Per funzionare, è necessario effettuare regolarmente esercitazioni. Al momento la Svizzera partecipa a esercitazioni internazionali, mentre a livello nazionale sono state condotte altre esercitazioni specifiche per ogni settore. Manca tuttavia un programma generale relativo alla pianificazione e all'attuazione delle esercitazioni per le crisi nell'ambito della cibersicurezza. È quindi necessario mettere a punto una pianificazione di questo genere e integrarla in quella delle esercitazioni generali.
Temi principali	- Ideazione e realizzazione di esercitazioni specifiche di ogni settore (p.es. fornitura di energia, fornitura di acqua, assistenza sanitaria) e intersettoriali in ambito ciber. La pianificazione e l'ideazione devono avvenire in coordinamento con la pianificazione delle esercitazioni generali per la gestione delle crisi. - Integrazione di aspetti legati alla cibersicurezza in tutte le esercitazioni previste. - Chiarimenti sulle basi, in linea con i lavori sovraordinati relativi all'organizzazione della gestione delle crisi: quali criteri definiscono una crisi in relazione alla cibersicurezza? Quali strutture sono responsabili della valutazione politica e dell'avvio di misure di gestione delle crisi? - Garanzia che la cibersicurezza sia rappresentata nel dispositivo di gestione delle crisi (a livello di Confederazione e di Cantoni). - Chiarimenti sul supporto (sussidiario) per la gestione delle crisi in collaborazione, compresi i mezzi di comunicazione da utilizzare.
Attori centrali	- Confederazione: *CaF, UFPP, NCSC,* esercito, UFCOM, UFT, UFAC, UFE, UFAE, DFAE, SG-DDPS, RSS - Cantoni: organizzazioni cantonali di condotta, centri di competenza cantonali per la cibersicurezza - Economia/società: gestori di infrastrutture critiche, produttori/fornitori di software critici, organizzazioni di settore (p.es. FS-CSC svizzero, SWITCH-CERT)

M11 Ciberdifesa

Tabella sinottica della misura	
Descrizione	La libertà di azione e l'integrità dello Stato, dell'economia e della popolazione devono essere protette nel ciberspazio e difese in caso di conflitto. La ciberdifesa comprende tutte le misure militari e del Servizio delle attività informative che servono ai seguenti scopi: protezione dei sistemi critici per la difesa del Paese, difesa dai ciberattacchi, garanzia dell'efficienza operativa dell'Esercito svizzero in ogni circostanza e creazione di capacità e competenze per fornire un supporto sussidiario alle autorità civili. Tra queste rientrano, tra le altre cose, le misure attive volte ad individuare le ciberminacce, identificare gli aggressori, ostacolare e bloccare gli attacchi.
Situazione di partenza e necessità d'intervento	Il Servizio delle attività informative della Confederazione (SIC) e l'Esercito svizzero hanno ampliato le loro capacità per assolvere i loro compiti nel settore della ciberdifesa. Il «Concetto generale ciber» descrive le capacità che l'Esercito svizzero deve sviluppare entro la metà degli anni 2030 per essere in grado di contrastare le minacce presenti e provenienti dal ciberspazio e dallo spazio elettromagnetico. Con la legge federale sulle attività informative (LAIn) e la riveduta legge militare (LM), la Confederazione dispone delle basi legali necessarie per adottare contromisure attive nell'ambito della ciberdifesa. L'aumento dei ciberattacchi negli ultimi anni e la loro crescente complessità richiedono tuttavia un numero maggiore di risorse per lunghi periodi. Pertanto, si evidenzia la necessità di continuare a intervenire per rafforzare le capacità e coordinare gli uffici competenti a fine di garantire il rispetto del diritto internazionale.
Temi principali	- Rafforzamento delle competenze centrali a livello di esercito. A questa categoria appartengono l'autoprotezione SEC, lungimiranza/autonomia, competenze di base sulla scienza dei dati. - Creazione di competenze decentrate. Esse comprendono, per esempio, il trattamento stabile e sicuro dei dati nei battaglioni e nelle compagnie. Un altro aspetto essenziale riguarda il rafforzamento della resilienza dell'infrastruttura di base rilevante ai fini dell'impiego nell'autoprotezione SEC. Inoltre, l'organizzazione delle associazioni verrà adattata. - Affinamento della gestione dei casi relativi a ciber campagne rilevanti ai fini della politica di sicurezza. - Maggiore integrazione delle competenze della Svizzera per proteggere nell'immediato gli stakeholder a livello nazionale. - Ampliamento delle competenze di base per le azioni nel ciberspazio da parte del SIC e dell'esercito.
Attori centrali	- Confederazione: *esercito*, CYD Campus, SG-DDPS, SIC - Cantoni: organizzazioni cantonali di condotta

3.4 Misure per l'obiettivo «Lotta e perseguimento penale efficaci in materia di cibercriminalità»

L'infrastruttura digitale che Internet ci mette a disposizione offre ai potenziali criminali nuove opportunità di commettere reati che possono arrecare ingenti danni alla società e all'economia. La cibercriminalità 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 i ciberincidenti, pur prendendo avvio nel mondo virtuale, possano sortire i loro effetti dannosi nel mondo reale.
Alla luce di tali sviluppi, è importante migliorare ulteriormente l'interoperabilità e la capacità di reazione su tutto il territorio nazionale ricorrendo alla collaborazione con partner internazionali. Risulta altrettanto importante coordinare efficacemente le competenze specialistiche, tecniche e personali senza per questo modificare l'attribuzione di poteri tra le diverse autorità e livelli statali.

M12 Intensificazione della collaborazione tra le autorità di perseguimento penale

Tabella sinottica della misura	
Descrizione	La collaborazione nel perseguimento penale dei cibercriminali tra la Confederazione e i Cantoni e tra i Cantoni stessi deve essere ulteriormente rafforzata. Si tratta di un aspetto fondamentale ai fini di un perseguimento penale efficiente ed efficace. Essa avviene già oggi nei limiti di quanto previsto dalla legge, in particolare attraverso la Rete di supporto alle indagini per la lotta alla criminalità digitale (NEDIK), ma deve essere consolidata e ulteriormente sviluppata. Questo include anche la verifica di quali adeguamenti delle basi legali siano necessari a tale scopo. La collaborazione può essere rafforzata attraverso diversi ulteriori provvedimenti. Definendo procedure comuni e standardizzando i processi, si pongono già le basi per una cooperazione più semplice. Nel caso di competenze specialistiche difficili da acquisire (p.es. nel campo della scienza forense digitale), uno scambio diretto tra addetti ai lavori o anche un raggruppamento regionale di competenze può essere molto utile, anche per quanto riguarda un'offerta coordinata di formazione e formazione continua. La cooperazione internazionale, in particolare la collaborazione con EUROPOL, va ulteriormente rafforzata in quanto decisiva in materia di perseguimento penale.

Situazione di partenza e necessità d'intervento	Il Cyberboard è una piattaforma di coordinamento e collaborazione per la lotta alla cibercriminalità in cui sono rappresentati tutti gli attori più importanti. Esso coordina l'elaborazione dei casi, offre alle autorità di perseguimento penale l'opportunità di scambiare informazioni sul modus operandi adottato in Svizzera, sui casi tipici e sulle costellazioni di casi, riconosce i riferimenti trasversali e, se necessario, esamina e avvia misure per migliorare i processi esistenti. Nell'ambito del Cyberboard, il Cyber-CASE intende facilitare lo scambio di informazioni e conoscenze tra i ministeri pubblici e le autorità inquirenti specializzati nel quadro di tre o quattro incontri annuali. Il Cyberboard verrà ulteriormente potenziato. La collaborazione tra le polizie cantonali sarà intensificata attraverso la NEDIK (Rete di supporto alle indagini per la lotta alla criminalità digitale), che effettua un regolare coordinamento delle questioni strategiche e operative, e il centro di competenza informatico regionale Cyber Competence Center RC3. Grazie a questi organi, sono già state poste ottime basi di collaborazione, che devono essere ulteriormente rafforzate. Ora la cooperazione può essere promossa in modo mirato in quei settori in cui si ottengono i maggiori benefici. Le regole di competenza locali del Codice di procedura penale complicano il perseguimento penale dei cibercriminali. La creazione di basi legali per lo scambio di dati a livello nazionale deve quindi essere esaminata con urgenza.
Temi principali	- Intensificazione della collaborazione esistente, standardizzando i processi e le interfacce e promuovendo lo scambio di conoscenze. - Raggruppamento delle competenze specialistiche (p.es. in materia di informatica forense) e degli acquisti rilevanti per la sicurezza. - Coordinamento in collaborazione con gli attori nazionali e internazionali, segnatamente nel settore dell'assicurazione delle prove e dell'assistenza giudiziaria. - Verifica delle basi legali per la collaborazione e creazione di nuove basi, se necessario.
Attori centrali	- Confederazione: *MPC*, *fedpol,* UFG - Cantoni: corpi di polizia cantonali, CDDGP, CCPCS, Ministeri pubblici, CPS - Organi comuni: Cyberboard, NEDIK, CPS

M13 Panoramica dei casi

Tabella sinottica della misura	
Descrizione	Una panoramica degli eventi è un presupposto fondamentale ai fini della valutazione della situazione di minaccia e rappresenta uno strumento di grande rilevanza anche in materia di perseguimento penale. Una panoramica dei casi è volta ad aumentare l'efficienza, la qualità e il tasso di risoluzione degli stessi in presenza di casi intercantonali o internazionali complessi. Si distinguono tre livelli di panoramica dei casi: eventi (p.es. incidenti notificati), segnalazioni ricevute e panoramica dei casi giudiziari in corso. Si ottiene una panoramica completa quando i dati provenienti dai diversi livelli possono essere correlati e valutati in tempo reale.
Situazione di partenza e necessità d'intervento	Con l'istituzione del servizio nazionale di contatto per le questioni legate alle ciberminacce presso l'NCSC e dei servizi di segnalazione presso le polizie cantonali (p.es. cybercrimepolice.ch), è stato possibile ottenere un numero significativamente maggiore di informazioni sui ciberincidenti dalla popolazione e dall'economia. L'Ufficio federale di statistica pubblica inoltre ogni anno le cifre relative all'evoluzione della cibercriminalità digitale. Già oggi le autorità giudiziarie e di perseguimento penale condividono i dati disponibili nei limiti di quanto previsto dalla legge. Per il rilevamento sistematico e strutturato dei casi, la piattaforma PICSEL (Plateforme d'Information de la Criminalité Sérielle En Ligne) è uno strumento che permette di stabilire serie e identificare nuovi fenomeni e modi di operare. PICSEL è già in uso e verrà ulteriormente sviluppata dal Centro di competenza per le tecniche informatiche e di polizia (PIT). Non tutti i Cantoni sono coinvolti nell'utilizzo della piattaforma. Il motivo risiede nella mancanza di basi legali comuni e unitarie che permetterebbero di utilizzare la piattaforma in tutta la Svizzera. È necessario chiarire come sia possibile creare le basi legali per una piattaforma finalizzata allo scambio di informazioni. La NEDIK redige mensilmente una panoramica degli eventi attuali nel campo della cibersicurezza e il servizio di notifica dell'NCSC pubblica settimanalmente i numeri di casi degli incidenti segnalati, suddivisi per fenomeno. Inoltre, la statistica criminale di polizia elenca annualmente il numero di casi per fenomeno. Tuttavia, lo scambio e l'approntamento delle statistiche sui casi non avviene ancora in modo completo e strategicamente controllato, motivo per cui non è ancora disponibile una panoramica dei casi a livello nazionale.
Temi principali	- Rappresentazione della situazione relativa ai ciberincidenti suddivisa per eventi: il servizio nazionale di contatto dell'NCSC registra le segnalazioni di incidenti ricevute e scambia informazioni con i servizi di contatto delle autorità di polizia. - È necessario chiarire le condizioni quadro giuridiche per lo scambio di informazioni tra i servizi di contatto e le autorità di perseguimento penale. - Panoramica dei casi delle segnalazioni ricevute e dei procedimenti giudiziari e di polizia in corso: verranno creati i presupposti legali e tecnici per consentire la registrazione centralizzata delle segnalazioni penali ricevute sui ciberincidenti e sui procedimenti in corso.
Attori centrali	- Confederazione: *MPC, fedpol,* NCSC - Cantoni: corpi di polizia e Ministeri pubblici cantonali, CDDGP, NEDIK, CPS, PTI

M14 Formazione delle autorità di perseguimento penale

Tabella sinottica della misura	
Descrizione	La cibercriminalità comprende reati molto diversi tra loro, che vengono commessi con metodi in continua evoluzione e che spesso non sono facili da definire e limitare, il che rende impegnativa la gestione dei ciber-reati per le autorità di perseguimento. A tutti i livelli del perseguimento penale deve essere garantita la disponibilità delle conoscenze necessarie sulla cibercriminalità per l'espletamento dei compiti.
Situazione di partenza e necessità d'intervento	La formazione di base sulla cibercriminalità si svolge nelle scuole di polizia e presso l'Istituto svizzero di polizia (ISP). Nella Svizzera romanda è disponibile anche l'offerta dell'«Ecole romande de la magistrature pénale (ERMP)» e dell'«Institut de lutte contre la criminalité économique (ILCE)». Oltre a questi programmi di formazione specifici, al personale delle autorità di perseguimento penale sono rivolte anche numerose offerte formative delle università e delle scuole universitarie professionali. Anche per procuratori, giudici e cancellieri esistono già opportunità di formazione. Su incarico della Conferenza dei comandanti delle polizie cantonali della Svizzera (CCPCS), con cyberpie.ch è stata creata una piattaforma che raccoglie le principali opportunità di formazione pertinenti. Inoltre, la NEDIK organizza ogni anno diversi corsi di formazione per specialisti in base alle esigenze attuali e con la creazione di CyberWiki mette a disposizione una piattaforma informativa nazionale. La PSC fornisce alle polizie cantonali opuscoli specifici contenenti informazioni sui singoli fenomeni, rafforzando così la formazione del personale di polizia. Sulla base delle possibilità esistenti, è importante promuovere ulteriormente la formazione delle autorità giudiziarie e di perseguimento penale. Occorre inoltre intensificare ulteriormente gli scambi di esperienze tra le autorità nonché tra le autorità stesse e il settore privato, in quanto costituiscono un modo per trasmettere le conoscenze del settore. L'Istituto svizzero di polizia dovrebbe essere in grado di svolgere un ruolo centrale di coordinamento in questo senso.
Temi principali	- Ulteriore sviluppo delle offerte formative: si verifica continuamente se le offerte esistenti soddisfano le esigenze. Qualora vi sia un fabbisogno supplementare, si chiarirà come creare nuove offerte. - Scambio di esperienze: attraverso praticantati, pool di esperti o piattaforme online, viene promosso lo scambio di conoscenze tra le autorità di perseguimento penale.
Attori centrali	- Confederazione: *MPC, fedpol,* NCSC - Cantoni: corpi di polizia cantonali, CCPCS, NEDIK, Ministeri pubblici, CPS, ISP, ASR-SVM - Economia/società: ISP, scuole universitarie

3.5 Misure per l'obiettivo «Ruolo centrale nella cooperazione internazionale»

La cibersicurezza è un aspetto importante della politica estera. I ciberattacchi vengono sempre più utilizzati dagli attori statali come 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 tra attori statali e non statali si combattono anche nello spazio digitale. Per ridurre i ciber-rischi è quindi imprescindibile la collaborazione internazionale a livello sia diplomatico che tecnico-operativo e nel settore della formazione e della formazione continua coordinata.
La tutela degli interessi della Svizzera in materia di politica estera e di sicurezza deve essere garantita anche nel ciberspazio. Pertanto, sia a livello diplomatico che a livello tecnico-operativo, nonché nel settore della formazione e della formazione continua, la Svizzera si impegna in favore del rafforzamento della cooperazione internazionale per ridurre al minimo i ciber-rischi.

M15 Rafforzamento della piazza internazionale digitale ginevrina

Tabella sinottica della misura	
Descrizione	Il Consiglio federale si è posto l'obiettivo di posizionare la Svizzera, e in particolare la Ginevra internazionale, come sede principale dei dibattiti sulla digitalizzazione e le tecnologie. Ciò implica che la Svizzera sia in grado di offrire alle organizzazioni internazionali e alle organizzazioni non governative internazionali con sede nel nostro Paese le migliori condizioni quadro possibili. Poiché molte di queste organizzazioni sono politicamente esposte, sono spesso oggetto di ciberattacchi. La Svizzera deve quindi valutare in che modo sia possibile migliorare le condizioni quadro per permettere a queste organizzazioni di proteggersi dalle ciberminacce.
Situazione di partenza e necessità d'intervento	Le organizzazioni della Ginevra internazionale devono affrontare sempre più spesso minacce provenienti dallo spazio digitale. Se la Svizzera vuole continuare a essere una sede interessante per le organizzazioni internazionali e le organizzazioni non governative, occorre verificare come si possano creare buone condizioni quadro anche per queste ultime nello spazio digitale. Inoltre, le organizzazioni internazionali e le ONG con sede in Svizzera devono essere supportate nella prevenzione. La Confederazione sta partecipando alla realizzazione dell'ISAC («Information Sharing and Analysis Centre») mettendo a disposizione di queste organizzazioni informazioni di carattere specialistico . In questo modo contribuisce e partecipa allo scambio di esperienze tra le organizzazioni.
Temi principali	- Istituzione dell'ISAC per la piazza internazionale ginevrina: lo scambio di informazioni ed esperienze tra le organizzazioni internazionali viene promosso attraverso l'istituzione del centro. - Per i servizi digitali vanno create condizioni quadro interessanti che vanno esaminate tenendo conto delle organizzazioni internazionali e delle ONG.
Attori centrali	- Confederazione: *DFAE,* UFCOM, SG-DDPS, NCSC, SIC - Economia/società: organizzazioni internazionali, ONG

M16 Regole internazionali nel ciberspazio

Tabella sinottica della misura	
Descrizione	La Svizzera si impegna attivamente a favore di un ciberspazio aperto, libero e sicuro, nel quale il diritto internazionale venga pienamente riconosciuto, rispettato e attuato, nonché chiarisce con gli altri Stati l'applicazione concreta delle norme attualmente in vigore. La Svizzera contribuisce inoltre alla creazione di condizioni quadro che facilitino la lotta internazionale contro la cibercriminalità. Il nostro Paese persegue questi obiettivi negli organismi internazionali come l'ONU, l'OSCE o l'OCSE, negli organi specializzati internazionali, come anche a livello bilaterale.
Situazione di partenza e necessità d'intervento	Dal 2004 la comunità internazionale negozia, all'interno di alcuni gruppi di lavoro dell'ONU, l'applicazione del diritto internazionale pubblico nel ciberspazio. La Svizzera è stata coinvolta in queste discussioni fin dall'inizio e, insieme agli Stati che condividono gli stessi interessi, si impegna a favore di un ciberspazio aperto, libero e sicuro in cui il diritto internazionale venga pienamente riconosciuto, rispettato e attuato. In quest'ottica, la Svizzera sostiene un approccio inclusivo e multistakeholder. Più concretamente, le sfide nella lotta alla cibercriminalità sono diventate più complesse e si rende necessaria una cooperazione internazionale più efficace tra le autorità di perseguimento penale. Il cloud computing si è delineato come una sfida da non sottovalutare, in quanto i dati vengono elaborati sempre più spesso in territorio straniero da aziende di Stati terzi. In questo caso, la Svizzera vuole creare maggiore certezza del diritto con accordi bilaterali.
Temi principali	- Partecipazione attiva ai processi dell'ONU: la Svizzera partecipa ai processi pertinenti, in particolare all'Open Ended Working Group (OEWG) e ai negoziati per una convenzione dell'ONU sulla cibercriminalità. - Partecipazione attiva della Svizzera all'ulteriore sviluppo e all'attuazione della Convenzione del Consiglio d'Europa sulla criminalità informatica (Convenzione di Budapest). - Partecipazione attiva all'attuazione delle misure dell'OCSE volte a creare un clima di fiducia. - La Svizzera tiene colloqui bilaterali per affrontare questioni tra gli Stati e conclude accordi con partner di importanza strategica.
Attori centrali	- Confederazione: *DFAE,* esercito, UFT, UFCOM, UFAC, UFE, UFG, SG-DDPS, NCSC

M17 Collaborazione bilaterale con partner strategici e centri di competenza internazionali

Tabella sinottica della misura	
Descrizione	La Svizzera adotta misure per intensificare, coordinare ed espandere in modo mirato la collaborazione operativa con i partner internazionali. Tenuto conto della portata internazionale della cibersicurezza, la cooperazione mirata con partner internazionali, centri di competenza e organizzazioni specializzate di spicco è determinante per il successo dell'attuazione di tutte le misure di protezione contro le ciberminacce.
Situazione di partenza e necessità d'intervento	Nel ciberspazio globale, la Svizzera necessita della collaborazione con altri Stati. L'esperienza dimostra che tali attività sono sostenibili solo se si fondano su ampie basi e interessi comuni. Nell'ambito delle varie attività, la Svizzera intrattiene relazioni bilaterali con partner strategici. La cooperazione internazionale è particolarmente importante in materia di perseguimento penale. Senza il reciproco sostegno tra i diversi Stati, infatti, non è possibile perseguire in maniera efficace i responsabili di reati che agiscono a livello globale. Per questo motivo, la Svizzera scambia informazioni relative ai suddetti temi a livello operativo e strategico con gli organi specializzati competenti, ma anche direttamente con altri Stati. Oltre alla collaborazione statale, è molto importante ai fini della cibersicurezza anche la cooperazione con iniziative private internazionali e centri di competenza tecnici. Una cooperazione di questo genere che implica un elevato livello di fiducia può contribuire in modo significativo a una migliore comprensione della situazione di minaccia rilevante e del suo sviluppo e a una protezione più efficace della società, dell'economia e dell'amministrazione. A tal fine è necessaria una collaborazione a lungo termine che goda del massimo livello di fiducia e l'istituzione e lo sviluppo mirati di reti internazionali di attori rilevanti in Svizzera.
Temi principali	- I ciberdialoghi esistenti con gli Stati partner continueranno a essere portati avanti e se ne auspica l'instaurazione con altri Stati. - La Svizzera verifica con gli Stati partner in che modo le condizioni quadro in materia di perseguimento penale della cibercriminalità possano essere migliorate mediante trattati internazionali. - La Svizzera, insieme a partner stranieri, partecipa a programmi operativi come l'«International Counter Ransomware Initiative». - Si auspicano accordi bilaterali per fornire assistenza reciproca nella lotta alla cibercriminalità. - Viene eventualmente auspicata una collaborazione con il Centro di competenza europeo per la cibersicurezza (ECCC). - Partecipazione attiva alle organizzazioni pertinenti che consentono e promuovono la collaborazione tecnico-operativa, come per esempio FIRST, TF-CSIRT, NatCSIRT (CERT nazionali). - Intensificazione della cooperazione nei gruppi di lavoro internazionali su questioni tecniche (p.es. OT Security, phishing ecc.).
Attori centrali	- Confederazione: *DFAE,* UFT, UFCOM, UFAC, UFE, fedpol, SG-DDPS, NCSC, SIC - Economia/società: associazioni specializzate, CERT, fornitori di servizi di sicurezza

4 Attuazione della strategia

L’attuazione della strategia viene coordinata dal comitato direttivo della CSN, il quale è responsabile della stesura del relativo piano. La pianificazione viene effettuata in consultazione diretta con gli attori centrali delle singole misure. Essi rappresentano gli interlocutori per l’attuazione delle misure in questione e presentano al comitato l’entità e la durata del contributo che possono fornire oltre a informarlo sullo stato di avanzamento delle attività. Qualora non fossero in grado di adottare le misure loro assegnate, sono tenuti a segnalarlo. Il comitato direttivo valuta poi le conseguenze risultanti per gli obiettivi della strategia e informa eventualmente il Consiglio federale e i Cantoni tramite l’NCSC, che assume la funzione di segretariato.
Il finanziamento dei lavori di attuazione viene sostanzialmente effettuato dagli stessi attori centrali. Gli attori della Confederazione utilizzano a questo scopo le risorse loro assegnate per l’attuazione delle prime due strategie. I Cantoni e le organizzazioni dell’economia e della società indicano al comitato direttivo quali contributi all’attuazione delle misure sono in grado di fornire con mezzi propri. L’NCSC sostiene gli attori centrali dell’Amministrazione federale nell’attuazione mettendo a disposizione un pool di esperti, cui gli stessi attori possono richiedere sostegno nell’ambito dell’attuazione della CSN. Gli attori coinvolti sono altresì tenuti a segnalare al comitato direttivo i casi in cui non dispongono di risorse sufficienti o di ulteriori mezzi per attuare una misura.
La verifica dell’attuazione spetta al comitato direttivo. In qualità di segretariato del comitato, l’NCSC rileva e documenta lo stato di attuazione di tutte le misure.
Dopo cinque anni, si provvede alla revisione della strategia stessa e della relativa attuazione. Sulla base dei risultati di tale revisione, il comitato direttivo decide se richiedere ai Cantoni e alla Confederazione una rielaborazione completa della strategia o se apportare singole integrazioni e modifiche per portarla avanti.

5 Elenco delle abbreviazioni

ADS	Amministrazione digitale Svizzera
CCPCS	Conferenza dei comandanti delle polizie cantonali della Svizzera
CDDGP	Conferenza delle direttrici e dei direttori dei dipartimenti cantonali di giustizia e polizia
Cdo Ciber	Comando Ciber
CDPE	Conferenza delle direttrici e dei direttori cantonali della pubblica educazione
CERT	Computer Emergency Response Team
CG Ciber	Concetto generale Ciber
CSIRT	Computer Security Incident Response Team
CSN	Ciberstrategia nazionale
CSSU	Conferenza svizzera delle scuole universitarie
CYD Campus	Cyber Defence Campus di armasuisse (Scienza e Tecnologia)
DDPS	Dipartimento federale della difesa, della protezione della popolazione e dello sport
DFAE	Dipartimento federale degli affari esteri
DFF	Dipartimento federale delle finanze
EUROPOL	Ufficio europeo di polizia
fedpol	Ufficio federale di polizia
IoT	Internet of Things
IT	Tecnologie dell’informazione
LAIn	legge federale sulle attività informative
LM	Legge militare
LSIn	Legge sulla sicurezza delle informazioni
MPC	Ministero pubblico della Confederazione
NCSC	Centro nazionale per la cibersicurezza/National Cyber Security Centre
NEDIK	Rete di supporto alle indagini per la lotta alla criminalità digitale
NTC	Istituto Nazionale di Test per la Cibersicurezza («National Test Institute for Cyber Security»)
OCSE	Organizzazione per la cooperazione e lo sviluppo economico
OEWG	Open Ended Working Group
ONU	Organizzazione delle Nazioni Unite
OSCE	Organizzazione per la sicurezza e la cooperazione in Europa
PMI	Piccole e medie imprese
PSC	Prevenzione Svizzera della Criminalità
RSS	Rete integrata Svizzera per la sicurezza
SATW	Accademia svizzera delle scienze tecniche
SEFRI	Segreteria di Stato per la formazione, la ricerca e l’innovazione
SIC	Servizio delle attività informative della Confederazione
SOC	Centri operativi di sicurezza («Security Operations Center»)
SSCC	Swiss Support Center für Cybersecurity
TDT	Settore Trasformazione digitale e governance delle TIC della Cancelleria federale
TIC	Tecnologie dell’informazione e della comunicazione
TIP	Tecnica e Informatica di Polizia Svizzera
UE	Unione europea
UFAE	Ufficio federale per l’approvvigionamento economico del Paese
UFCOM	Ufficio federale delle comunicazioni
UFG	Ufficio federale di giustizia
UFPP	Ufficio federale della protezione della popolazione

6 Glossario

Ciberattacco	Ciberincidente provocato intenzionalmente.
Cibercriminalità	La criminalità informatica costituisce l'insieme dei reati e delle omissioni punibili commessi nel ciberspazio. Si distingue tra «cibercrime» e «criminalità digitale». Il primo concetto designa reati perpetrati ai danni della rete, dei sistemi o dei dati informatici che rendono necessario l'utilizzo di strumenti tecnici per il lavoro d'indagine svolto dalle autorità di perseguimento penale. Il secondo si riferisce a reati finora commessi prevalentemente al di fuori dell'infrastruttura informatica. A causa della crescente digitalizzazione, i classici tipi di reati vengono commessi sempre più con l'ausilio delle tecnologie informatiche.
Ciberincidente	Evento che, nell'ambito dell'utilizzo di mezzi informatici, compromette la confidenzialità, l'accessibilità o l'integrità delle informazioni e la tracciabilità del loro trattamento.
Ciberminaccia	Qualsiasi circostanza o evento potenzialmente in grado di causare un ciberincidente.
Cibersabotaggio	Attività mirata a ostacolare 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.
Cibersicurezza	Stato auspicabile in cui il trattamento dei dati e in particolare lo scambio di dati tra persone e organizzazioni mediante infrastrutture di informazione e comunicazione funziona come previsto.
Ciberspazio	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.
Ciberspionaggio	Attività compiuta nel ciberspazio a scopi politici, militari o economici per accedere illecitamente a informazioni protette.
Infrastrutture critiche	Processi, sistemi e installazioni essenziali per il funzionamento dell'economia o il benessere della popolazione.
Resilienza	Capacità di un sistema, di un'organizzazione o di una società di resistere a perturbazioni di origine interna o esterna e di mantenere il regolare funzionamento o di ripristinarlo il più rapidamente e completamente possibile.
Sicurezza delle informazioni	La sicurezza delle informazioni è data dalla garanzia dell'autenticità, della confidenzialità, dell'integrità e dell'accessibilità di un sistema TIC e dei dati che vengono elaborati e salvati in questo sistema.