EBP

econcept
Forschung / Beratung / Evaluation

Centro nazionale per la cibersicurezza, NCSC

Verifica dell'efficacia della Strategia nazionale per la protezione della Svizzera contro i cyber-rischi 2018–2022

Rapporto finale
28 marzo 2022

Elaborato da
econcept AG, Gerechtigkeitsgasse 20, 8002 Zurigo
www.econcept.ch / + 41 44 286 75 75

EBP Schweiz AG, Mühlebachstrasse 11, 8032 Zurigo
www.ebp.ch / +41 44 395 16 16

Autori
Benjamin Buser, dr. sc. PF, dipl. geogr., Executive MBA HSG
Jasmin Gisiger, MA ETH UZH in Comparative and International Studies
Christof Egli, ing. dipl. PF Zurigo, CAS Protezione dei dati e sicurezza delle informazioni

Indice

Elenco delle abbreviazioni

Abbreviazione	Significato
CD	Comitato direttivo
CYD	Cyber-Defence Campus
DATEC	Dipartimento federale dell'ambiente, dei trasporti, dell'energia e delle comunicazioni
DDPS	Dipartimento federale della difesa, della protezione della popolazione e dello sport
DFAE	Dipartimento federale degli affari esteri
DFF	Dipartimento federale delle finanze
DFI	Dipartimento federale dell'interno
Governance delle TIC	Governance delle tecnologie dell'informazione e della comunicazione nella Confederazione -> confluita nella Trasformazione digitale e governance delle TIC (TDT) (vedi sotto)
IT	Information technology (tecnologia dell'informazione)
MELANI	Centrale d'annuncio e d'analisi per la sicurezza dell'informazione -> trasformato in Centro nazionale per la cibersicurezza (NCSC) (vedi sotto)
NCSC	Centro nazionale per la cibersicurezza
NEDIK	Rete di supporto digitale alle indagini sulla criminalità informatica
NTC	Istituto nazionale di test per la cibersicurezza
OCiber	Ordinanza sui ciber-rischi
OCSE	Organizzazione per la cooperazione economica e lo sviluppo
ODIC	Organo direzione informatica della Confederazione
PFL	Politecnico federale di Losanna
PFZ	Politecnico federale di Zurigo
PMI	Piccole e medie imprese
RS	Raccolta sistematica della Confederazione
SDVN	Rete di dati sicura
SIC	Servizio delle attività informative della Confederazione
SNPC	Strategia nazionale per la protezione della Svizzera contro i cyber-rischi
SSCC	Swiss Support Center for Cybersecurity
TDT	Trasformazione digitale della Confederazione
UFAE	Ufficio federale per l'approvvigionamento economico del Paese
UFCOM	Ufficio federale delle comunicazioni
UFPP	Ufficio federale della protezione della popolazione

Sintesi

Mandato di verifica dell'efficacia

La trasformazione digitale della Svizzera porta con sé una serie di vantaggi, ma anche dei rischi per lo Stato, la politica, la società e l'economia. Dal 2012 il Consiglio federale affronta le minacce che ne derivano attraverso la Strategia nazionale per la protezione della Svizzera contro i cyber-rischi (SNPC). Nel secondo periodo di attuazione della SNPC (2018–2022) l'Esecutivo ha reagito a un maggior numero di situazioni di minaccia e adottato ulteriori misure rivolte a quattro gruppi di destinatari. Ha quindi fissato sette obiettivi strategici orientati allo sviluppo delle capacità di prevenzione e gestione dei ciberincidenti e alla collaborazione tra gli attori statali, civili e militari. Per l'attuazione sono stati definiti dieci campi d'azione e un relativo piano, che definisce le misure attraverso progetti di attuazione concreti.

Il Consiglio federale ha incaricato il Centro nazionale per la cibersicurezza (NCSC) di verificare l'efficacia della SNPC per poterla ulteriormente sviluppare così come previsto. La verifica dell'efficacia, eseguita esternamente, risponde a quattro domande:

Quadro generale / raggiungimento degli obiettivi: la SNPC 2018–2022 raggiunge gli obiettivi strategici?

Efficienza / risorse: qual è il rapporto tra i mezzi impiegati e le prestazioni fornite?

Efficacia / effetti: in che misura è stato possibile raggiungere gli effetti desiderati?

Ulteriore sviluppo / raccomandazioni: quali raccomandazioni possono essere date in vista della revisione della strategia per il futuro impiego delle risorse?

La verifica dell'efficacia della SNPC si basa su un modello di efficacia che descrive «income», «input», «implementation», «output», «outcome» e «impact».

Adeguatezza e idoneità della SNPC 2018–2022

L'efficacia della SNPC dipende da come viene concepita, dal modo in cui affronta le sfide e dalle misure concrete con cui viene attuata. Le valutazioni relative a come è stata concepita la SNPC mettono in evidenza i livelli di efficacia di income (contesto nazionale e internazionale), input (basi, obiettivi e risorse) e implementation (strutture e processi) e possono essere riassunte in sette punti.

— Per quanto riguarda le **ciberminacce e le sfide** la SNPC si fonda su basi attuali e si concentra sulle sfide centrali e sugli sviluppi per aumentare la cibersicurezza nazionale.

— I contenuti della SNPC tengono debitamente in considerazione le **basi giuridiche e strategiche**. L'armonizzazione della SNPC con altre strategie di digitalizzazione e protezione della Confederazione presenta un potenziale di miglioramento.

— Attraverso le **risorse disponibili** gli organi incaricati dell'attuazione adempiono ai loro compiti principali. Adeguando le modalità con cui i vari organi interessati collaborano tra loro è possibile impiegare i mezzi disponibili in modo più efficiente. Inoltre, sarebbe necessario più personale per l'attuazione della SNPC.

— La rete possiede una struttura adeguata per l'attuazione della SNPC, ma le sue potenziali sinergie devono essere sfruttare ancora meglio. Lo stesso vale anche per i punti di contatto con altre strategie di livello superiore o collegate. In questo senso la **governance** avanzata della SNPC favorisce la **collaborazione**.

— Le basi, le necessità di intervento individuate e le sfide sono state tenute in debita considerazione nella formulazione degli **obiettivi strategici** della SNPC. In alcuni casi viene criticata l'eccessiva focalizzazione sull'Amministrazione federale e il fatto che non venga valutata la possibilità di creare un «ecosistema cyber» in Svizzera.

— Attraverso i **quattro gruppi di destinatari** individuati la SNPC si rivolge a un gruppo molto ampio di attori. Al loro interno, però, non viene data la stessa attenzione a tutti i gruppi di attori.

— **I campi d'azione e le misure** si integrano bene nella strategia. Il piano di attuazione è uno strumento chiave adeguato e i campi d'azione e le misure sono sufficienti a fronteggiare le sfide.

Prestazioni ed effetti dei campi d'azione

La SNPC dovrebbe raggiungere il proprio scopo attraverso le misure e i progetti di attuazione previsti per i dieci campi d'azione. Nella verifica dell'efficacia i campi d'azione e le misure vengono valutati sulla base delle prestazioni fornite (output) e degli effetti perseguiti (outcome). Per quanto riguarda i campi d'azione è stato possibile giungere alle seguenti conclusioni.

— Con la realizzazione di gran parte dei progetti di attuazione del campo d'azione **Acquisizione di competenze e conoscenze** sono state fornite le prestazioni principali, sono state realizzate le strutture auspicate ed è stata creata una rete di conoscenze. Gli outcome sono stati raggiunti e l'impact è stato realizzato in altri campi d'azione.

— Con il loro outcome, i progetti di attuazione realizzati nel campo d'azione **Situazione di minaccia** hanno creato una buona base, a partire dalla quale gli organi responsabili possono raggiungere gli effetti sperati. Valutando la situazione di minaccia dal punto di vista dei contenuti sono auspicabili ulteriori progressi. La situazione di tensione riguardante la disponibilità di esperti rende però difficile uno sviluppo in tal senso.

— Nel campo d'azione **Gestione della resilienza**, le misure volte a migliorare la resilienza delle TIC delle infrastrutture critiche e dell'Amministrazione federale sono state notevolmente sviluppate. L'output è ritenuto elevato, la consapevolezza riguardo al problema è maggiore ma l'effetto sul gruppo di destinatari non è ancora soddisfacente.

— Per quanto riguarda la standardizzazione nel campo d'azione **Standardizzazione / regolamentazione** sono state create delle basi, che fino a questo momento hanno però trovato scarsa applicazione poiché poco diffuse e su base prevalentemente volontaria. I progetti di regolamentazione elaborati creano condizioni quadro che favoriscono la diffusione delle basi. Al momento si ritiene che outcome e impact siano molto limitati. Tuttavia vi sono i presupposti per un aumento dell'efficacia in futuro.

— Nel campo d'azione **Gestione degli incidenti**, le competenze, i processi e le capacità sviluppati nell'ambito della gestione degli incidenti hanno rafforzato la resilienza dei gruppi di destinatari in misura diversa. Non è stato tuttavia rilevato un effetto preventivo.

— Le capacità di reazione e intervento dell'Amministrazione federale sono state aumentate attraverso il campo d'azione **Gestione delle crisi** e, grazie alla regolamentazione delle responsabilità e delle formazioni, è stata garantita la costante capacità di agire da parte delle autorità e dell'Amministrazione. Continua però a essere complesso riuscire a intervenire in modo tempestivo.

— Nel campo d'azione **Perseguimento penale**, attraverso il coordinamento e il rafforzamento della collaborazione a livello intercantonale è possibile aumentare l'efficacia e l'efficienza del perseguimento penale della cibercriminalità. Le differenze tecniche, giuridiche, processuali e di altra natura tra le autorità di perseguimento penale organizzate a livello federale nonché le limitate capacità in termini di personale al momento stanno ostacolando il raggiungimento degli outcome e degli effetti possibili. Le misure per aumentare le capacità sono in fase di attuazione.

— Attraverso i progetti di attuazione realizzati nel campo d'azione **Ciberdifesa** sono state chiaramente rafforzate le capacità dell'esercito e del Servizio delle attività informative della Confederazione (SIC) nonché la loro prontezza operativa nel ciberspazio. La Strategia Ciber DDPS rafforza ulteriormente il campo d'azione attraverso ulteriori misure. Rimane ancora da estendere l'offerta formativa a soggetti terzi. In questo modo sarebbe possibile migliorare l'interoperabilità interna e l'efficacia della Rete integrata Svizzera per la sicurezza (RSS).

— Il campo d'azione **Politica estera e di sicurezza informatica** ha un effetto indiretto sulla protezione dei gruppi di destinatari. Le autorità svizzere e altri attori chiave (p. es. nell'ambito del «Geneva Dialogue») sono stati coinvolti nelle discussioni a livello internazionale sulla cyber governance.

— Una maggiore comunicazione ha permesso di migliorare notevolmente la visibilità. A trarne vantaggio sono stati soprattutto le imprese più grandi e quelle operanti a livello internazionale e i gestori di infrastrutture critiche. La popolazione e le PMI spesso sono raggiunte ancora in modo inadeguato dal campo d'azione **Visibilità e sensibilizzazione**. Occorre intervenire anche sul coordinamento delle attività di comunicazione dei diversi attori. L'impact è indiretto.

Effetti sui gruppi di destinatari

La SNPC intende aumentare la resilienza alle ciberminacce dei quattro gruppi di destinatari, ovvero Amministrazione e autorità, gestori di infrastrutture critiche, popolazione ed economia, per garantire la loro capacità di agire e integrità. Nel rapporto di verifica dell'efficacia si è esaminato in che misura la SNPC abbia gli effetti auspicati su questi gruppi di destinatari.

— L'attuazione della strategia è ben ancorata **all'interno dell'Amministrazione e tra le autorità**. Campi d'azione e misure costituiscono un pacchetto coerente, poiché la struttura della strategia e le misure proposte sono fortemente orientate al modo in cui è organizzata l'Amministrazione. La SNPC permette anche una migliore collaborazione tra la Confederazione e i Cantoni.

— I gestori delle **infrastrutture critiche** conoscono bene i contenuti della strategia e sono fortemente coinvolti nelle misure e nei progetti di attuazione. Nei rami cui appartengono gli attori più grandi si rilevano uno scambio più intenso e un maggiore impegno. Nei settori in cui sono presenti tante imprese diverse di minori dimensioni finora questo fenomeno è stato osservato in maniera meno marcata, e si ha anche una minore consapevolezza del problema. Le prestazioni fornite con l'attuazione della strategia al momento non sono sufficienti per proteggere in modo adeguato tutti i settori in cui sono presenti infrastrutture critiche.

— Negli ultimi anni la **popolazione** è sempre più attenta alla sicurezza nel ciberspazio, tuttavia finora la SNPC non ha portato a una generale sensibilizzazione né garantito una formazione di base della popolazione in ambito informatico. Le misure della SNPC raggiungono la popolazione saltuariamente e non vi è un effetto su larga scala per quanto riguarda la sensibilizzazione in merito alla sicurezza nel ciberspazio.

— All'interno dell'**economia**, le imprese internazionali di grandi dimensioni adottano misure di protezione adeguate contro i ciber-rischi. Le PMI, invece, sono meno consapevoli delle minacce presenti nel ciberspazio e quindi sono meno protette. La SNPC fa fatica a promuovere nelle aziende attività volte a garantire una migliore protezione.

Conclusioni sull'efficacia della SNPC

La SNPC 2018–2022 è una strategia coerente. Il suo piano di attuazione è adeguato agli obiettivi strategici e si sta svolgendo secondo i programmi, portando a outcome rilevanti che, in generale, garantiscono il **raggiungimento degli obiettivi strategici**. Gli outcome, però, non raggiungono tutti i gruppi di destinatari allo stesso modo. Attraverso interventi mirati, come una misurazione degli effetti e una maggiore gestione strategica, i responsabili possono ulteriormente aumentare l'efficacia delle misure di attuazione della SNPC.

Finora le risorse a disposizione hanno permesso ai responsabili dell'attuazione della SNPC di **svolgere i loro compiti principali in modo efficiente**. L'allocazione delle risorse,

tuttavia, potrebbe essere maggiormente orientata agli obiettivi riguardanti l'efficacia. Sarebbe inoltre opportuno mettere a disposizione ulteriori risorse in termini di personale per il restante periodo, fino alla fine del 2022, nonché per le attività continuative.

Finora la SNPC ha mostrato i propri effetti soprattutto sulle infrastrutture critiche, sulle autorità e istituzioni nazionali e cantonali nonché sulle grandi aziende. Sebbene non sia possibile avere delle prove empiriche in quanto la SNPC è ancora in corso, è evidente che questa non raggiunge in misura adeguata le PMI, le città, i Comuni e la popolazione. La protezione informatica di questi gruppi di destinatari è ancora insufficiente.

Prospettive e raccomandazioni

A seguito della verifica dell'efficacia è possibile individuare soluzioni che potrebbero migliorare il modo in cui è strutturata la SNPC, così da incrementare l'efficienza e l'efficacia e ottenere il miglior impact possibile.

— Nella fase di sviluppo della SNPC per le attività successive al 2022 si dovranno sfruttare in modo mirato i vantaggi di un **processo di sviluppo partecipativo**. Attraverso un processo efficiente e gestito in modo rigoroso, i vari titolari delle conoscenze saranno più propensi a collaborare.

— La **governance** della SNPC dovrebbe essere rafforzata riducendo il numero di membri del Comitato direttivo (CD), così da permettergli un maggior controllo strategico. Inoltre dovrebbero essere promosse ulteriori opportunità di interconnessione. Sarebbe opportuno valutare un maggior coinvolgimento delle PMI e delle autorità comunali nella governance della SNPC.

— Gli **obiettivi strategici** dovrebbero essere formulati nel modo più concreto e indipendente possibile a tutti i livelli della strategia, anche nei progetti di attuazione, in modo tale da favorire interventi più mirati e l'accorpamento di attività e risorse per una maggiore efficacia. A tal proposito può essere di aiuto la regola SMART (specifico, misurabile, riconosciuto, realistico, scadenzato).

— Gli **sforzi nell'ambito della comunicazione** devono essere potenziati, integrati e coordinati. Dovrebbe essere presa in considerazione la possibilità di inserire un ulteriore obiettivo strategico «Trasferimento e comunicazione».

— Il modo migliore per far sì che la SNPC sortisca gli effetti sperati è rivolgersi in modo adeguato ai **gruppi di destinatari** e coinvolgerli direttamente nella pianificazione e nell'attuazione delle misure, che dovranno soddisfare nel modo più diretto possibile le loro esigenze. Inoltre, è importante capire se possano essere utili dei «progetti ponte» mirati creati dalla SNPC che coinvolgano tutti e tre i livelli istituzionali, ovvero Confederazione, Cantoni e città/Comuni.

— Il **piano di attuazione** si è rivelato uno strumento fondamentale per avviare rapidamente le attività e perseguire gli obiettivi strategici. Il piano di attuazione dovrebbe essere strutturato e messo in pratica in modo più flessibile e, se necessario,

su cicli di durata maggiore. Inoltre dovrebbe essere posta maggiore attenzione alla misurazione dell'efficacia e al controlling.

— Le **misure** sono di ampia portata e riguardano molte tematiche. Occorre però cercare di organizzarle in base al tipo di misura («misure immediate», «best practice», «progetti di regolamentazione», «progetti trasversali di base» e «progetti pilota»). Inoltre dovrebbero essere trattate esplicitamente tematiche quali «rischi legati alla supply chain», «formazione» ed «ecosistema cyber»», al fine di concentrarsi sulle opportunità. Per favorire la gestione e l'allocazione delle risorse della SNPC secondo principi strategici, in futuro si dovrà inserire la misurazione dell'efficacia nella pianificazione della strategia e delle misure.

— Le **risorse** disponibili finora sono state sufficienti per portare a termine i compiti principali della SNPC. Tuttavia si sono verificate carenze di risorse e si auspica un aumento mirato del personale. Per fare in modo che le risorse vengano impiegate in modo più semplice lì dove vi è un maggior bisogno, è necessario analizzare con occhio critico i processi di pianificazione e di definizione del budget. In particolare, si dovrà verificare se i mezzi o i budget di progetto debbano essere gestiti in modo più diretto dal Comitato ristretto Ciber o dal CDCD, così che le risorse possano essere assegnate in modo più semplice. In ogni caso vi è sicuramente bisogno di un maggior numero di esperti in materia in tutti i gruppi di destinatari e a tutti i livelli. Il pool di esperti deve essere ampliato attraverso programmi mirati di formazione e formazione continua.

1 Mandato di verifica dell'efficacia

1.1 Strategia nazionale per la protezione della Svizzera contro i cyber-rischi 2018–2022 (SNPC 2018–2022)

La protezione nel ciberspazio

La trasformazione digitale della Svizzera porta con sé una serie di vantaggi, ma anche dei rischi per lo Stato, la politica, la società e l'economia. Le tecnologie dell'informazione e della comunicazione e i collegamenti digitali globali sono già oggi ampiamente utilizzati. Di pari passo con la digitalizzazione, però, nel ciberspazio si stanno diffondendo sempre di più anche attività illecite, che minano l'integrità, la riservatezza e la disponibilità di sistemi IT e dati[1]. Quindi per garantire anche in futuro la capacità di agire e l'integrità di soggetti pubblici e privati rispetto alle ciberminacce, è necessario adottare misure mirate per la loro tutela.

Strategia del Consiglio federale

Il Consiglio federale ha deciso di affrontare le minacce che derivano dalla trasformazione digitale attraverso la Strategia nazionale per la protezione della Svizzera contro i cyber-rischi (Consiglio federale, 2018). Nel secondo periodo di attuazione 2018–2022, ancora in corso, il Consiglio federale ha reagito a un maggior numero di situazioni di minaccia e adottato ulteriori misure rispetto al periodo precedente.

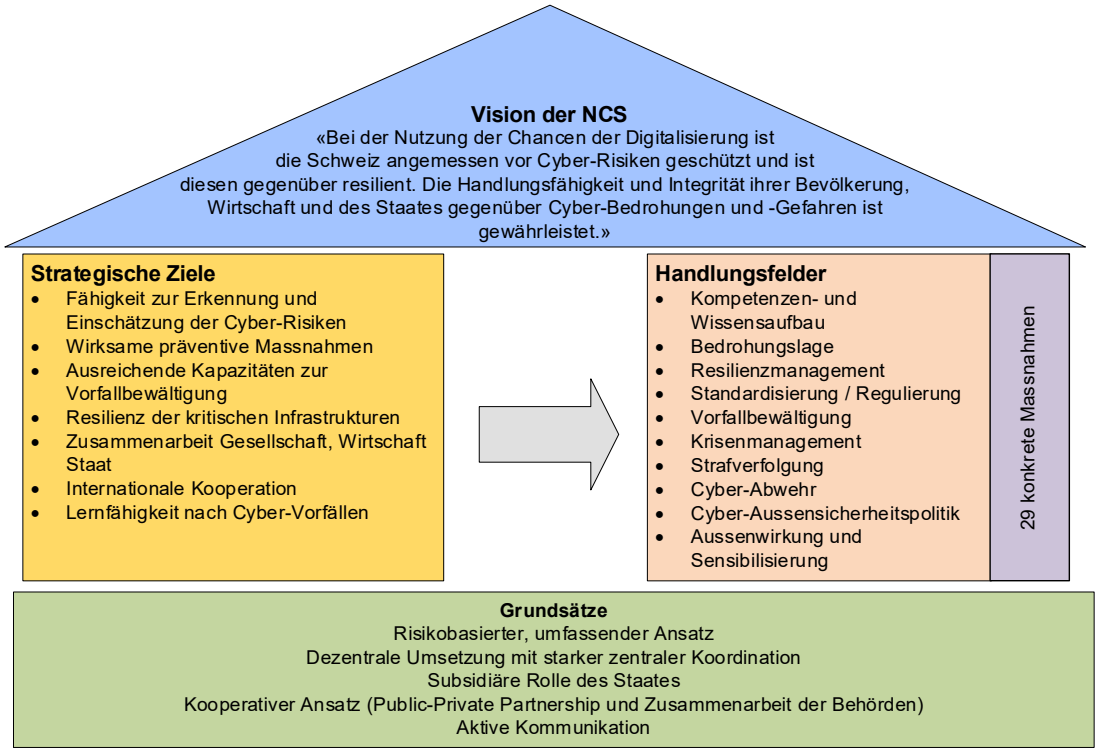
Con la SNPC 2018–2022 la strategia è stata rielaborata tenendo conto delle esperienze maturate e degli obiettivi raggiunti attraverso le misure, ma anche prendendo in considerazione le situazioni di minaccia correnti e attese e gli sviluppi del ciberspazio. Nel processo di elaborazione della strategia, gestito dall'ex Centrale d'annuncio e d'analisi per la sicurezza dell'informazione (MELANI) dell'ODIC, sono state coinvolte circa 50 organizzazioni governative e non governative. La strategia è stata elaborata attraverso un processo in più fasi e approvata e adottata dal Consiglio federale il 18 aprile 2018. Nel decreto del Consiglio federale viene stabilito che annualmente deve essere redatto un rapporto sullo stato di attuazione ed entro fine del 2022 un rapporto di verifica generale della strategia.

La visione della SNPC 2018–2022 è proteggere in maniera adeguata la Svizzera dai cyber-rischi e aumentare la resilienza del Paese nei confronti di questi ultimi. La capacità di agire e l'integrità della popolazione, dell'economia e dello Stato nei confronti delle ciberminacce devono essere sempre garantite. Per questo il Consiglio federale ha fissato sette obiettivi strategici orientati allo sviluppo delle capacità di prevenzione e gestione degli incidenti informatici e alla collaborazione tra gli attori statali, civili e militari (v. Figura 1).

[1] La cosiddetta triade della CIA: «confidentiality», «integrity» e «availability», ovvero riservatezza, integrità e disponibilità

Nell'attuazione della strategia sono coinvolti numerosi uffici federali, i Cantoni e l'economia.

Schema della SNPC 2018–2022



Fonte: Consiglio federale, 2018

Figura 1: struttura e contenuti della SNPC 2018–2022

In un piano di attuazione della strategia vengono definiti dei progetti di attuazione concreti per tutte le misure. Il piano di attuazione è quindi come un piano di lavoro e stabilisce le responsabilità e le tappe fondamentali da raggiungere. Il CD della SNPC può decidere di integrarlo con ulteriori progetti di attuazione, così come è stato fatto diverse volte tra il 2019 e il 2021. All'allegato A-5 è riportata una tavola sinottica dei campi d'azione con le relative misure e i progetti di attuazione previsti.

Gruppi di destinatari

Attraverso le sue misure la SNPC 2018–2022 si rivolge a destinatari diversi, che sono stati suddivisi in quattro gruppi.

Gruppo di destinatari	Descrizione
Infrastrutture critiche	Questo è il principale gruppo di destinatari delle misure, volte a garantire in ogni momento la disponibilità di beni e servizi essenziali.
Autorità	Le autorità della Confederazione, dei Cantoni e dei Comuni sono responsabili di servizi che possono essere equiparati alle infrastrutture critiche per le loro caratteristiche e per l'elevata resilienza richiesta.

Gruppo di destinatari	Descrizione
Popolazione	Lo scopo della SNPC è proteggere la popolazione, direttamente minacciata dalla cibercriminalità. La popolazione dovrebbe poter gestire le TIC in modo sicuro, informatizzato e affidabile.
Economia	La sicurezza in ambito informatico e l'approvvigionamento stabile di beni e servizi sono elementi fondamentali per l'integrità dei processi aziendali. Le aziende svizzere devono quindi poter contare sulle migliori condizioni quadro possibili e livelli di sicurezza elevati.

Tabella 1: gruppi di destinatari della SNPC 2018–2022

In alcuni casi all'interno delle singole misure i gruppi di destinatari sono definiti in modo più puntuale.

Competenze

Dal 2019 il responsabile dell'attuazione della SNPC 2018–2022 è il delegato federale alla cibersicurezza, l'NCSC. Subordinato alla Segreteria generale del DFF, l'NCSC, essendo il centro di competenza della Confederazione per la cibersicurezza, costituisce il servizio centrale di contatto per l'economia, l'amministrazione, gli istituti di formazione e le autorità.

La gestione strategica della SNPC 2018–2022 è affidata al delegato federale alla cibersicurezza e al CD. Quest'ultimo, attraverso i suoi 23 membri, coinvolge in una gestione coerente della SNPC 2018–2022 unità amministrative di tutti i dipartimenti, l'esercito, i Cantoni (attraverso la Conferenza delle direttrici e dei direttori dei dipartimenti cantonali di giustizia e polizia responsabile) nonché i rappresentanti dell'economia e delle scuole universitarie. Il CD si riunisce ogni tre mesi.

La struttura direttiva, nella sua forma attuale, si è costituita nel 2018. In precedenza il responsabile della SNPC era l'ODIC e l'attuazione era affidata a MELANI. Da maggio 2020 l'ordinanza sulla protezione contro i ciber-rischi nell'Amministrazione federale (Ordinanza sui ciber-rischi, OCiber; RS *120.73*) disciplina le competenze.

1.2 Obiettivi e domande a cui risponde la verifica dell'efficacia

Il Consiglio federale ha affidato al DFF l'incarico di esaminare entro la fine del 2022 l'attuale SNPC e, se opportuno, di modificarla. Il CD della SNPC ha deciso di farne valutare l'efficacia a organi esterni. Il rapporto sull'efficacia costituirà il punto di partenza dei successivi lavori. Oltre a valutare l'efficacia della SNPC 2018–2022, quindi, la verifica dell'efficacia fornirà anche suggerimenti su come adeguare e ottimizzare la strategia in occasione della sua revisione e del suo sviluppo.

Il presente rapporto riassume i risultati della verifica dell'efficacia condotta tra luglio 2021 e gennaio 2022, che si è concentrata su quattro domande generali.

Quadro generale / raggiungimento degli obiettivi: in che misura la SNPC 2018–2022 raggiunge gli obiettivi strategici definiti al suo interno? (valutazione sommativa)

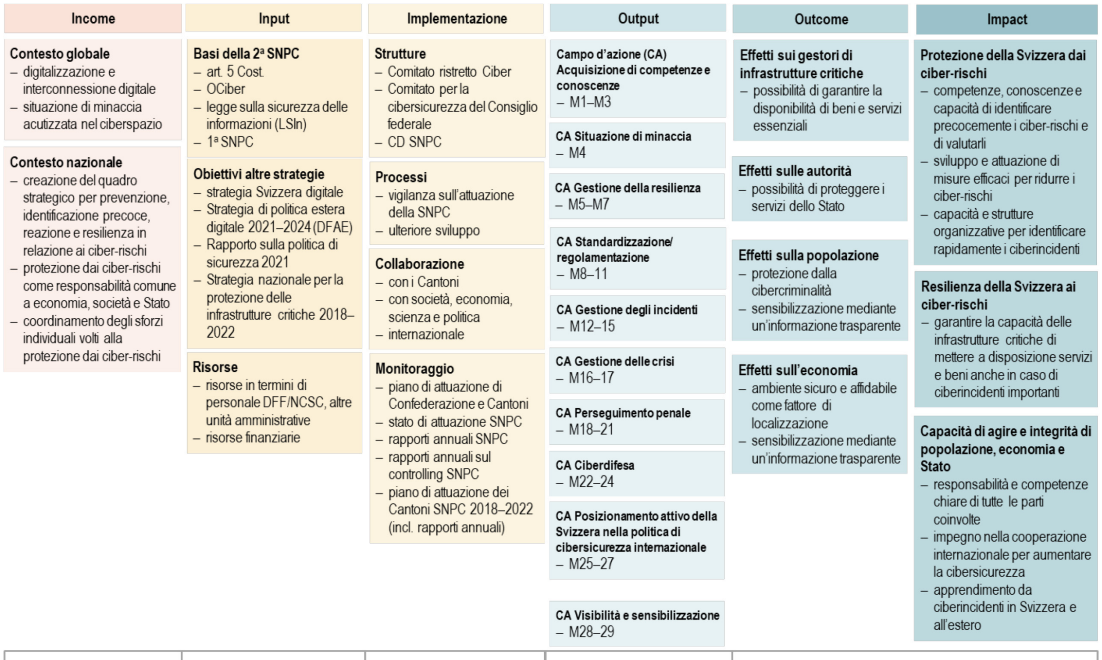
Efficienza / risorse: qual è il rapporto tra l'impiego di mezzi e le prestazioni fornite con l'attuazione della strategia? (valutazione sommativa)

Efficacia / effetti: in che misura è stato possibile raggiungere gli effetti voluti grazie alle prestazioni fornite? (valutazione sommativa)

Ulteriore sviluppo / raccomandazioni: quali suggerimenti possono quindi essere forniti per la revisione della strategia da un lato e per quanto riguarda il futuro impiego delle risorse finanziarie e di personale dall'altro? (valutazione formativa)

Attraverso la SNPC 2018–2022 si è riflettuto sul relativo modello di efficacia, che è stato poi rielaborato. In base alla «Theory of Change» il modello di efficacia può essere rappresentato come in Figura 2 e può costituire un modello di riferimento generale per la verifica dell'efficacia.

Modello di efficacia



econcept ed EBP, 2021

Figura 2: modello di efficacia della SNPC 2018–2022. La verifica dell'efficacia si concentra su «output», «outcome» e «impact».

Di seguito alcune osservazioni che possono servire a spiegare meglio il modello di efficacia.

— *Income*: comprendono il contesto globale e nazionale nel quale è stata sviluppata la SNPC 2018–2022. Sono caratterizzati dalla sempre maggiore interconnessione digitale globale, dalle opportunità e dai rischi connessi nonché dagli sforzi attuati a livello nazionale per fornire protezione in questo ambito.

— *Input*: sono gli obiettivi della SNPC 2018–2022 derivanti dalle basi legali, dalla prima SNPC e dagli obiettivi di altre strategie della Confederazione. Inoltre nell'input rientrano

anche le risorse messe a disposizione dalla Confederazione per fornire le prestazioni previste dalla SNPC 2018–2022.

— *Implementation*: comprende le strutture e i processi di esecuzione adottati dalla Confederazione in collaborazione con altri attori nazionali e internazionali. Include anche il monitoraggio attraverso piani di attuazione e rapporti annuali.

— *Output*: sono le prestazioni fornite da tutti gli attori coinvolti e derivanti dall'esecuzione della SNPC 2018–2022, quindi tutte le attività e i progetti concreti nei campi d'azione definiti nella strategia 2018–2022. Gli «output» sono definiti in modo esaustivo attraverso un totale di 29 misure e 246 tappe fondamentali (v. allegato A-5).

— *Outcome*: la SNPC 2018–2022 ha effetti diretti a breve e medio termine sui propri gruppi di destinatari, come i gestori di infrastrutture critiche, le autorità, la popolazione e l'economia (v. allegato A-5). Oltre agli effetti voluti, possono esserci anche effetti non voluti.

— *Impact*: comprende gli effetti generali a lungo termine della SNPC 2018–2022 e che riguardano l'intera società. Anche a questo livello si avranno sia effetti voluti che non voluti (v. allegato A-5).

Oltre alle quattro domande generali sono state prese in considerazione anche le seguenti questioni più specifiche (Tabella 2).

	Domanda	Livello dell'effetto
1	**Contesto**: in quale misura la SNPC 2018–2022 tiene conto delle sfide rilevanti e degli sviluppi a livello nazionale e globale nonché delle disposizioni legali?	income
2	**Basi**: in quale misura le basi giuridiche, strategiche ed eventualmente di altro tipo sono state integrate negli obiettivi della SNPC 2018–2022?	input
3	**Risorse**: in che misura le risorse impiegate per l'attuazione della SNPC 2018–2022 sono ritenute adeguate?[2]	input
4	**Strutture/processi**: in che misura le strutture e i processi per l'implementazione della SNPC 2018–2022 sono ritenuti efficaci?	implementazione
5	**Campi d'azione**: in che misura i campi d'azione definiti sono adeguati per affrontare le sfide attese in relazione ai ciber-rischi?	output
6	**Misure**: quanto le singole misure e le relative tappe fondamentali sono adeguate a raggiungere gli obiettivi della SNPC 2018–2022? (P. es. sarebbero opportune ulteriori misure? Bisognerebbe estendere determinate misure? Ci sono eventualmente misure che dovrebbero essere eliminate?)	output
7	**Coerenza**: quanto sono coerenti i campi d'azione e le misure della SNPC 2018–2022?	output
8	**Vantaggi**: fino a che punto le misure della SNPC 2018–2022 riescono a raggiungere i gruppi di destinatari rispetto a quanto auspicato? (P. es. i gruppi di destinatari utilizzano le misure o le strutture e i processi consolidati o i prodotti, i servizi, le reti, i metodi elaborati?)	output
9a	**Effetti auspicati sui gruppi di destinatari**: in che misura gli effetti auspicati della SNPC 2018–2022 sui quattro gruppi di destinatari esplicitamente individuati (infrastrutture critiche, autorità, economia, popolazione) sono stati effettivamente raggiunti? (P. es. rispetto alla qualifica degli attori, alla resilienza ecc.)	outcome

[2] L'NCSC prevedeva di effettuare un'indagine quantitativa propria in merito alle risorse impiegate per ciascuna misura nell'autunno 2021.

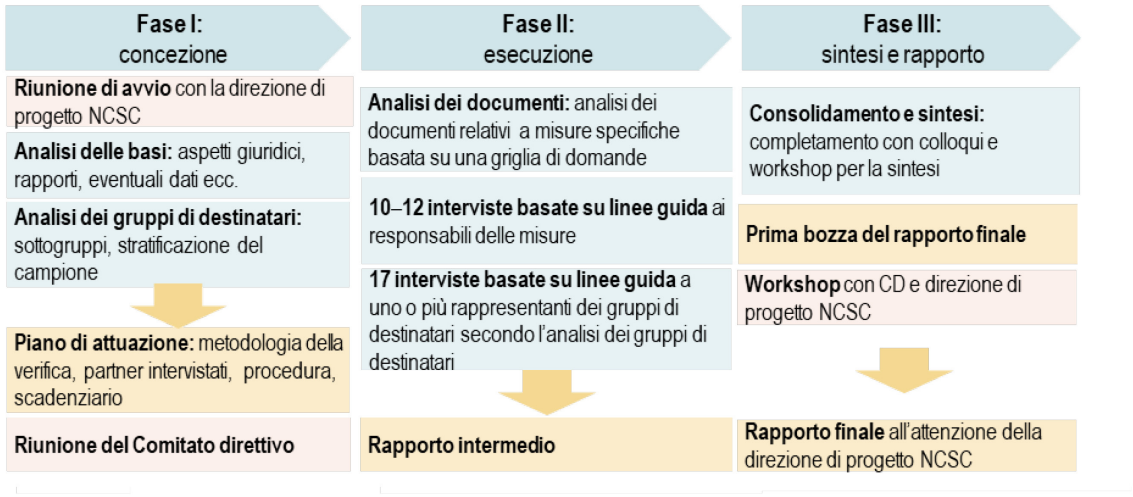
	Domanda	Livello dell'effetto
9b	**Ulteriori effetti sui gruppi di destinatari**: vi sono stati altri effetti non intenzionali sui gruppi di destinatari? Come possono essere classificati?	outcome
9c	**Effetti su altri attori**: in che misura sono stati osservati effetti (non intenzionali) su altri attori e come possono essere classificati?	outcome
10	**Effetti sull'intera società**: in che misura la SNPC 2018–2022 ha permesso di ottenere gli effetti desiderati sulla società nel suo complesso? – Protezione della Svizzera contro i ciber-rischi – Resilienza della Svizzera ai ciber-rischi Salvaguardia della capacità di agire e dell'integrità della popolazione, dell'economia e dello Stato: vi sono stati, oltre a questi, altri effetti non intenzionali? Come possono essere classificati?	impact
11	**Raccomandazioni**: quali suggerimenti possono essere forniti e quali sono i margini di miglioramento che è possibile individuare in relazione... – ...alla futura SNPC 2023–2027? – ...al futuro impiego di risorse finanziarie e di personale?	tutti i livelli del modello di efficacia

Tabella 2: domande specifiche per la verifica dell'efficacia della SNPC 2018–2022

1.3 Procedura e rapporto

Per la verifica dell'efficacia sono stati scelti diversi approcci metodologici: analisi di documenti interni e/o rilevanti per l'attuazione, analisi della letteratura nazionale e internazionale, analisi degli attori e dei gruppi di destinatari coinvolti nonché interviste basate su linee guida definite (v. linee guida all'allegato A-2) e focus group con responsabili e soggetti coinvolti nelle misure previste dalla SNPC 2018–2022 nonché con rappresentanti dei gruppi di destinatari (v. allegati A-3 e **Fehler! Verweisquelle konnte nicht gefunden werden.**). Questo permette di valutare la SNPC 2018–2022 sia da un punto di vista interno che da un punto di vista esterno. La verifica è stata strutturata in tre fasi (v. Figura 3) e il CD della SNPC è stato coinvolto nella fase I e nella fase II.

Articolazione del progetto in tre fasi



econcept ed EBP, 2021

Figura 3: organizzazione del progetto di verifica dell'efficacia inclusi metodi, interazione con l'NCSC e calendario. La fase I si conclude con l'approvazione del piano di attuazione.

Ulteriori dettagli sulla procedura sono riportati all'allegato A-1. I dati sono stati elaborati tra luglio 2021 e gennaio 2022. Il presente rapporto riassume i risultati della verifica dell'efficacia come riportato di seguito.

— Al punto 2 viene fornita una valutazione generale della SNPC 2018–2022 e chiarito se e in che misura la SNPC 2018–2022 possa essere considerata adeguata e idonea a incrementare la protezione della Svizzera dai ciber-rischi.

— Al punto 3 si analizza quali prestazioni sono state fornite finora nei dieci campi d'azione e quali effetti, nel senso di outcome, si sono riscontrati.

— Il punto 4 si concentra sui quattro gruppi di destinatari per chiarire se e in che modo è aumentata la loro integrità e capacità di agire rispetto alle ciberminacce.

— Al punto 5 viene riportata una valutazione generale dell'efficacia, effettuata rispondendo alle domande di carattere generale della ricerca il cui scopo è una valutazione sommativa (v. punto 1.2).

— Infine, in vista del futuro aggiornamento della SNPC, al punto 6 vengono riportati alcuni suggerimenti che potrebbero essere utili per aumentare l'efficacia della strategia (v. anche la quarta domanda generale al punto 1.2).

La presente valutazione dell'efficacia riflette il giudizio che gli autori si sono costruiti sulla base di una procedura sistematica, multimetodica e multiprospettiva. In questa occasione, inoltre, gli autori desiderano ringraziare tutte le persone coinvolte per la disponibilità e la collaborazione.

2 Adeguatezza e idoneità della SNPC 2018–2022

L'efficacia della SNPC 2018–2022 dipende dal modo in cui viene concepita e dal suo orientamento rispetto alle relative sfide, ma è anche il modo in cui viene attuata a determinarne l'efficacia. Di seguito vengono riportate le valutazioni in merito alla concezione della SNPC 2018–2022. L'analisi si concentra sull'efficacia di income (contesto nazionale e internazionale), input (basi, obiettivi e risorse) e implementation (strutture e processi). I campi d'azione, come output della SNPC, vengono valutati rispetto alla loro adeguatezza per il raggiungimento degli obiettivi. L'efficacia dei campi d'azione viene poi valutata al punto 3.

Di seguito vengono riportate le domande specifiche a cui si è cercato di dare una risposta attraverso la valutazione effettuata sulla base dei documenti analizzati e delle interviste ai responsabili delle misure e i rappresentanti dei gruppi di destinatari.

2.1 Ciberminacce e sfide

Contesto: in quale misura la SNPC 2018–2022 tiene conto delle sfide rilevanti e degli sviluppi a livello nazionale e globale nonché delle disposizioni legali?

L'attuale strategia si occupa innanzitutto delle minacce a livello centrale e dei ciber-rischi per la Svizzera e identifica le sfide che mettono a rischio la resilienza del Paese. Viene quindi fatta una distinzione tra atti illeciti intenzionali (i cosiddetti ciberattacchi, nei quali rientrano la cibercriminalità, il ciberspionaggio, il cibersabotaggio e il terrorismo informatico, la disinformazione e la propaganda e i ciberconflitti) e incidenti provocati da azioni non intenzionali, come errori umani (p. es. truffa con carte di credito) e guasti tecnici.

Sulla base delle situazioni di minaccia individuate e delle esperienze maturate con la SNPC 2013–2017, è stato avviato uno sviluppo strategico in cinque ambiti. La strategia rivista si concentra quindi sulla protezione contro le minacce e su un'infrastruttura resiliente, in grado di mantenere la propria capacità di agire. Per raggiungere questi obiettivi sono però necessari una maggiore gestione strategica e un ulteriore pacchetto di misure, maggiori capacità e conoscenze, un sostegno maggiore dato dal coinvolgimento di una platea di destinatari più ampia e un rafforzamento della collaborazione. In particolare viene data notevole importanza al rafforzamento delle strutture organizzative.

Secondo gli intervistati sono stati tratti i giusti insegnamenti dalla prima strategia e con la SNPC 2018–2022 sono state create condizioni quadro adeguate per poter affrontare le ciberminacce. Il contesto strategico, che comprende il Rapporto sulla politica di sicurezza 2016, la strategia Svizzera digitale del Consiglio federale e la Strategia nazionale per la protezione delle infrastrutture critiche, ha permesso di comprendere la necessità di intervenire. Gli intervistati si sono detti soddisfatti soprattutto dell'estensione ad altri gruppi di destinatari e del rafforzamento della collaborazione.

Uno studio del PFZ (CSS, 2019) che mette a confronto la SNPC 2013–2017 e la SNPC 2018–2022 con altre strategie nazionali per la cibersicurezza adottate in altri Paesi conferma quanto detto in precedenza. Finora la SNPC ha affrontato otto sfide generali che si possono ritrovare anche in diverse analisi sulle situazioni iniziali e sulle strategie di altri Paesi.

Conclusione: la SNPC 2018–2022 si fonda su basi attuali e si concentra sulle sfide centrali e sugli sviluppi volti ad aumentare la cibersicurezza nazionale.

2.2 Contesto istituzionale della strategia

Basi: in quale misura le basi giuridiche, strategiche ed eventualmente di altra natura sono state integrate negli obiettivi della SNPC 2018–2022?

La SNPC 2018–2022 si basa sui lavori preparatori e sulle conoscenze acquisite in precedenza attraverso la SNPC 2012–2017. Nell'elaborazione della strategia per gli anni 2018–2022 sono stati riuniti in modo adeguato ed esaustivo da un lato le basi esistenti e le esperienze maturate e dall'altro i risultati di recenti studi e le valutazioni degli attori coinvolti fornite dalle persone intervistate. Stando al giudizio generale, le sfide individuate corrispondono a quelle attuali (v. punto 2.1). Sono state prese in considerazione le precedenti condizioni quadro legali e sono stati anticipati anche i processi attualmente in corso, come l'OCiber e la legge federale del 18 dicembre 2020 sulla sicurezza delle informazioni in seno alla Confederazione (Legge sulla sicurezza delle informazioni, LSIn; RS *128*).

Oltre alla SNPC esiste anche la strategia Svizzera digitale[3], di cui dal 2021 è responsabile il delegato del Consiglio federale per la trasformazione digitale e la governance delle TIC all'interno della Cancelleria federale (ruolo rivestito in precedenza dall'UFCOM). Il DFAE dispone della Strategia di politica estera digitale 2021–2024[4], mentre il DDPS della Strategia Ciber DDPS[5]. Per quanto riguarda i contenuti, le tre strategie sono in gran parte coerenti e connesse tra loro. Ad esempio, il campo d'azione relativo alla politica estera di sicurezza informatica della SNPC propone un'integrazione tra la politica estera e quella interna in ambito informatico. Le persone intervistate hanno sottolineato come l'armonizzazione tra le diverse strategie e la SNPC 2018–2022 presenti potenziali di miglioramento. I comitati preposti alla gestione strategica delle strategie, tuttavia, non sono sufficientemente interconnessi.

Conclusione: all'interno della SNPC 2018–2022 le basi giuridiche e strategiche sono adeguatamente prese in considerazione. Tuttavia vi sono delle incongruenze a livello istituzionale.

---

3 https://www.bakom.admin.ch/bakom/it/pagina-iniziale/digitale-e-internet/strategia-svizzera-digitale/digitale-schweiz.html, consultato il 7 gennaio 2022.

4 https://www.eda.admin.ch/dam/eda/it/documents/publications/SchweizerischeAussenpolitik/20201104-strategie-digitalaussenpolitik_IT.pdf, consultato il 7 gennaio 2022.

5 La Strategia Ciber DDPS – in sintesi (admin.ch), consultato il 22 gennaio 2022.

2.3 Risorse

Risorse: in che misura le risorse impiegate per l'attuazione della SNPC 2018–2022 sono ritenute adeguate?

Nel 2019 il PFZ ha condotto uno studio comparativo a livello internazionale da cui, riassumendo, è emerso che in altre nazioni gli attori politici sono disposti a mettere a disposizione ampie risorse per garantire la cibersicurezza nazionale adottando un approccio strategico (CSS, 2019). A confronto, le uscite della Svizzera in questo settore sarebbero piuttosto basse.

Dal 2018 le risorse in termini di personale a disposizione della SNPC sono state più volte aumentate. Nell'autunno 2021 l'NCSC ha condotto un'indagine per rilevare le risorse e il fabbisogno corrente nel 2021 degli uffici coinvolti nella SNPC (NCSC, 2021c). Dall'indagine è emerso che la maggior parte degli uffici avrebbe bisogno di maggiori risorse in termini di personale per le attività collegate all'attuazione delle misure della SNPC 2018–2022.

Nell'ambito della verifica dell'efficacia, le persone responsabili dell'attuazione delle misure hanno precisato che finora le risorse di personale disponibili hanno permesso di portare a termine gli elementi centrali e i compiti principali previsti dalle 29 misure. Di seguito elenchiamo i motivi per cui viene chiesto un maggiore impiego di personale.

- *Doppi incarichi*: numerosi progetti sono gestiti da persone che contemporaneamente devono svolgere anche ruoli dirigenziali nella loro organizzazione. Questo porta a una concorrenza delle risorse e a doppi incarichi che, in molti casi, sono percepiti come un peso. Se venissero messe a disposizione ulteriori risorse, invece, queste potrebbero svolgere le mansioni correnti assegnate a funzioni dirigenziali.
- *Posti vacanti*: diverse unità amministrative lamentano posti vacanti, questo a causa dei ritardi con cui le direzioni degli uffici prendono le decisioni e delle difficoltà nel trovare persone con le competenze necessarie per rivestire le posizioni corrispondenti.
- *Necessità di formazione continua*: l'elevato dinamismo con cui si evolve il ciberspazio richiede un'intensa attività di formazione continua, che però, a sua volta, riduce il numero di persone operative. Aumentando le risorse, quindi, si potrebbe garantire una continua capacità di intervento e, contemporaneamente, anche un'elevata attività di formazione continua.
- *Aumento dei compiti*: la SNPC 2018–2022 comprende misure volte allo sviluppo delle attività operative (p. es. panoramica dei casi). L'aumento dei ciberattacchi ha portato a una costante crescita dei casi operativi da gestire e quindi si sono rese necessarie risorse aggiuntive. Per le misure con una forte componente operativa sarebbe opportuna una stabilizzazione di queste risorse, perché saranno necessarie per un lungo periodo.

Diversi dei partner intervistati ritengono che con le risorse disponibili si sarebbero potuti ottenere risultati migliori per quanto riguarda la governance e i processi di attuazione. La SNPC ha promosso un forte orientamento agli obiettivi e all'efficacia della strategia stessa, senza analizzare sempre in modo critico l'allocazione delle risorse. Allo stesso modo, si

sarebbero potute ripartire maggiormente le risorse, in particolare tra tre settori, ovvero il perseguimento penale in ambito informatico, la cibersicurezza e la ciberdifesa. A tal proposito diversi attori suggeriscono da tempo la costituzione di un pool di esperti comune con un numero sufficiente di persone dedicate che possa influenzare fortemente la collaborazione trasversale tra i vari ambiti. Non bisogna tuttavia dimenticare di garantire sempre il rispetto dei principi dello Stato di diritto e delle relative basi legali che stabiliscono limiti precisi tra i vari settori.

Conclusione: con le risorse finora disponibili è stato possibile svolgere le attività principali necessarie per l'attuazione delle misure della SNPC 2018–2022. Tuttavia questi mezzi potrebbero essere impiegati in modo più efficiente intensificando e/o adeguando la collaborazione tra tutti i settori (p. es. attraverso la costituzione di un pool di esperti). Inoltre è stata rilevata un'effettiva necessità di incrementare il personale da dedicare all'attuazione della SNPC.

2.4 Governance e collaborazione

Strutture/processi: in che misura le strutture e i processi per l'implementazione della SNPC 2018–2022 sono ritenuti efficaci?

L'attuazione della SNPC si basa su un approccio decentralizzato, quindi vari uffici federali coinvolti nella SNPC realizzano direttamente i progetti di attuazione loro assegnati (v. Consiglio federale, 2018). L'NCSC si occupa del coordinamento tra i vari uffici federali e si assume anche in prima persona la responsabilità dei progetti di attuazione. In base a quanto stabilito dalla SNPC, questo approccio decentralizzato di gestione e attuazione deve essere inteso come una rete. Questa struttura è caratterizzata da un organo di coordinamento comune e pochi accordi formali sia tra gli ambiti «ciberdifesa», «cibersicurezza» e «perseguimento penale della cibercriminalità» che tra i diversi campi d'azione.

Secondo gli intervistati questa rete è in genere funzionale. Da un lato, dal momento dell'introduzione della SNPC 2018–2022 ha consentito un rapido avvio delle attività e l'integrazione di competenze pregresse attraverso le strutture già esistenti, dall'altro garantisce costantemente un'elevata agilità e capacità di reazione e consente quindi di integrare man mano altri attori in modo rapido e senza disuguaglianze. La collaborazione all'interno della rete è ritenuta efficiente, orientata alle soluzioni e basata sulla fiducia, sia a livello operativo, per l'attuazione delle misure, sia a livello di gestione strategica. Tutto questo è favorito dalle condizioni quadro date e dall'orientamento fornito a livello di contenuti dalla SNPC. Tali affermazioni sono basate sulle dichiarazioni di alcuni intervistati secondo i quali il processo di sviluppo della SNPC 2018–2022 ha richiesto molto lavoro in quanto era stata lasciata molta libertà a livello contenutistico e le persone coinvolte erano molte.

Le potenziali sinergie della rete a livello di contenuto, però, non vengono sfruttate completamente. Stando alle dichiarazioni la causa sarebbe il fatto che la rete coinvolge

sostanzialmente solo i tre ambiti generali «ciberdifesa», «cibersicurezza» e «perseguimento penale della cibercriminalità» dell'Amministrazione federale. Non c'è un'integrazione laterale diffusa, che va oltre questi tre settori e coinvolge tutti i campi d'azione. Un esempio di questo mancato sfruttamento delle possibili sinergie è il mancato coordinamento integrale delle analisi dei pericoli, delle misure di resilienza e dei percorsi formativi tra i reparti «Defence» e «Security» nonché tra le autorità civili e gli elementi militari. Alcuni attori, però, fanno notare che in base alle riserve dello Stato di diritto e ai sensi di leggi specifiche non è permessa una completa armonizzazione tra «Defence» e «Security». Per esempio, non è consentito lo scambio di informazioni sulle vulnerabilità individuate. Al contrario sarebbe auspicabile uno sviluppo comune delle competenze. Ne è un esempio il percorso di formazione per diventare Cyber Security Specialist (CSS) con attestato professionale federale (APF), che rappresenta una nuova offerta importante sia per l'esercito che per le organizzazioni civili.

Per creare una rete ancora più forte tra tutti i settori, oltre a un CD mancano anche le opportunità per favorire lo scambio e il dialogo diretto con altri attori.

Con l'istituzione del ruolo di delegato federale alla cibersicurezza e la costituzione del Centro nazionale per la cibersicurezza NCSC, la governance della SNPC 2018–2022 è stata ulteriormente istituzionalizzata. Queste misure legate alla governance e la collaborazione con il personale dell'NCSC sono in generale ritenute positive.

La SNPC 2018–2022 ha gettato le basi per il consolidamento di varie attività del Centro nazionale per la cibersicurezza. Allo stesso tempo, l'NCSC ha avuto un effetto positivo sulla strategia rafforzando la gestione strategica e aumentando la capacità di reazione. Il Centro, con le sue pubblicazioni periodiche, e il delegato, stando a quando dichiarato dalla maggior parte delle persone intervistate responsabili delle misure, hanno dato visibilità e reso riconoscibile la SNPC. Questo è evidente dalla maggiore copertura mediatica dei ciber-rischi e dal fatto che viene fatto riferimento al delegato e agli organi della Confederazione (incluso l'NCSC). Capacità tecniche e strategiche, abbinate a una personalità in grado di mediare, sono spesso indicate dagli intervistati come caratteristiche essenziali del delegato federale alla cibersicurezza.

Alcuni intervistati hanno giudicato poco efficiente ed efficace dal punto di vista della governance e dei processi il collegamento tra la SNPC e le altre strategie digitali, informatiche e di protezione interne all'Amministrazione federale. A loro avviso, da un lato non tutte le unità amministrative coinvolte di livello strategico superiore sarebbero state inserite nel Comitato ristretto Ciber, dall'altro la governance della SNPC non prende sufficientemente in considerazione le attività operative che coinvolgono tutte le unità amministrative interessate.

Conclusione: la struttura a rete viene ritenuta vantaggiosa per l'attuazione della SNPC 2018–2022. Tuttavia, nell'attuazione operativa questi vantaggi non si sono pienamente realizzati, anche se il lavoro di ulteriore sviluppo della governance della SNPC avviato nel 2018 viene considerato adeguato in quest'ottica. Per quanto riguarda invece l'integrazione

a livello strutturale e processuale con strategie collegate e di livello superiore, si ritiene che vi sia margine per un miglioramento.

2.5 Definizione degli obiettivi strategici

Basi: in quale misura le basi giuridiche, strategiche ed eventualmente di altro tipo sono state integrate negli obiettivi della SNPC 2018–2022?

I partner intervistati ritengono che il processo di revisione abbia contribuito notevolmente a mettere fin da subito i titolari delle conoscenze coinvolti in contatto tra di loro e rafforzato la collaborazione. L'impegno profuso da tutte le parti è stato molto apprezzato. Questo coinvolgimento tempestivo degli stakeholder nello sviluppo della strategia è uno dei suggerimenti forniti dalla European Union Agency for Network and Information Security nelle sue linee guida (ENISA, 2016). Gli obiettivi della strategia individuati, dal punto di vista di allora, sono corretti. Si basano sulle conoscenze rilevanti di tutte le parti coinvolte e sono il risultato di un accordo, quindi in pratica ognuna delle parti in questo modo ha dato anche il proprio consenso a impegnarsi per raggiungere tali obiettivi.

Secondo gli interlocutori i sette obiettivi strategici generali e i principi operativi stabiliscono in modo sufficientemente preciso cosa è necessario fare per realizzare la visione della SNPC e quindi garantire una protezione adeguata della Svizzera contro i ciber-rischi e assicurare che popolazione, economia e Stato mantengano la capacità di agire e l'integrità quando devono affrontare le ciberminacce. È stata apprezzata anche la ripartizione tra sicurezza, perseguimento penale e difesa, ritenuta utile dagli intervistati. Dall'indagine è emerso inoltre che a favorire l'accettazione degli obiettivi è stato anche il coinvolgimento di numerosi attori, tra cui i Cantoni e altre istituzioni. Alcuni dei partner intervistati, però, hanno criticato questo approccio federale o decentralizzato, perché a loro avviso in questo modo si farà più fatica a vedere rapidamente degli effetti nel quotidiano.

In diversi hanno osservato che, così come in passato, la strategia è ancora fortemente incentrata sulla Confederazione e sull'Amministrazione federale. Secondo gli intervistati, al momento della stesura del piano di attuazione a livello cantonale potevano essere stabilite anche altre priorità. In futuro, quindi, dovrebbero poter essere prese maggiormente in considerazione le questioni dei Cantoni.

In particolare è stato fatto notare che le possibilità della digitalizzazione teorizzate nella visione della strategia non trovano riscontro negli obiettivi strategici definiti. Non sono infatti state stabilite misure specifiche in tal senso. Gli obiettivi strategici si concentrano soltanto sul modo di affrontare i ciber-rischi. Alcuni si sono però contrapposti a questa opinione ribadendo in modo deciso come l'obiettivo principale della SNPC sia la tutela e la protezione dai rischi. A loro avviso le possibilità derivanti da una maggiore protezione della Svizzera dal punto di vista informatico e dalla maggiore capacità di agire e integrità rispetto alle ciberminacce dovrebbero essere sfruttate altrove, ad esempio nella strategia Svizzera digitale del Consiglio federale (Confederazione Svizzera, 2020a).

Conclusione: le basi, la necessità di intervento riconosciuta e le sfide sono state inserite adeguatamente negli obiettivi della SNPC 2018–2022. Alcuni hanno criticato il forte orientamento all'Amministrazione federale e la mancata attenzione alle possibili opportunità.

2.6 Gruppi di destinatari

Basi: in quale misura le basi giuridiche, strategiche ed eventualmente di altro tipo sono state integrate negli obiettivi della SNPC 2018–2022?

Vantaggi: fino a che punto le misure della SNPC riescono a raggiungere i gruppi di destinatari rispetto a quanto auspicato?

L'orientamento ai gruppi di destinatari rappresenta un punto di partenza importante per una strutturazione efficace della SNPC 2018–2022 (v. anche modello di efficacia «outcome», punto 1.2). La SNPC 2018–2022, classificando i destinatari in infrastrutture critiche, autorità, popolazione ed economia, ha definito quattro gruppi molto ampi. Questa aggregazione, con la possibilità di suddividere ulteriormente i gruppi durante l'attuazione delle misure, è stata giudicata in generale adeguata dai responsabili delle misure. Il vero problema della SNPC 2018–2022 è piuttosto il fatto che le sue misure non si rivolgono a tutti e quattro i gruppi di destinatari allo stesso modo e quindi non tutti i gruppi di destinatari sono raggiunti nella misura auspicata.

Queste differenze vengono ricondotte, tra le altre cose, alla mancanza di basi giuridiche. Per questo la Confederazione deve proteggere innanzitutto se stessa dai ciber-rischi[6]. Le misure per la protezione delle infrastrutture critiche previste dalla SNPC si basano sulle attuali basi legali delle parti coinvolte (p. es. SIC, UFPP, UFAE, UFCOM). Inoltre, durante l'attuazione della SNPC il Parlamento ha anche approvato la LSIn, che assegna esplicitamente alla Confederazione l'incarico di supportare i gestori delle infrastrutture critiche per garantire la sicurezza informatica.

Per le attività volte a proteggere la popolazione o, ad esempio, le PMI non esistono basi legali sufficienti.

L'elevata attenzione rivolta alle infrastrutture critiche in generale è ritenuta corretta tenuto conto degli obiettivi di efficacia della SNPC. Le difficoltà emergono nel momento in cui è necessario stabilire nel concreto quali soggetti rientrano in questo gruppo di destinatari. Secondo gli intervistati il problema è dato dal fatto che vi è poca consapevolezza dei rischi legati alla catena di fornitura di componenti fondamentali o di servizi per le infrastrutture critiche e tale problematica non è affrontata in modo coerente nella SNPC. La stessa cosa vale anche a livello comunale per la gestione delle infrastrutture da parte di città e Comuni.

Inizialmente un'ulteriore incertezza nell'ambito della SNPC era data dal fatto che l'Ufficio federale della protezione della popolazione (UFPP), l'Ufficio federale per

6 OCiber

l'approvvigionamento economico del Paese (UFAE) e altri uffici specializzati del settore avevano idee diverse su come dovevano essere considerate le infrastrutture critiche e quindi ognuno stabiliva requisiti diversi. Quando poi la responsabilità del coordinamento delle attività di gestione della resilienza è stata interamente trasferita all'UFPP, sono stati garantiti anche un'analisi unica e un quadro consolidato delle minacce. All'UFAE, invece, è stata affidata interamente la responsabilità di elaborare gli standard minimi per la protezione delle infrastrutture critiche. Alcuni degli intervistati hanno dichiarato che sarebbe tuttora utile stabilire in modo definitivo cosa si intende per infrastrutture critiche, in modo da poter poi applicare tale definizione in tutta l'Amministrazione federale.

Per quanto riguarda il gruppo di destinatari delle autorità, 'sia le persone responsabili delle misure che i rappresentanti dei gruppi di destinatari hanno fatto presente che al momento dell'entrata in vigore, la SNPC 2018–2022 non si rivolgeva in modo adeguato ai Comuni. Attraverso il progetto di attuazione messo in atto successivamente per la creazione di un marchio di qualità per la sicurezza informatica dei Comuni e delle PMI (Cyber-Safe) si è cercato di colmare questa lacuna. La collaborazione tra Confederazione e Comuni non è sufficientemente sancita dall'attuale principio di sussidiarietà, per questo sia all'interno della Confederazione che dei Comuni non viene svolto un grande lavoro di sensibilizzazione sulle possibili opportunità e collaborazioni. Attraverso la SNPC 2018–2022, invece, è stata fortemente intensificata la collaborazione con i Cantoni, i quali però non sono in grado di creare una rete capillare con i Comuni.

In vari casi è stato sottolineato come la SNPC all'interno della Confederazione non coinvolga allo stesso modo tutti gli attori principali. Ad esempio, alcuni importanti uffici del DATEC non sono presi adeguatamente in considerazione. L'UFAC, l'UFT, l'USTRA e l'UFE sono responsabili delle rispettive infrastrutture critiche, ma non fanno parte degli organismi della SNPC. Per svolgere i compiti loro affidati nell'ambito della SNPC, questi uffici in alcuni casi hanno dato vita a organi autonomi aggiuntivi appositamente istituiti per assolvere a questi compiti.

La maggior parte degli intervistati ritiene poi che la comunicazione rivolta al gruppo di destinatari «economia» non sia stata equilibrata. Il settore dell'economia può infatti essere suddiviso in sottogruppi, che si differenziano per le strutture e le sfide che devono affrontare, l'attuale standard di protezione dai ciber-rischi e i regolamenti a cui sono sottoposti:

- *Gestori di infrastrutture critiche*: la SNPC 2018–2022 li considera un gruppo di destinatari a parte, anche se le aziende che vi rientrano presentano differenze sostanziali in termini di dimensioni e portata delle attività svolte.
- *Imprese operanti a livello internazionale*: le imprese che operano a livello internazionale spesso investono notevoli risorse per garantire l'integrità dei processi aziendali e la conformità alle disposizioni di legge nazionali in materia di sicurezza e protezione dei dati. Lo stesso vale anche per le imprese internazionali che operano in Svizzera attraverso filiali. Le imprese operanti a livello internazionale si occupano da sole della loro sicurezza a livello informatico e solo un numero limitato di queste aziende entra

regolarmente in contatto con la SNPC. Negli ultimi anni, quindi, l'NCSC ha ampliato la sua cerchia ristretta di clienti e coinvolto sempre di più le PMI.

– *Piccole e medie imprese*: sia i responsabili dell'attuazione delle misure sia i rappresentanti del mondo economico ritengono che le tante PMI costituiscano una falla della sicurezza informatica. Il problema in questo caso è principalmente di «awareness», anche perché questo gruppo di destinatari non è preso sufficientemente in considerazione nella SNPC 2018–2022.

Molti attori ritengono che la popolazione sia l'anello più debole nella catena di efficacia per la protezione contro i ciber-rischi. In più nella SNPC 2018–2022 la popolazione è il gruppo di destinatari al quale ci si rivolge meno in modo diretto. Gli intervistati hanno espresso opinioni diverse in merito all'importanza della popolazione, a seconda che il focus fosse sulla riduzione dei ciber-rischi e dei danni alle economie domestiche private o sulla popolazione attiva, che dovrebbe essere un minimo sensibilizzata e possedere delle conoscenze di base sulla sicurezza informatica ai fini della propria attività lavorativa.

Conclusione: attraverso i quattro gruppi di destinatari individuati la SNPC 2018–2022 si rivolge a un gruppo molto ampio di attori. Questi gruppi, però, non sono presi in considerazione tutti allo stesso modo e per diversi sottosegmenti dei vari gruppi di destinatari si rileva anche una mancanza di misure concrete a loro destinate.

2.7 Campi d'azione e misure nella struttura della strategia

Coerenza: quanto sono coerenti i campi d'azione e le misure della SNPC 2018–2022?

Per poter raggiungere gli obiettivi strategici, la SNPC 2018–2022 stabilisce dieci campi d'azione che riguardano diversi aspetti dei ciber-rischi e all'interno dei quali definisce in totale 29 misure.

Tutti gli interlocutori giudicano la struttura della SNPC 2018–2022 appropriata e coerente. La portata, la struttura e il livello di approfondimento sono ritenuti idonei e consentirebbero di ottenere rapidamente una panoramica adeguata sulle modalità con cui la Svizzera intende far fronte ai ciber-rischi.

Gli orientamenti dei singoli campi d'azione sono ritenuti funzionali al raggiungimento dei sette obiettivi strategici. Considerato il livello di maturità attuale della Svizzera per quanto riguarda i ciber-rischi, si ritiene corretto che la SNPC 2018–2022 copra uno spettro così ampio di aspetti attraverso dieci campi d'azione. Questo crea i presupposti per coinvolgere molti più gruppi di destinatari e tenere conto di più sfide, ma vi è anche il rischio di una dispersione delle risorse. Molti degli intervistati ritengono quindi che quando il livello di maturità aumenterà sarebbe opportuno valutare la possibilità di concentrarsi maggiormente su singoli aspetti. All'interno della SNPC 2018–2022 i campi d'azione servono soprattutto a strutturare il modo di procedere. Per i partner intervistati il piano di attuazione della strategia è uno strumento chiave in quanto si ricollega ai campi d'azione della strategia. Inoltre, rispecchia le tante sfaccettature dell'Amministrazione e dei gruppi

di destinatari coinvolti, il che gli conferisce un maggior carattere organizzativo. La suddivisione gerarchica in campo d'azione --> misura --> progetto d'attuazione viene inoltre percepita come troppo complessa e rigida. Secondo alcuni dei partner intervistati questa struttura non permette dei collegamenti trasversali a livello di contenuti e non consente di sfruttare potenziali sinergie. Inoltre è stato fatto notare come i campi d'azione e le misure siano fortemente orientati all'Amministrazione federale. Alcuni interlocutori hanno anche sottolineato come non sia stato ancora fornito un metro soddisfacente per valutare o controllare l'efficacia delle misure.

I metodi poco concreti di valutazione dell'efficacia fanno sì che le verifiche sull'attuazione delle misure siano molto formali e poco incentrate sui contenuti. A questo riguardo sarebbe auspicabile una classificazione più flessibile, che permetta una maggiore differenziazione in base al tipo di misura, come ad esempio misure immediate, progetti e nuovi compiti correnti.

Conclusione: i campi d'azione e le misure si integrano bene nella strategia. Nel complesso si ritiene che la struttura della strategia sia adeguata e il piano di attuazione uno strumento chiave appropriato. I campi d'azione e le misure sono sufficienti a fronteggiare tutte le sfide e sono direttamente riconducibili agli obiettivi della strategia.

3 Prestazioni ed effetti dei campi d'azione

La SNPC 2018–2022 è concepita per dare i risultati sperati attraverso le misure associate ai dieci campi d'azione. I campi d'azione e le misure nel complesso e nell'ottica della strategia si ritrovano a livello di output. Al contrario i campi d'azione con le rispettive misure possono essere differenziati in base alle prestazioni raggiunte (output) e agli effetti auspicati (outcome) che si punta a ottenere attraverso gli stessi. Le considerazioni riportate di seguito si riferiscono al livello degli output e degli outcome dei campi d'azione e delle misure e forniscono un'analisi bilanciata dei campi d'azione. Per ogni campo d'azione viene data una risposta alle seguenti domande:

Campi d'azione: in che misura i campi d'azione definiti sono adeguati per affrontare le sfide attese in relazione ai ciber-rischi?

Misure: quanto le singole misure e le relative tappe fondamentali sono adeguate a raggiungere gli obiettivi della SNPC 2018–2022? (P. es. sarebbero opportune altre misure? Bisognerebbe estendere determinate misure? Ci sono eventualmente misure che dovrebbero essere eliminate?)

3.1 Acquisizione di competenze e conoscenze

N.	Misura	Progetto di attuazione	Stato
1	Individuazione precoce di tendenze e tecnologie e acquisizione delle conoscenze	Monitoraggio delle tecnologie	realizzato
		Analisi delle tendenze	realizzato
2	Ampliamento e promozione delle competenze di ricerca e formazione	Analisi del fabbisogno per la creazione di offerte formative	realizzato
		Centro di ricerca e supporto dei due politecnici federali	realizzato
		Cyber Defence Campus	realizzato
		Promozione della ricerca e della formazione interdisciplinare in materia di cibersicurezza	realizzato
		Promozione dell'«hackeraggio etico»	realizzato
		Svolgimento del programma pilota bug bounty	realizzato
3	Creazione di condizioni quadro vantaggiose per un'economia della sicurezza delle TIC innovativa in Svizzera	Creazione di centri di innovazione	accantonato
		Think tank sulla cibersicurezza	realizzato

Tabella 3: misure e tappe fondamentali incl. stato di attuazione nel campo d'azione «Acquisizione di competenze e conoscenze ». Fonte: Consiglio federale, 2021

Misure e obiettivo: il campo d'azione «Acquisizione di competenze e conoscenze» comprende le misure da M1 a M3, il cui obiettivo è creare condizioni e requisiti adeguati per le attività che dovranno basarsi su di esse.

Valutazione delle prestazioni: per tutte le misure sono stati realizzati importanti progetti di attuazione, in due misure i progetti di attuazione sono stati accantonati. Nel campo d'azione «Acquisizione di competenze e conoscenze» è stato possibile fornire le prestazioni principali (output) e con lo SSCC è stato possibile creare come auspicato una rete tra università, amministrazione, industria e società civile. Si è anche intensificata la collaborazione tra i PF e il DDPS, soprattutto per quanto riguarda la formazione nell'ambito della sicurezza informatica. Sono stati inoltre elaborati o sono in fase di elaborazione molti altri progetti concreti e progetti di attuazione in altri campi d'azione (outcome).

Valutazione degli effetti: gli intervistati hanno sottolineato la grande importanza di questo campo d'azione, in quanto il suo outcome pone le basi per affrontare in modo adeguato i ciber-rischi. Tra gli outcome più importanti sono stati citati il rapporto del CYD di armasuisse sullo sviluppo tecnologico e le conferenze del CYD insieme alle università, ma anche i workshop dello SSCC – l'iniziativa congiunta dei politecnici federali di Losanna e Zurigo – e la panoramica delle offerte di formazione presso le università. In base ai giudizi espressi, l'effetto del campo d'azione viene percepito in modo indiretto. Questa percezione coincide con i risultati di una ricerca condotta dall'università di Oxford, che, utilizzando una scala di maturità che va da uno a cinque, assegna al cosiddetto «Framework for Professional Training» un punteggio di 4,5 decisamente superiore alla media (Università di Oxford, 2020, v. allegato A-5).

Conclusione: con la realizzazione di gran parte dei progetti di attuazione del campo d'azione sono state fornite le prestazioni principali, sono state realizzate le strutture desiderate ed è stata creata una rete di conoscenze. Gli outcome sono stati raggiunti e l'impact si è avuto su altri campi d'azione.

3.2 Situazione di minaccia

N.	Misura	Progetto di attuazione	Stato
4	Rafforzamento delle capacità di valutazione e rappresentazione delle ciberminacce	Identificazione dei gruppi target e delle loro esigenze	realizzato
		Definizione del catalogo di prodotti per ogni gruppo target (catalogo delle prestazioni)	realizzato
		Creazione delle fonti e delle risorse produttive necessarie	realizzato

Tabella 4: misure e tappe fondamentali incl. stato di attuazione nel campo d'azione «Situazione di minaccia». Fonte: Consiglio federale, 2021

Misura e obiettivo: nel campo d'azione «Situazione di minaccia» è inserita la misura M4, il cui obiettivo è promuovere una prevenzione efficace orientata alle minacce effettive fornendo una panoramica il più possibile completa della situazione di minaccia.

Valutazione delle prestazioni: la misurata è stata in gran parte attuata. Secondo i partner intervistati sono stati realizzati i progetti di attuazione pertinenti, in grado cioè di informare

la Confederazione e altri «clienti» in modo adeguato in base al gruppo di destinatari a cui appartengono.

Valutazione degli effetti: in questo caso è stato fatto riferimento soprattutto al grafico radar della situazione, elaborato per informare in modo regolare e sistematico il Comitato per la cibersicurezza del Consiglio federale e il Comitato ristretto Ciber sulla situazione di minaccia. Altrettanto apprezzati sono stati l'impegno dell'NCSC nel fornire informazioni sulle minacce correnti alla collettività e i progetti di prevenzione e sensibilizzazione del SIC.

Durante le interviste i responsabili delle misure hanno richiamato l'attenzione su questioni specifiche relative alla situazione di minaccia: la rapidità con cui si evolve la situazione di minaccia rappresenta una grande sfida per tutto il personale del settore. La difficoltà sta nel fornire l'input corrispondente come presupposto per l'efficacia. Oltre a quelle necessarie per la gestione delle attività operative programmate è necessario avere capacità sufficienti per garantire una reazione rapida a nuove situazioni e una formazione continua costante. In futuro quindi ci si dovrà concentrare maggiormente sulla creazione di un pool di esperti ben formati. Secondo gli intervistati questa è una sfida molto importante, anche se nel frattempo si sta già lavorando con successo agli aspetti infrastrutturali per lo sviluppo delle capacità e delle competenze.

Conclusione: con il loro outcome, i progetti di attuazione realizzati hanno creato una buona base, che in futuro permetterà agli organi preposti (in particolare SIC e NCSC) di ottenere gli effetti sperati. Valutando dal punto di vista dei contenuti la situazione di minaccia sarebbero auspicabili ulteriori passi avanti. La criticità della situazione per quanto riguarda la disponibilità di esperti rende però difficile uno sviluppo in questo senso.

3.3 Gestione della resilienza

N.	Misura	Progetto di attuazione	Stato
5	Miglioramento della resilienza delle TIC delle infrastrutture critiche (UFPP, in collaborazione con gli uffici specializzati in settori sottoposti a regolamentazione)	Attuazione dei progetti previsti e in corso per rafforzare la resilienza nei sottosettori critici	realizzato
		Costituzione del gruppo di lavoro accademico per la cibersicurezza	realizzato
6	Miglioramento della resilienza delle TIC all'interno dell'Amministrazione federale [7]	Sviluppo di disposizioni in materia di sicurezza per consentire metodi di progetto agili	realizzato
		Campagna di sensibilizzazione nell'Amministrazione federale	realizzato
		Trasmissione sicura dei dati (SCION)	realizzato
		Security Operations Center (SOC) UFIT	realizzato

7 Il Consiglio federale già nel 2015 ha dato incarico di realizzare una rete di dati sicura (SDNV) (Consiglio federale, 2015). Il relativo progetto non è un progetto di attuazione della SNPC, ma è strettamente connesso alla misura n. 6 della SNPC 2018–2022.

N.	Misura	Progetto di attuazione	Stato
		Creazione di un'interfaccia con il settore dei politecnici federali	realizzato
7	Scambio di conoscenze e creazione di basi per migliorare la resilienza delle TIC nei Cantoni	Scambi permanenti tra Cantoni e Centro di competenza per la cibersicurezza	accantonato
		Svolgimento della «Ciber-Landsgemeinde»	realizzato
		Creazione di un'interfaccia tra PF e Cantoni	realizzato

Tabella 5: misure e tappe fondamentali incl. stato di attuazione nel campo d'azione «Gestione della resilienza». Fonte: Consiglio federale, 2021

Misure e obiettivi: le infrastrutture critiche e le autorità devono attuare delle misure che, in caso di possibili incidenti, possano limitare i danni e ridurre il più possibile i tempi di inattività. Le misure dalla M5 alla M7 servono a individuare e attuare soluzioni che permettano di aumentare la resilienza.

Valutazione delle prestazioni: gran parte delle misure sono in una fase di attuazione avanzata. Grazie all'attenzione rivolta all'aumento della resilienza delle infrastrutture critiche, alle direttive per l'Amministrazione federale e allo scambio tra i Cantoni, è stato possibile compiere notevoli passi avanti. Soprattutto per quanto riguarda la misura M7, l'impegno dei Cantoni gioca un ruolo molto importante e attraverso un proprio piano di attuazione permette di aumentare ulteriormente la cibersicurezza. Tra gli output più rilevanti è stato menzionato l'aggiornamento delle analisi dei rischi e delle vulnerabilità in vari settori, il rafforzamento della resilienza dell'Amministrazione federale attraverso l'OCiber nonché lo svolgimento della «Ciber-Landsgemeinde» e l'istituzione dell'Istituto Nazionale di Test per la Cibersicurezza a Zugo. È stato inoltre sottolineato come il campo d'azione Gestione della resilienza dovrà essere assolutamente presente anche nel prossimo ciclo della strategia.

Valutazione degli effetti: dalle interviste ai responsabili delle misure è emerso che le misure scelte sono ritenute corrette e funzionali agli obiettivi da raggiungere e che debbano essere proseguite. Nelle infrastrutture critiche le misure hanno portato all'avvio di attività (outcome) a supporto della protezione contro i ciber-rischi. In base alla Strategia nazionale per la protezione delle infrastrutture critiche 2018–2022 (strategia PIC, Consiglio federale, 2017) attualmente sarebbero coperti 27 diversi sottosettori. L'approccio basato sul rischio, scelto già per la strategia SNPC 2012–2017, nelle linee guida dell'European Union Agency for Network and Information Security viene citato come un esempio da seguire (ENISA, 2016). Dalla valutazione fatta dall'università di Oxford, nell'attuazione delle sue misure la Svizzera è a un grado di maturità pari a tre («established stage») su cinque («dynamic stage») (University of Oxford, 2020). Nonostante l'elevato livello delle conoscenze e le strategie adeguate, mancano ancora le capacità per attuare rapidamente e su tutto il territorio nazionale le conoscenze e le strategie di protezione.

L'approccio adottato, fortemente incentrato sulla responsabilità individuale dei gestori, sta però dimostrando i suoi limiti, perché lascia molto margine di manovra ai soggetti coinvolti e sono loro stessi a poter decidere l'entità delle attività svolte per raggiungere l'outcome.

Secondo la maggior parte degli intervistati sarebbe auspicabile rendere le disposizioni più vincolanti, prevedendo ad esempio disposizioni specifiche per un determinato settore o approcci maggiormente normativi (v. punto 3.4). Una revisione esterna sulla cibersicurezza condotta nel 2020 giungeva alla stessa conclusione (University of Oxford, 2020). Uno studio del Politecnico federale di Zurigo (CSS, 2016) su questo punto invita a un confronto con altri modelli. Alcuni degli intervistati hanno sottolineato l'importanza della responsabilità individuale e accolto con scetticismo la possibilità di una maggiore regolamentazione. Occorre inoltre ricordare che il grado di regolamentazione dei sottosettori critici è molto diverso.

Conclusione: le misure relative alla resilienza delle TIC destinate alle infrastrutture critiche e all'Amministrazione federale sono state notevolmente sviluppate. L'output è ritenuto elevato, la consapevolezza riguardo al problema è maggiore, ma l'effetto sui gruppi di destinatari non è ancora soddisfacente. Finora non è stato possibile far approvare degli standard minimi.

3.4 Standardizzazione / regolamentazione

N.	Misura	Progetto di attuazione	Stato
8	Sviluppo e introduzione di standard minimi	Sviluppo e attuazione di standard minimi per migliorare la resilienza delle TIC Sviluppo e approntamento di ausili per le PMI	realizzato
		Marchio di qualità Cyber Safe per Comuni	realizzato
		Marchio di qualità per fornitori di servizi IT	realizzato
9	Verifica dell'obbligo di notifica dei ciberincidenti e decisione in merito alla relativa introduzione	Studio dei modelli di massima degli obblighi di notifica	realizzato
		Dibattito di principio con il mondo economico e le autorità	realizzato
10	Internet governance globale	Incontro del gruppo di alto livello istituito dal Segretario generale delle Nazioni Unite	realizzato
		Piattaforme di scambio multistakeholder per il coordinamento a livello nazionale	realizzato
11	Acquisizione di know-how su aspetti della standardizzazione collegati alla sicurezza informatica	Rafforzamento dei progetti di standardizzazione con il supporto delle Scuole universitarie	realizzato
		Contributo della Svizzera ad ancorare il tema della cibersicurezza nella politica finanziaria internazionale	realizzato

Tabella 6: misure e tappe fondamentali incl. stato di attuazione nel campo d'azione «Standardizzazione / regolamentazione». Fonte: Consiglio federale, 2021

Misure e obiettivi: le misure da M8 a M11 sulla standardizzazione e regolamentazione della SNPC 2018–2022 si concentrano sulla creazione di basi che promuovano la standardizzazione e la regolamentazione. Sono stati sviluppati tre marchi di qualità per la cibersicurezza di Comuni e PMI (Cyber-Safe), per fornitori di servizi IT (CyberSeal) e per

aziende tecnologiche (Digital Trust). Per quanto riguarda la regolamentazione è stato concluso un nuovo progetto in materia in base al quale dal 2022 determinati «apparecchi radio», come telefoni cellulari, tablet e altri dispositivi che possono comunicare tramite Internet, e le applicazioni del cosiddetto Internet delle cose, dovranno soddisfare determinati requisiti per quanto riguarda la cibersicurezza. Queste nuove disposizioni dovrebbero garantire una maggiore protezione delle reti di telecomunicazione, una migliore tutela della privacy dei consumatori e una riduzione dei rischi di frode finanziaria. Inoltre sono stati elaborati i progetti posti in consultazione per l'istituzione dell'obbligo di notifica e dell'ordinanza sulle telecomunicazioni e le commissioni delle Camere federali hanno approvato la LSIn.

Valutazione delle prestazioni: fino a questo momento le misure sono state attuate secondo i piani. Per tutte e quattro le misure i progetti di attuazione che preparavano le basi tecniche e formulavano le proposte per la strutturazione sono stati attuati dagli uffici coinvolti. A questo riguardo è stato fatto notare che, oltre ai progetti di attuazione, negli standard sono confluite direttamente e in vari modi le conoscenze tecniche delle università (p. es. relative all'eliminazione delle vulnerabilità nella tecnologia 5G).

Gli attori intervistati hanno sottolineato come l'applicazione degli standard richieda molte risorse. Le cause sono:

— *Volontarietà*: per la gran parte dei destinatari del mondo economico, della popolazione e delle autorità l'attuazione delle misure per garantire una maggiore sicurezza contro i ciber-rischi è su base volontaria. I principi di buona prassi sono da considerarsi come delle offerte e parte di condizioni quadro a sostegno. Soprattutto per le infrastrutture critiche sarebbe quindi necessario un intervento più su larga scala che obblighi all'applicazione degli standard.

— *Processo legislativo*: la SNPC 2018–2022 è una strategia del Consiglio federale relativa ai contenuti. Può soltanto stimolare processi legislativi e fornire un supporto per quanto riguarda i contenuti. Il loro eventuale svolgimento e le relative modalità vengono decisi dai responsabili politici.

— *Rete e strutture decentrate*: nelle strutture decentralizzate interconnesse di internet non è possibile applicare in modo unilaterale standard e requisiti in termini di governance omogenei. Numerosi attori (statali, semistatali ma anche privati) devono sostenere gli sforzi compiuti in questo senso. Attraverso proposte fondate dal punto di vista dei contenuti e contribuiti alla discussione la Svizzera può giocare il proprio ruolo all'interno degli organi internazionali.

Riassumendo, le persone intervistate sono arrivate alla conclusione che gli output delle misure hanno fornito le basi necessarie per supportare la standardizzazione e permettere in futuro un'eventuale regolamentazione. Non è stato tuttavia possibile incentivare in modo significativo l'attuazione e la diffusione di queste misure nell'ambito della SNPC 2018–2022 e tra gli attori che fanno parte della rete della SNPC.

Valutazione degli effetti: gli effetti derivanti dai progetti di attuazione messi in atto sono considerati ancora limitati. Come misura «indiretta» sarebbe stata creata un'offerta che dovrebbe essere accolta dal gruppo di destinatari come domanda. Con i progressi ottenuti nell'ambito della regolamentazione si presume che questa domanda possa essere incentivata e quindi che in futuro gli effetti possano essere maggiori.

Il potenziale impatto degli standard elaborati è smorzato anche dal fatto che le aziende hanno la possibilità di scegliere tra standard diversi di attori e istituzioni diversi. A questo proposito, nel prossimo ciclo della strategia sarebbe opportuno valutare la possibilità di puntare non tanto su standard sviluppati internamente quanto su standard e framework riconosciuti a livello internazionale.

Conclusione: per quanto riguarda la standardizzazione sono state create delle basi, che fino a questo momento hanno però trovato scarsa applicazione perché poco diffuse e su base prevalentemente volontaria. I progetti di regolamentazione elaborati creano condizioni quadro che favoriscono la diffusione delle basi. Outcome e impact al momento sono ritenuti molto limitati, tuttavia vi sono i presupposti necessari perché in futuro l'impatto di queste misure possa aumentare.

3.5 Gestione degli incidenti

N.	Misura	Progetto di attuazione	Stato
12	Potenziamento di MELANI come partenariato pubblico-privato (PPP) per i gestori di infrastrutture critiche	Ampliamento mirato della cerchia chiusa di clienti	realizzato
		Sviluppo e ampliamento della gamma di servizi e prodotti	realizzato
		Potenziamento dell'attuale piattaforma di scambio	realizzato
13	Creazione di servizi per tutte le imprese	Istituzione di un servizio nazionale di contatto ciber	realizzato
		Informazione tempestiva mediante l'app Alertswiss in caso di incidente	realizzato
14	Collaborazione della Confederazione con gli uffici competenti e i centri di competenze	Panoramica dei SOC e dei CERT attualmente operativi con i rispettivi interlocutori	realizzato
		Scambio di informazioni con i CERT e i SOC	realizzato
15	Processi e basi della gestione degli incidenti nell'Amministrazione federale	Elaborazione di un'ordinanza in materia di cibersicurezza	realizzato
		Predisposizione di un processo di gestione degli incidenti informatici per l'Amministrazione federale	realizzato

Tabella 7: misure e tappe fondamentali incl. stato di attuazione nel campo d'azione «Gestione degli incidenti». Fonte: Consiglio federale, 2021

Misure e obiettivi: le quattro misure dalla M12 alla M15 per la gestione degli incidenti devono creare i presupposti legali, organizzativi, processuali e contenutistici per consentire una gestione rapida ed efficace degli incidenti informatici.

Valutazione delle prestazioni: i progetti di attuazione delle quattro misure sono stati praticamente completati e sono disponibili i relativi outcome. I partner intervistati si sono concentrati in particolare sull'NCSC come servizio di contatto e sulla OCiber, che stabilisce le competenze in materia di gestione degli incidenti all'interno dell'Amministrazione federale. L'NCSC nel 2021 ha ricevuto e verificato oltre 21 400 segnalazioni di ciberincidenti (www.ncsc.admin.ch, consultato il 31.01.2022). Le cosiddette cerchie chiuse di clienti sono state ulteriormente ampliate rafforzando così il ruolo del servizio di contatto come partenariato pubblico-privato.

Valutazione degli effetti: nel valutare gli effetti è stata fatta una distinzione tra i singoli casi e l'effetto complessivo sulla protezione dai ciber-rischi.

Analizzando i singoli casi le persone intervistate ritengono che le strutture, le competenze e i processi messi in atto per la gestione degli incidenti siano efficaci. L'NCSC dispone delle competenze e delle strutture necessarie per garantire la propria capacità di reazione. Il processo di gestione degli incidenti, inoltre, viene costantemente controllato e, se necessario, adeguato sulla base degli eventi trattati. Le condizioni quadro giuridiche per la gestione degli incidenti all'interno dell'Amministrazione federale sono chiarite nell'OCiber, mentre i margini di manovra dell'NCSC in ambito civile dovrebbero essere ampliati mediante il progetto sull'introduzione dell'obbligo di notifica attualmente in consultazione. Parallelamente l'esercito ha sviluppato le capacità per essere pronto a intervenire nella gestione degli incidenti in ambito militare. Ne risultano strutture e processi pronti all'impiego giudicati adeguati per garantire la capacità di agire e l'integrità di autorità, economia, infrastrutture critiche e popolazione.

Per quanto riguarda l'Amministrazione federale, dal 2018 la procedura di gestione degli incidenti è stata chiarita e l'OCiber ne ha definito le responsabilità. La gestione degli incidenti è stata affidata principalmente all'NCSC, decisione giudicata importante dalle parti coinvolte per garantire una gestione agile ed efficace degli incidenti. Da allora non si sono verificati incidenti gravi, pertanto non si hanno esperienze dirette che possano dimostrare l'adeguatezza e l'efficacia immediata della procedura stabilita.

Una gestione efficace degli incidenti può avere un effetto preventivo ed evitare potenziali attacchi. Gli attori intervistati non hanno rilevato un effetto di questo tipo. Le segnalazioni di attacchi nel ciberspazio pervenute all'NCSC sono in forte aumento.

Conclusione: le competenze, i processi e le capacità maggiori sviluppati nell'ambito della gestione degli incidenti hanno rafforzato la resilienza dei gruppi di destinatari in misura diversa. Non è stato però osservato alcun effetto preventivo.

3.6 Gestione delle crisi

N.	Misura	Progetto di attuazione	Stato
16	Integrazione degli uffici competenti operanti nel settore della cibersicurezza negli stati maggiori di crisi della Confederazione	Arricchimento del lessico del ciberspazio	realizzato
17	Esercizi congiunti di gestione delle crisi	Creazione delle basi per le esercitazioni di crisi che implicano aspetti inerenti al ciberspazio	realizzato
		Svolgimento di esercitazioni di settore specifiche	realizzato
		Introduzione di aspetti inerenti al ciberspazio nelle esercitazioni di crisi trasversali	realizzato

Tabella 8: misure e tappe fondamentali incl. stato di attuazione nel campo d'azione «Gestione delle crisi». Fonte: Consiglio federale, 2021

Misure e obiettivi: attraverso le misure M16 e M17 la Confederazione sviluppa ulteriormente le proprie capacità di gestione delle crisi e le mette alla prova. Determinate conoscenze e opportunità di formazione sono condivise soprattutto con il gruppo di destinatari delle infrastrutture critiche.

Valutazione delle prestazioni: il sistema di gestione delle crisi pianificato nell'ambito delle misure M16 e M17 è stato sviluppato. Le procedure di formazione e le modalità di lavoro degli stati maggiori di crisi sono stati definiti, cosicché le attività operative possano essere avviate rapidamente. Sono state svolte esercitazioni di crisi insieme al settore finanziario e a quello sanitario. Il delegato federale alla cibersicurezza è stato inserito nello Stato maggiore federale Protezione della popolazione (SMFP).

Valutazione degli effetti: le parte coinvolte ritengono che tempi di reazione rapidi e periodi di intervento sufficienti (outcome) aumentino la resilienza dell'Amministrazione federale. Allo stesso modo si ritiene che anche la capacità di agire sia maggiore data una tendenziale riduzione dei tempi di inattività provocati da incidenti.

In generale sarebbe chiaro come vengono individuati gli obiettivi e pianificati gli attacchi. Dopo ogni crisi si svolge un debriefing con l'obiettivo di adeguare i processi e le strutture alla luce di quanto appreso durante la gestione dell'incidente. Le persone intervistate non sono state però in grado di valutare del tutto se e in quale misura questo possa avere un effetto preventivo. Gli stati maggiori di crisi seguono corsi di formazione specifici volti a migliorare la loro capacità di agire, verificata poi attraverso apposite esercitazioni. Tuttavia non sono chiari gli effetti a lungo termine delle esercitazioni nelle modalità precedenti.

Conclusione: le capacità di reazione e intervento dell'Amministrazione federale sono state aumentate e questo assicura meglio una capacità di agire costante da parte delle autorità e dell'Amministrazione grazie alla regolamentazione delle responsabilità e delle formazioni. Vista la complessità, rimane tuttavia difficile garantire un intervento rapido. Gli effetti di queste misure potranno essere verificati soltanto in occasione di eventi futuri.

3.7 Perseguimento penale

N.	Misura	Progetto di attuazione	Stato
18	Casistica della cibercriminalità (fedpol, CCPCS con NEDIK)	Casistica della cibercriminalità (PICSEL)	fase di test in corso
		Elaborazione di una casistica giudiziaria	realizzato
		Presentazione degli sviluppi, degli scenari e delle ripercussioni della cibercriminalità	realizzato
19	Rete di supporto alle indagini nella lotta alla criminalità digitale (fedpol come componente della CCPCS)	Basi giuridiche concernenti la collaborazione e il computo delle prestazioni tra Confederazione e Cantoni nonché tra Cantoni	realizzato
20	Formazione (CCPCS incl. fedpol, RSS incl. Ministero pubblico della Confederazione)	Attuazione dei piani di formazione	realizzato
21	Ufficio centrale per la cibercriminalità (fedpol)	Nessuna tappa fondamentale entro il secondo trimestre del 2021	

Tabella 9: misure e tappe fondamentali incl. stato di attuazione nel campo d'azione «Perseguimento penale». Fonte: Consiglio federale, 2021

Misure e obiettivi: per quanto riguarda il perseguimento penale in ambito informatico la Confederazione ha il compito di favorire la collaborazione a livello intercantonale e possiede le competenze dirette in materia di perseguimento penale. Il Tribunale federale ha più volte confermato queste competenze sui Cantoni in materia di perseguimento penale, ad esempio per quanto riguarda la lotta alla criminalità organizzata e alla grave criminalità economica nel ciberspazio. Questa lotta viene combattuta insieme ai Cantoni attraverso il cosiddetto cyberboard (Cyber-STRAT e Cyber-CASE). Dal 2018 lo scambio di informazioni e di conoscenze si è intensificato grazie al ruolo centrale svolto dalla rete di sostegno alle indagini nella lotta contro la criminalità informatica (NEDIK), nella quale dovranno essere integrate 26 organizzazioni cantonali autonome con i propri processi, sistemi informatici, sistemi di lotta alla cibercriminalità eccetera. L'Ufficio federale di polizia (fedpol) con le misure M18–M21 elabora le basi, favorisce la formazione e sostiene il coordinamento.

Valutazione delle prestazioni: le misure M18–M21 nel complesso procedono secondo le previsioni e l'attuazione operativa viene gradualmente realizzata con i Cantoni. La casistica PICSEL è in una fase di test. Con NEDIK viene messa a disposizione una rete a sostegno delle indagini e viene studiato un percorso formativo. In questo caso i rapporti tra i Cantoni sono ben consolidati, ma ognuno fornisce un contributo diverso alla NEDIK. Tutte le misure inerenti al perseguimento penale non sono state ancora completamente concluse. Pertanto il fatto di avere ancora un quadro incompleto della situazione (progetto di attuazione della casistica «PICSEL») rappresenta una sfida importante. Infine, in merito alle attività del 2022 sono state discusse alcune modifiche al progetto, ma non sono state ancora prese delle decisioni in merito.

Valutazione degli effetti: grazie soprattutto a NEDIK è stato possibile compiere notevoli passi avanti a livello nazionale nella lotta coordinata alla cibercriminalità. Nel caso di NEDIK così come di altri progetti di attuazione conclusi, però, è ancora presto per stabilire

gli outcome e poter dimostrare quali siano stati gli effetti, perché si sono conclusi da troppo poco tempo.

Tutti gli attori intervistati hanno sottolineato l'estrema importanza di una panoramica completa e aggiornata della situazione generale di polizia. Secondo gli intervistati le relative misure della SNPC avrebbero un approccio preventivo e sarebbero incentrate principalmente sulla polizia. Quindi alla SNPC al momento manca una dimensione giudiziaria. Anche i «rappresentanti degli utenti» dei Cantoni intervistati hanno segnalato diversi ostacoli per quanto riguarda questioni organizzative, basi legali cantonali e ripartizione delle competenze tra autorità inquirenti e addette al perseguimento penale. Tali ostacoli dovrebbero essere superati per sfruttare appieno le possibilità che sono state create.

Per quanto riguarda il chiarimento a livello giuridico, gli attori interpellati ritengono che sia necessario che il legislatore si stacchi maggiormente dall'hardware per quanto riguarda la cibercriminalità. Per quanto concerne i media di archiviazione decentralizzati e non legati a una determinata posizione geografica con collegamento in tempo reale si dovrebbe applicare la «triade CIA»[8]. In questi casi le autorità di perseguimento penale adotterebbero approcci diversi, come il «principio di trasparenza» (evoluzione del diritto) per la garanzia/assunzione delle prove nel luogo di disponibilità e un «Swiss CLOUD-Act» (applicazione del diritto), in base al quale tutte le imprese operanti a livello internazionale con filiali in Svizzera sarebbero obbligate alla pubblicazione dei dati ai sensi del diritto svizzero. All'interno delle Camere federali in passato sono stati presentati interventi al riguardo.

Conclusione: coordinando e rafforzando la collaborazione a livello intercantonale per quanto riguarda il perseguimento penale della cibercriminalità, tali azioni possono essere più efficaci ed efficienti nonché prevenire possibili reati. Le differenze tecniche, giuridiche, processuali e di altra natura tra le autorità di perseguimento penale organizzate a livello federale e le capacità limitate in termini di personale al momento stanno ostacolando il raggiungimento dei possibili outcome ed effetti. Sono in corso misure volte ad aumentare le capacità. Inoltre sono presenti delle lacune di tipo giudiziario per quanto riguarda l'attuazione a livello processuale del perseguimento penale nell'ambito dei reati informatici.

3.8 Ciberdifesa

N.	Misura	Progetto di attuazione	Stato
22	Ampliamento delle capacità di acquisizione delle informazioni e di attribuzione degli attacchi informatici	Capacità di acquisizione delle informazioni e di attribuzione	realizzato
		Svolgimento di una formazione specifica in ciberdifesa (esercito)	realizzato

[8] Triade CIA: «confidentiality», «integrity» e «availability», ovvero riservatezza, integrità e disponibilità

23	Capacità di eseguire misure attive nel ciberspazio secondo LAIn e LM	Utilizzo delle capacità del COE-BAC sviluppate nel quadro della LAIn	realizzato
24	Garanzia della prontezza operativa dell'esercito nel ciberspazio in ogni circostanza e regolamentazione del suo ruolo sussidiario di supporto delle autorità civili	Conclusione del progetto per lo sviluppo della ciberdifesa	realizzato

Tabella 10: misure e tappe fondamentali incl. stato di attuazione nel campo d'azione «Ciberdifesa». Fonte: Consiglio federale, 2021

Misure e obiettivi: ai sensi dell'articolo 6 lettera b OCiber, per ciberdifesa si intendono «tutte le misure militari e del SIC 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; vi rientrano anche le misure attive volte a individuare le minacce, identificare gli aggressori nonché ostacolare e bloccare gli attacchi». Con le tre misure M22, M23 e M24 si fornisce un sostegno alla ciberdifesa per lo svolgimento di tutti i suoi compiti attraverso lo sviluppo delle capacità necessarie, comprese quelle in termini di personale.

Valutazione delle prestazioni: le misure M22 e M23 sono state interamente attuate e la misura M24 è in gran parte completata. Tra i principali progressi vengono citati la decisione del Consiglio federale di trasformare la Base d'aiuto alla condotta (BAC) dell'esercito in un Comando Ciber e la nuova Strategia Ciber DDPS 2021–2024 (DDPS, 2021), che stabilisce i principi fondamentali in base ai quali è chiamato ad agire il dipartimento nel settore della ciberdifesa. L'esercito ha la capacità di implementare misure attive nel ciberspazio. La sua capacità di intervento in ambito informatico è garantita in ogni circostanza. Allo stesso modo è stata attuata anche la misura relativa alla formazione in ambito informatico dei componenti dell'esercito. La creazione del Cyber Training Center con un'offerta formativa aperta anche a terzi è stata posticipata al 2026 circa.

Valutazione degli effetti: secondo i partner intervistati gli output ottenuti attraverso questo campo d'azione hanno avuto un impatto evidente e la ciberdifesa ora viene percepita come uno dei tre pilastri della strategia. Il SIC e l'esercito nel periodo della strategia in esame hanno subìto un importante sviluppo e notevolmente potenziato alcune capacità. In questo modo sono state create le basi per garantire il raggiungimento, in futuro, degli outcome necessari.

Conclusione: attraverso i progetti di attuazione realizzati sono state chiaramente rafforzate le capacità dell'esercito e del SIC nonché la loro prontezza operativa nel ciberspazio. La Strategia Ciber DDPS rafforza ulteriormente il campo d'azione attraverso ulteriori misure. Rimane ancora da ampliare l'offerta formativa a soggetti terzi. In questo modo sarebbe possibile migliorare l'interoperabilità e l'efficacia della RSS.

3.9 Politica estera e di sicurezza informatica

N.	Misura	Progetto di attuazione	Stato
25	Ruolo attivo nella definizione e partecipazione ai processi di politica in materia di cibersicurezza esterna	Partecipazione ai processi dell'ONU	realizzato
		Rappresentanza degli interessi nell'ambito dell'OSCE (consolidamento del clima di fiducia tra gli Stati)	realizzato
		Creazione e istituzione dell'iniziativa «Geneva Dialogue on Responsible Behaviour in Cyberspace»	realizzato
		Osservazione degli sviluppi in seno all'Unione europea (in particolare del Servizio europeo per l'azione esterna e dell'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione e di ENISA)	realizzato
		Impegno per la promozione di un ciberspazio aperto e libero	realizzato
26	Cooperazione internazionale per la crescita e lo sviluppo delle capacità nel settore della cibersicurezza	Organizzazione di workshop con organizzazioni regionali	realizzato
		Organizzazione di workshop per la creazione di istituzioni e strutture per la cibersicurezza esterna	realizzato
27	Consultazioni politiche bilaterali e dialoghi multilaterali sulla politica estera di cibersicurezza	Sino-European Cyber Dialogue (SECD)	realizzato
		MENA Cybersecurity Forum	realizzato

Tabella 11: misure e tappe fondamentali incl. stato di attuazione nel campo d'azione «Politica estera e di sicurezza informatica». Fonte: Consiglio federale, 2021

Misure e obiettivi: le misure relative alla politica estera e di sicurezza informatica (M25, M26 e M27) puntano a garantire un posizionamento attivo della Svizzera nella politica internazionale di sicurezza informatica. Rientrano nelle misure di politica estera e non sono concepite per avere un effetto diretto sui gruppi di destinatari.

Valutazione delle prestazioni: dal 2018 i responsabili delle misure hanno apportato diverse modifiche alle misure stesse con l'obiettivo di concentrarsi maggiormente su quelle misure che sembravano fornire un contributo alla strategia, ovvero potevano mettere in contatto gli attori internazionali e la Svizzera. Nell'ambito delle misure M26 e M27 è stato instaurato un dialogo o sta per essere avviato un confronto con Svezia, Paesi Bassi, Austria, Gran Bretagna, Giappone, USA, Israele, Cina e, a livello multilaterale, con l'ASEAN. In collaborazione con la missione permanente in Kenia delle Nazioni Unite (ONU) e altri Stati e organizzazioni africani si sono tenuti dei workshop sul capacity building (fonte: prospetto del DFAE del 26.01.2022).

Valutazione degli effetti: in relazione all'outcome si è osservato come i contributi alle discussioni forniti all'interno di organi multilaterali sono stati presi maggiormente in considerazione rispetto a quelli espressi nell'ambito di scambi bilaterali tra Stati. Per questo, contrariamente a quanto si pensava inizialmente, l'OCSE si è rivelato un organo adeguato a livello operativo e di efficacia. A partire dal 1° gennaio 2022, inoltre, il delegato

federale è anche presidente del gruppo di lavoro dell'OCSE «Security in Digital Economy». La SNPC 2018–2022 ha contribuito in modo rilevante anche alla creazione del «Geneva Dialogue» per un comportamento responsabile nel ciberspazio[9].

Stando ai risultati di un recente sondaggio tra la popolazione (Sotomo, 2022), il 56 per cento degli intervistati dichiara di essere soddisfatto del modo in cui la Confederazione rappresenta gli interessi della Svizzera nell'ambito delle discussioni sulla regolamentazione multilaterale del ciberspazio.

A loro avviso, la partecipazione attiva e strategica della Svizzera al dialogo internazionale rappresenterebbe un supporto ai contatti internazionali derivanti dai campi d'azione di tipo applicativo (in particolare situazione di minaccia, perseguimento penale e ciberdifesa) e rafforzerebbe ulteriormente le basi della collaborazione. Questo outcome fornisce anche un sostegno ad altri campi d'azione affinché possano raggiungere i loro outcome fino a realizzare l'impact previsto.

Conclusione: la politica estera e di sicurezza informatica ha un effetto indiretto sulla protezione dei gruppi di destinatari. Le autorità svizzere e altri attori chiave (nell'ambito del «Geneva Dialogue») sono stati coinvolti nelle discussioni a livello internazionale sulla cyber governance al fine di sostenere la SNPC 2018–2022.

3.10 Visibilità e sensibilizzazione

N.	Misura	Progetto di attuazione	Stato
28	Creazione e attuazione di un piano per la comunicazione di informazioni sulla SNPC	Elaborazione di un piano per la comunicazione di informazioni sulla SNPC	realizzato
29	Sensibilizzazione del pubblico sui ciber-rischi	Sviluppo e svolgimento di una campagna nazionale di sensibilizzazione	realizzato
		Piattaforma di informazione sui ciber-rischi	realizzato

Tabella 12: misure e tappe fondamentali incl. stato di attuazione nel campo d'azione «Visibilità e sensibilizzazione». Fonte: Consiglio federale, 2021

Misure e obiettivi: il campo d'azione «Visibilità e sensibilizzazione» è costituito dalle misure M28 e M29. Esse sono rivolte all'esterno, alla popolazione e all'economia e servono, da un lato, a fornire informazioni sulla strategia e sulla sua attuazione e, dall'altro, a informare sugli sviluppi e sugli avvenimenti attuali.

Valutazione delle prestazioni: in base al piano per la comunicazione e a vari progetti di attuazione, dal 2018 sono state lanciate diverse campagne di sensibilizzazione all'interno e all'esterno dell'Amministrazione federale, anche in collaborazione con Prevenzione Svizzera della Criminalità (PSC). Contemporaneamente sono stati ampliati il sito web con le informazioni a disposizione di popolazione, aziende, esperti e autorità nonché i rapporti semestrali, detti «End-of-Week Report».

9 www.genevadialogue.ch, consultato il 10 gennaio 2022.

I progetti di attuazione di entrambe le misure sono stati in gran parte realizzati. Date le risorse disponibili, la comunicazione si è dovuta concentrare su pochi argomenti. Partendo dagli argomenti chiave utilizzati a livello comunicativo per l'attuazione della SNPC, la Confederazione ha cercato non soltanto il contatto diretto con i gruppi di destinatari, ma ha anche collaborato con diversi partner e utilizzato sistemi già esistenti e piattaforme di terzi. I progetti di attuazione realizzati hanno portato a idee e proposte per una prosecuzione del progetto e una continua sensibilizzazione, ma finora sono mancate le risorse per portarle avanti.

Valutazione degli effetti: come outcome gli intervistati hanno rilevato una visibilità decisamente migliore che hanno attribuito alle costanti attività di comunicazione dell'NCSC, alle campagne di sensibilizzazione e ai sondaggi sostenuti dai partner nonché alla comunicazione puntuale tramite progetti scelti. Le valutazioni effettuate sulla base dei cosiddetti equivalenti degli annunci pubblicitari e degli accessi, dei tempi di permanenza e dei bounce rate indicano una copertura a livello nazionale e una buona capacità di raggiungere vari segmenti dei diversi gruppi di destinatari. I gravi incidenti degli ultimi mesi hanno contribuito a richiamare l'attenzione dei gruppi di destinatari su questo tema.

Risulta tuttavia ancora evidente la necessità di misure specifiche dirette alla popolazione e alle PMI. Una situazione non certo favorita dall'atteggiamento passivo di una parte dei gruppi di destinatari, che si preoccupa di queste tematiche soltanto in caso di incidenti.

Alcuni ritengono poi necessario fornire maggiori informazioni sulle responsabilità. In alcuni casi, all'interno dell'Amministrazione federale e del Parlamento non è chiaro quali organi debbano occuparsi di quali mansioni, in particolare quando si tratta di fare una distinzione tra i compiti dell'NCSC e quelli del settore Trasformazione digitale e governance delle TIC (TDT) della Cancelleria federale.

In particolare è stato fatto riferimento alle molteplici attività svolte da diversi organi di comunicazione dell'Amministrazione federale al di fuori dell'NCSC che trattano anche il tema della protezione contro i ciber-rischi ma spesso senza prima confrontarsi con l'NCSC. In questo caso sarebbe opportuno agire in modo più coordinato per ottenere outcome migliori e anche l'effetto desiderato sui gruppi di destinatari.

Conclusione: la visibilità è notevolmente migliorata grazie a una comunicazione decisamente più forte, percepita soprattutto dall'economia e dalle infrastrutture critiche. Al contrario, si riesce a raggiungere ancora troppo poco la popolazione e le PMI. Occorre intervenire anche sul coordinamento delle attività di comunicazione dei diversi attori. L'impact generato da questo campo d'azione è indiretto.

4 Effetti sui gruppi di destinatari

La SNPC 2018–2022 intende aumentare la resilienza della popolazione, dell'economia e dello Stato nei confronti delle ciberminacce, per garantire la loro capacità di agire e la loro integrità. Attraverso la verifica dell'efficacia si è voluto indagare se e in quale misura si possono constatare questi effetti sui gruppi di destinatari. Le osservazioni e le valutazioni sottostanti riguardano quindi in particolare gli outcome della strategia.

Nello specifico sono state analizzate le seguenti domande:

Vantaggi: le misure della SNPC raggiungono i gruppi di destinatari così come auspicato? In che misura (p. es. i gruppi di destinatari sfruttano le misure o le strutture e i processi consolidati così come i prodotti, i servizi, le reti e i metodi elaborati)?

Effetti auspicati sui gruppi di destinatari: in che misura sono stati raggiunti gli effetti auspicati della SNPC 2018–2022 come, ad esempio, la competenza degli attori o la maggiore resilienza dei quattro gruppi di destinatari cui le misure sono esplicitamente rivolte (infrastrutture critiche, autorità, economia, popolazione)?

Effetti su altri attori: in che misura si possono poi osservare effetti su altri attori e come possono essere classificati?

4.1 Autorità

Secondo gli intervistati, lo sviluppo e l'attuazione della strategia sarebbero ben consolidati nell'Amministrazione e nelle autorità. I campi d'azione e le misure ovviamente formano un pacchetto coerente, dal momento che la struttura e le misure sono fortemente orientate all'organizzazione dell'Amministrazione. Gli intervistati, inoltre, hanno sottolineato come grazie alla SNPC sia migliorata la collaborazione tra Confederazione e Cantoni.

Gli effetti positivi hanno riguardato principalmente gli attori e i gruppi di destinatari che sono stati maggiormente coinvolti nella SNPC e, in particolare, le autorità. Qui la strategia è riuscita in un'importante opera di sensibilizzazione. Quando i compiti sono assegnati in modo chiaro, anche la strategia risulta efficace. Nei casi in cui, invece, ci si limita alla sensibilizzazione, si ottengono al massimo effetti a breve termine.

Come è stato sottolineato, la strategia nazionale è stata ripresa anche da altre autorità, come i Cantoni, e a partire da questa sono stati avviati alcuni progetti relativi alla gestione dei ciber-rischi. A questo riguardo non è ancora chiara la situazione nelle città e nei grandi Comuni, dove si presume vi sia ancora bisogno di intervenire. Questa necessità d'intervento, portata alla luce nei mesi scorsi dai media, è percepita anche dalla popolazione. In occasione di un sondaggio, alla domanda su come reputano la cibersicurezza dell'Amministrazione e delle infrastrutture critiche soltanto il 28 per cento degli intervistati ha dichiarato di ritenerla sufficiente (Sotomo, 2022).

Anche per quanto riguarda le autorità è stata sottolineata l'importanza della creazione di reti orizzontali che, al momento, non sarebbero ancora sufficienti. Secondo gli intervistati, le persone che si occupano degli stessi temi ma in diversi ambiti dovrebbero avere maggiori opportunità di confronto.

Conclusione: le autorità federali e cantonali sono ben integrate nella strategia e nei progetti di attuazione. L'output contribuisce alla sensibilizzazione e, quando competenze e responsabilità sono definite in modo chiaro, la strategia risulta efficace.

4.2 Infrastrutture critiche

La maggioranza dei partner intervistati ritiene che le attività di sensibilizzazione nel caso delle infrastrutture critiche avrebbero potuto essere più approfondite. Per quanto riguarda il loro settore, i gestori delle infrastrutture critiche sono completamente integrati attraverso il progetto per la protezione delle infrastrutture critiche (PIC) dell'Ufficio federale della protezione della popolazione e attraverso le relative misure cantonali stabilite sulla base del rispettivo piano di attuazione della SNPC, elaborato dalla RSS.

Rispetto al passato i gestori delle infrastrutture critiche ora prendono molto più seriamente la protezione contro i ciber-rischi. All'interno dei settori in cui operano grandi attori si rileva un avvicinamento e uno scambio più intenso, si percepisce un maggiore impegno. Nei settori in cui sono presenti imprese di dimensioni contenute e tanti attori diversi, invece, finora questo fenomeno è stato osservato meno frequentemente e si ha anche una minore consapevolezza del problema.

L'impressione che il livello di consapevolezza del problema sia diverso e, in alcuni casi, insufficiente è confermata da diversi studi, analisi e sondaggi. Da uno studio condotto dall'Ufficio federale dell'energia, per esempio, emerge che il settore svizzero dell'approvvigionamento di energia elettrica è ancora poco «maturo» per quanto riguarda l'attuazione delle misure suggerite (UFE, 2021). Nel rapporto semestrale 2020/2 l'NCSC ha trattato i rischi cui è esposto il settore della sanità e consigliato l'attuazione di diverse misure di protezione aggiuntive (NCSC, 2021a). Infine, da un sondaggio condotto nell'autunno 2021 che ha coinvolto 1254 persone della Svizzera tedesca (Sotomo, 2022) è emerso che il 72 per cento degli intervistati ritiene le infrastrutture critiche e le autorità in Svizzera non sufficientemente protette dai ciber-rischi.

I partecipanti al sondaggio percepiscono un conflitto negli obiettivi definiti, perché se da un lato si auspica che i gestori delle infrastrutture critiche operino in modo autonomo assumendosi le responsabilità, dall'altro non vi è alcun vincolo che li obblighi ad adottare le misure di protezione. Questo fa capire come il potenziale effetto di queste misure non sia ancora interamente sfruttato. È necessario quindi valutare altre modalità con cui promuovere l'attuazione delle misure. Tra le idee proposte vi è stata quella di una maggiore regolamentazione, che può andare da un principio di prevenzione a un obbligo di revisione (simile alla contabilità) fino al rispetto di uno standard minimo legale. Un'altra possibile soluzione potrebbe essere condurre analisi più approfondite degli eventi pericolosi, delle

relative cause e dei motivi più profondi, così da evitare situazioni di pericolo ed eventi futuri. L'attuale progetto sull'introduzione dell'obbligo di notifica di ciberattacchi per i gestori di infrastrutture critiche posto in consultazione rappresenta un possibile approccio.

Conclusione: i gestori delle infrastrutture critiche sono consapevoli del problema e strettamente coinvolti nelle misure e nei progetti di attuazione, tuttavia esistono delle differenze evidenti tra i vari settori. Le prestazioni fornite in attuazione della strategia non sono ancora sufficienti per proteggere in modo adeguato tutte le infrastrutture critiche.

4.3 Popolazione

Molti degli intervistati hanno notato una maggiore consapevolezza da parte della popolazione riguardo alla cibersicurezza. Le valutazioni fornite dalle persone responsabili delle misure partono dal presupposto che le campagne di sensibilizzazione e le pubbliche relazioni nell'ambito della SNPC e da parte dell'NCSC hanno potuto avere un raggio d'azione adeguato ai mezzi. Tuttavia non si hanno ancora prove empiriche né di questo né dei contributi delle iniziative e delle campagne di sensibilizzazione portate avanti in parallelo[10].

Le segnalazioni inviate dalla popolazione all'NCSC sono in costante aumento (nel 2021 sono state oltre 21 400), tuttavia non è chiaro il nesso tra un numero crescente di attacchi e una maggiore sensibilizzazione alla valutazione e alla segnalazione di un evento. Per la popolazione l'NCSC rappresenta anche uno strumento di orientamento volto a compiere un'attività di sensibilizzazione che raggiunge determinate fasce della popolazione. Inoltre è necessario tenere conto del fatto che gruppi diversi di popolazione non soltanto possiedono competenze digitali diverse, ma utilizzano anche gli strumenti TIC in maniera differente (v. p. es. Università di Zurigo, 2020). Per quanto riguarda la gestione degli incidenti, però, a detta degli intervistati l'NCSC sarebbe orientato solo in parte alla popolazione.

Quello che la SNPC non garantisce o non è finora riuscita a garantire sarebbe un'attività di sensibilizzazione e una formazione di base in ambito informatico rivolta ai giovani. Secondo i rappresentanti del mondo economico intervistati, infatti, sarebbe proprio questa la chiave per garantire una protezione a lungo termine della popolazione dai ciber-rischi. La SNPC, tuttavia, sembra avere scarse possibilità di raggiungere l'obiettivo, anche perché la formazione in generale rientra nelle competenze dei Cantoni.

La mancata formazione di base in ambito informatico lamentata da più parti si somma anche a competenze digitali giudicate, in generale, insufficienti (Sotomo, 2022). In un sondaggio condotto tra la popolazione è emerso che il 60 per cento degli intervistati ritiene che lo sviluppo delle competenze digitali nel settore della formazione sia troppo lento.

[10] Non è disponibile una panoramica delle rispettive iniziative e campagne di terzi.

Conclusione: le misure della SNPC 2018–2022 raggiungono solo alcune fasce molto specifiche della popolazione, e finora non si è ancora avuta una sensibilizzazione su larga scala.

4.4 Economia

Durante i colloqui relativi alla tutela del settore economico, tutti i partecipanti sono stati concordi nell'affermare che le grandi imprese internazionali sono capaci di proteggersi meglio dai ciber-rischi e, in alcuni casi, mettono a disposizione della SNPC le loro capacità ed esperienze. Al contrario le PMI, ovvero la maggior parte delle imprese che compongono l'economia svizzera, sono troppo poco protette e non sono sufficientemente consapevoli delle minacce presenti nel ciberspazio. Secondo gli esperti, inoltre, l'impegno profuso per garantire una maggiore protezione da queste realtà non riuscirebbe a tenere il passo con l'aumento dei ciberattacchi. Due i principali punti deboli:

— *Target degli attacchi*: le imprese si considerano obiettivi «poco interessanti».

— *Consapevolezza dei dati*: quando si parla di consapevolezza dei dati ci si concentra soprattutto sulla loro protezione, tralasciando la loro disponibilità e integrità (compresa quella dei processi aziendali).

Recenti sondaggi condotti tra le imprese confermano che spesso queste non sono sufficientemente protette dai ciberattacchi (gfs-Zürich, 2021). Ad esempio, se nel 2020 le aziende che avevano subìto attacchi tali da richiedere un impegno notevole per risoluzione dei danni erano il 25 per cento, alla fine del 2021 tale percentuale ha raggiunto il 33 per cento (gfs-Zürich, 2021). Anche l'NCSC rileva un aumento degli attacchi. A essere colpite sono sempre di più imprese note operanti a livello internazionale (NCSC, 2021b). Approssimativamente in Svizzera già 55 000 imprese hanno subìto attacchi informatici con conseguenze gravi.

Dal sondaggio condotto da gfs-Zürich (2021) emerge inoltre una forte correlazione tra la dimensione dell'azienda e la consapevolezza del pericolo rappresentato dai ciber-rischi. Anche la popolazione ritiene che le competenze digitali delle imprese siano molto diverse (Sotomo, 2022). In un recente sondaggio, il 78 per cento ha affermato che le aziende di maggiori dimensioni possiedono competenze digitali elevate. Ma, parlando delle PMI, soltanto il 45 per cento degli intervistati ritiene che le loro competenze digitali siano elevate. Per quanto riguarda la cibersicurezza, invece, l'87 per cento delle persone interpellate si aspetta che lo Stato faccia di più per proteggere le imprese dai ciberattacchi.

Come si può notare, le aziende attualmente starebbero investendo molto in misure di protezione tecnica, andamento accelerato durante la pandemia per garantire le condizioni necessarie al lavoro da casa, . Tuttavia continuano a essere riscontrate lacune dal punto di vista organizzativo. Le cosiddette «truffe del CEO», ad esempio, sono sempre più diffuse. Le misure della SNPC 2018–2022 sarebbero troppo poco efficaci per portare a un miglioramento generale delle misure di protezione delle PMI. La SNPC 2018–2022 ha

gettato delle buone basi attraverso vari provvedimenti (p. es. campo d'azione «Acquisizione di competenze e conoscenze», campo d'azione «Standardizzazione / regolamentazione», campo d'azione «Visibilità e sensibilizzazione»). Mancano tuttavia le misure e le risorse (finanziarie, organizzative, normative ecc.) per favorire una diffusione e un'applicazione su larga scala delle basi e delle best practice sviluppate.

L'inserimento delle imprese nella cerchia chiusa dei clienti dell'NCSC è ritenuto una misura molto efficace per favorire il loro coinvolgimento e questo dovrebbe portare, come outcome, a un aumento esponenziale del numero di imprese coinvolte. Inoltre, la pubblicazione di informazioni sugli incidenti gravi occorsi a imprese note potrebbe con molta probabilità avere anche un effetto di sensibilizzazione. In merito a questo argomento l'NCSC viene menzionato sempre più spesso nei media, anche grazie al supporto del delegato federale alla cibersicurezza, funzione istituita nel 2019.

Conclusione: attraverso la SNPC 2018–2022 l'economia non è riuscita a migliorare a sufficienza la propria protezione contro i ciber-rischi. Gli output della SNPC, soprattutto nel caso delle PMI, difficilmente hanno portato all'avvio di attività volte a migliorare la protezione di queste aziende.

5 Conclusioni sull'efficacia della SNPC

Le spiegazioni riportate di seguito rispondono alle domande generali della verifica dell'efficacia (valutazione sommativa).

5.1 Raggiungimento degli obiettivi strategici

Domanda: in che misura la SNPC 2018–2022 raggiunge gli obiettivi strategici definiti al suo interno?

La visione della SNPC 2018–2022 dovrebbe essere raggiunta perseguendo in modo coerente sette obiettivi strategici (v. Figura 1). Attraverso i campi d'azione, le misure e i piani di attuazione correlati, la SNPC 2018–2022 favorisce il raggiungimento degli obiettivi, contribuendo alla realizzazione della visione come illustrato di seguito.

— La SNPC 2018–2022 crea un contesto coerente di misure orientate al raggiungimento degli obiettivi. La definizione degli obiettivi e la struttura della strategia formano un insieme logico, orientato alle convenzioni istituzionali e tematiche e coerente con l'impatto potenziale.

— L'attuazione della SNPC 2018–2022 è stata in gran parte già completata, tutte le misure hanno portato a outcome rilevanti prima del termine del periodo di validità della strategia. Il lasso di tempo intercorso tra l'attuazione delle misure, con i relativi outcome, e l'impact atteso sulla protezione a livello informatico è troppo breve e non consente quindi osservazioni fondate o misurabili.

— In generale, gli outcome auspicati attraverso le misure sono stati giudicati adatti al raggiungimento degli obiettivi, ma non sono orientati in egual misura a tutti i gruppi di destinatari. Da un lato, vi sono notevoli differenze per quanto riguarda il contributo dato per il raggiungimento degli obiettivi sia tra i gruppi di destinatari che all'interno di uno stesso gruppo. Dall'altro, l'eterogeneità dei gruppi di destinatari rende più difficile il raggiungimento degli obiettivi strategici stabiliti dalla SNPC 2018–2022.

— Dall'analisi della SNPC 2018–2022 si rilevano lacune nella gestione strategica, nella pianificazione delle misure di attuazione e nelle risorse a disposizione. Di conseguenza, l'efficacia potenziale della strategia si riduce. Una misurazione poco attenta dell'efficacia a livello del campo d'azione e delle misure limita la capacità di reazione e quindi anche l'adeguamento delle misure volte a garantire una massimizzazione costante degli effetti.

— L'elevato dinamismo con cui si evolvono le ciberminacce (in particolare la forte crescita degli attacchi) può rappresentare un rischio per il raggiungimento degli obiettivi strategici, a meno che attraverso le misure della SNPC non si riesca ad aumentare la protezione della Svizzera in maniera adeguata e rendendola capace di adattarsi in modo dinamico.

Conclusione: la SNPC 2018–2022 è una strategia coerente con un piano di attuazione che sostiene il raggiungimento degli obiettivi strategici. La strategia è stata attuata secondo i programmi e portando ad outcome rilevanti, che però non hanno raggiunto tutti i gruppi di destinatari in egual misura. Attraverso interventi mirati (p. es. misurazione dell'efficacia e gestione strategica) è possibile incrementare ulteriormente l'efficacia delle misure di attuazione della SNPC.

5.2 Effetti

Domanda: in quale misura è stato possibile raggiungere gli effetti auspicati con le prestazioni fornite?

Gli effetti della SNPC 2018–2022 sotto forma di impact a lungo termine sulla società e sull'economia svizzere al momento non possono essere ancora misurati o dimostrati empiricamente in altro modo. Le valutazioni consolidate ottenute nel corso dei colloqui con le persone responsabili delle misure e i rappresentanti dei gruppi di destinatari nonché da recenti studi possono essere così riassunte:

— Finora gli effetti maggiori si sono registrati sulle infrastrutture critiche, sulle autorità e istituzioni nazionali nonché sulle autorità cantonali e sulle scuole universitarie. Finora economia e popolazione sono state interessate in misura contenuta o quasi per niente dagli outcome delle misure.

— All'interno del mondo economico vi sono forti differenze a seconda della gamma di attività e delle dimensioni aziendali. Mentre i gestori delle infrastrutture critiche e le grandi imprese operanti a livello internazionale sono riusciti ad aumentare la loro protezione in ambito informatico, la maggior parte delle PMI continua ad essere troppo poco protetta.

— Anche città e Comuni vengono ritenuti troppo poco protetti. Le misure della SNPC 2018–2022 li raggiungono a fatica. Le istituzioni cantonali integrate nella SNPC non sono in grado di trasferire efficacemente a città e Comuni gli output ottenuti attraverso le misure.

— Per quanto riguarda la popolazione come gruppo di destinatari, non è stato rilevato un aumento della protezione in ambito informatico riconducibile direttamente alle misure della SNPC 2018–2022. Le misure messe in atto non sono quasi mai rivolte direttamente alla popolazione.

— In generale, i canali e le capacità che la SNPC 2018–2022 ha a disposizione per far conoscere ai gruppi di destinatari gli outcome delle misure e spingerli a intraprendere iniziative volte a garantire un livello di sicurezza maggiore in ambito informatico sono troppo pochi. Questo quindi impedisce alle prestazioni fornite attraverso l'attuazione delle misure di dimostrare tutta la loro potenziale efficacia.

Conclusione: finora la SNPC 2018–2022 ha mostrato i propri effetti soprattutto sulle infrastrutture critiche, sulle autorità e istituzioni nazionali e cantonali nonché sulle grandi

aziende. Dal momento che la SNPC 2018–2022 è ancora in corso, non è possibile avere delle prove empiriche. Inoltre vi è motivo di credere che le PMI, le città e i Comuni nonché la popolazione non siano raggiunti in maniera significativa dalle misure in attuazione della SNPC e non siano supportati nello sviluppo delle misure volte a proteggerli in ambito informatico.

5.3 Efficienza

Domanda: qual è il rapporto tra l'impiego di mezzi e le prestazioni fornite con l'attuazione della strategia?

Facendo un confronto a livello internazionale, i mezzi impiegati per la SNPC 2018–2022 sono ridotti. In relazione alle performance è possibile affermare quanto segue.

- Le risorse impiegate sono state sufficienti per garantire gli outcome pianificati delle misure per i compiti principali in base al piano di attuazione entro il momento della verifica (autunno 2021). Questi outcome costituiscono i presupposti per la realizzazione dei potenziali effetti della SNPC 2018–2022.
- L'efficienza del metodo con cui i mezzi sono stati allocati viene criticata soprattutto perché
  - il numero elevato di misure e progetti di attuazione ha reso difficile concentrare le risorse;
  - in alcuni casi si è dovuto scegliere se destinare le risorse alle attività di progetto o alle attività operative. In questo modo però si possono mettere a rischio la capacità di agire e l'integrità di fronte alle ciberminacce durante lo svolgimento degli incarichi esecutivi;
  - la mancanza di risorse non ha permesso di trasferire in maniera adeguata le prestazioni fornite ai gruppi di destinatari.
- La richiesta di risorse aggiuntive in termini di personale per il restante periodo di validità della SNPC 2018–2022 è ritenuta giustificata e necessaria per garantire un'elevata qualità nello svolgimento degli incarichi (per le attività di progetto e le attività operative). Il numero esatto di personale aggiuntivo richiesto deve essere ancora deciso. È opportuno compiere una distinzione tra le attività di progetto e le attività continuative (p. es. elaborazione della casistica in corso).

Conclusione: la SNPC 2018–2022 finora è riuscita a portare a termine i propri compiti principali con le risorse a disposizione. L'allocazione delle risorse, tuttavia, potrebbe essere maggiormente orientata agli obiettivi di efficacia. Risulterebbe inoltre giustificato mettere a disposizione ulteriori risorse in termini di personale per il restante periodo nonché per le attività continuative.

6 Prospettive e raccomandazioni

Il ciberspazio è caratterizzato da un elevato dinamismo. La cibersicurezza deve quindi essere considerata un settore in costante evoluzione e predisposta a garantire in qualsiasi momento la capacità di agire e l'integrità di aziende, organizzazioni nonché soggetti pubblici e privati in base alle rispettive condizioni quadro, possibilità tecnologiche, direttive organizzative e situazione di minaccia contingente. L'aumento della protezione contro i ciber-rischi sarà un compito da portare avanti anche dopo il 2022. Pensando ai successivi cicli della strategia SNPC (p. es. 2023–2027) si è cercato di rispondere alla seguente domanda generale (valutazione formativa):

Domanda: in base alla verifica dell'efficacia, quali raccomandazioni possono essere fornite, da un lato, per la revisione della strategia e, dall'altro, per quanto riguarda il futuro impiego delle risorse finanziarie e di personale?

La verifica dell'efficacia evidenzia diversi fattori di successo critici a livello di contenuto e di organizzazione. Per fattori di successo critici si intendono le circostanze specifiche fondamentali per il raggiungimento dell'obiettivo generale della SNPC 2018–2022. Se non vi sono questi presupposti o se sussistono presupposti contrari, si hanno delle lacune che possono ostacolare in modo significativo l'efficacia della SNPC (secondo la definizione del Gabler Wirtschaftslexikon, www.wirtschaftslexikon.gabler.de, consultato il 22 gennaio 2022).

Partendo dai fattori di successo critici identificati è possibile formulare delle raccomandazioni su come migliorare la struttura già adeguata della SNPC e, di conseguenza, su come aumentare l'efficienza e l'efficacia per ottenere il migliore impact possibile. Le raccomandazioni seguono la struttura della SNPC attuale.

6.1 Processo e accettazione

Uno dei principali fattori di successo della SNPC 2018–2022 è il suo processo di elaborazione, tenutosi in maniera strutturata e con il coinvolgimento di diversi attori. Questo modo di procedere:

- permette di tenere ampiamente in considerazione elementi fondamentali nonché problematiche e abilità specifiche di singoli gruppi di destinatari;
- aumenta l'accettazione delle misure, poiché sviluppate congiuntamente;
- getta le basi per la futura partecipazione alla fase di attuazione, perché fin dall'inizio si è creato lo spirito collaborativo necessario;
- forma una rete che, per la diffusione di output, ha portato ad attività nei gruppi di destinatari che garantiscono gli effetti sperati.

Il processo di elaborazione della SNPC 2018–2022 ha funto da esempio quale «nuovo tipo di sviluppo» della strategia fondamentale. Le esperienze raccolte al termine della prima SNPC 2012–2017 sono state sfruttate in modo mirato per favorire un approccio più strategico e coinvolgere maggiormente molti attori nel secondo ciclo della strategia.

Raccomandazione: i vantaggi di un processo di elaborazione partecipativo dovranno essere sfruttati in modo mirato per l'ulteriore sviluppo della SNPC. Attraverso un processo efficiente e gestito in modo rigoroso, i vari titolari delle conoscenze saranno più propensi a collaborare.

6.2 Governance

La governance della SNPC, garantita da una struttura capillare con un CD, è ritenuta vantaggiosa per l'esecuzione della strategia. Con l'istituzione dell'NCSC, inoltre, sono state rafforzate le capacità operative di coordinamento e la gestione operativa di tematiche trasversali. Molti attori coinvolti ritengono che il CD non sia abbastanza efficace. A causa delle sue dimensioni, della sua organizzazione e della mancanza di una visione generale condivisa dai singoli membri, finora non è stato in grado di guidare in modo strategico. Le capacità del CD sono impiegate principalmente per il controlling delle misure. Le discussioni generali su argomenti strategici non vengono tenute in maniera sufficientemente esauriente.

Durante le interviste più volte è emersa la necessità di ridurre il numero di membri del CD e di definirne le priorità. Lo scambio tra tutte le persone coinvolte nell'attuazione della SNPC dovrebbe avvenire in modo formale e informale in seno ad altri comitati e organismi, lasciando che siano gli interessati stessi a organizzarsi autonomamente.

Raccomandazione: il CD dovrebbe essere riorganizzato sia dal punto di vista della sua organizzazione (in particolare riducendone i membri) che delle sue funzioni e compiti, al fine di aumentare le sue capacità di gestione strategica. Inoltre dovrebbero essere promosse ulteriori opportunità di interconnessione.

L'analisi degli effetti sui gruppi di destinatari ha evidenziato come all'interno di ciascun gruppo i destinatari siano stati raggiunti in modi molto diversi. Le maggiori difficoltà si sono riscontrate soprattutto nelle PMI, nelle autorità comunali e nella popolazione. La Confederazione ha difficoltà a entrare direttamente in contatto con queste realtà e quindi ha anche informazioni ridotte sulle loro problematiche ed esigenze attuali. Per migliorare la collaborazione e il trasferimento delle informazioni a livello operativo viene consigliata la realizzazione di «progetti ponte». L'importanza e l'efficacia di simili progetti potrebbero essere aumentate se gruppi di interesse di PMI, autorità comunali e Amministrazione fossero maggiormente coinvolti nelle misure strategiche della SNPC.

Raccomandazione: sarebbe opportuno valutare un maggior coinvolgimento delle PMI e delle autorità comunali nella governance della SNPC.

6.3 Obiettivi strategici

La verifica dell'efficacia mostra che, nel complesso, gli obiettivi strategici definiti dalla SNPC sono adeguati e idonei e si inseriscono in una struttura classica costituita da una visione, da obiettivi e da campi d'azione definiti per il loro raggiungimento. In aggiunta è stato definito un piano di attuazione, che concretizza le misure attraverso progetti di attuazione.

Alcuni hanno suggerito di assegnare alla visione della SNPC un orizzonte temporale più esteso rispetto ai precedenti cicli della strategia. In questo modo si garantirebbe anche un orientamento adeguato per i progetti a più lungo termine. Numerosi progetti di attuazione presenti nelle misure attuali, infatti, non potrebbero quasi essere realizzati con efficacia nel corso di un unico ciclo della strategia.

L'analisi dell'efficacia dimostra inoltre che non si pone la medesima attenzione nell'attuazione dei diversi obiettivi strategici. Una parte delle misure ha infatti obiettivi poco concreti e può essere inserita soltanto in un contesto generale. In alcuni casi, poi, dall'analisi emerge che non sarebbe possibile un'esecuzione indipendente. Quando gli obiettivi non sono definiti in modo chiaro è difficile focalizzarsi sulle misure (frammentazione, gruppi di destinatari poco chiari ecc.) e questo rende più complicata anche la misurazione e la valutazione degli effetti ottenuti. Per garantire una formulazione degli obiettivi e una misurazione dell'efficacia precise, una possibile soluzione può essere l'adozione della regola SMART (specifico, misurabile, riconosciuto, realistico, scadenzato).

Per riunire in modo efficace attività e risorse è importante che a tutti i livelli gli obiettivi siano definiti in modo semplice e comprensibile. Nel caso della SNPC 2018–2022 non sempre è così. Mentre la visione e gli obiettivi strategici sarebbero definiti in modo concreto, gli attori coinvolti descriverebbero gli obiettivi di diversi progetti in maniera troppo poco concreta.

Raccomandazione: gli obiettivi devono essere formulati nel modo più concreto e indipendente possibile a tutti i livelli della strategia, compresi nei progetti di attuazione.

Uno dei punti deboli della SNPC 2018–2022 è stato il trasferimento degli output ai gruppi di destinatari. Questo nonostante nell'ambito della SNPC 2018–2022 sia stato elaborato un piano di comunicazione e le capacità di comunicazione decisamente più elevate abbiano garantito una visibilità maggiore e misurabile di queste tematiche e dell'NCSC tra i gruppi di destinatari e nell'opinione pubblica.

Molti dei partner intervistati, tuttavia, ritengono che nell'ambito della comunicazione sia necessario un impegno ulteriore. La visibilità dovrebbe essere aumentata e i messaggi dovrebbero essere lanciati in modo più conciso e d'impatto prendendo spunto, ad esempio, dalle campagne in ambito sanitario. Le attività in programma e le tappe fondamentali raggiunte dovrebbero essere «vendute» ancora meglio, mentre determinati progetti e successi avere una risonanza adeguata nei media. Gli intervistati hanno poi proposto che le attività di comunicazione relative al tema dei ciber-rischi vengano svolte in modo congiunto e più coordinato tra i diversi uffici federali. Inoltre i «key player», in particolare

l'economia, dovrebbero svolgere un ruolo di moltiplicatori. Maggiori sforzi nell'ambito della comunicazione dovrebbero essere rivolti alla popolazione utilizzando messaggi che catturano l'attenzione, come quelli utilizzati nelle campagne della Suva o nelle campagne informative della Confederazione sul coronavirus.

Raccomandazione: gli sforzi nell'ambito della comunicazione devono essere potenziati, integrati e coordinati, prendendo in considerazione la possibilità di inserire un ulteriore obiettivo strategico, ovvero «trasferimento e comunicazione».

6.4 Gruppi di destinatari

La SNPC può dare i suoi frutti unicamente rivolgendosi in modo adeguato ai gruppi di destinatari. Soltanto le attività dei gruppi di destinatari, infatti, portano a una maggiore protezione della Svizzera contro i ciber-rischi (vedi modello di efficacia Figura 2). È dunque importante differenziare i vari gruppi di destinatari in base alle sfide che devono affrontare e fare in modo che le misure scelte abbiano un effetto diretto sul maggior numero possibile di attori.

Per ottenere il massimo dai risultati delle misure è necessario coinvolgere nelle fasi di pianificazione e attuazione direttamente i rappresentanti dei gruppi di destinatari. La SNPC 2018–2022 ha coinvolto direttamente pochi gruppi di destinatari con un elevato valore strategico attraverso i loro rappresentanti. Quando i gruppi di destinatari sono considerati soltanto dei beneficiari o dei soggetti interessati dalle misure, solitamente gli effetti ottenuti non sono stati giudicati sufficienti (come nel caso della popolazione e in parte dell'economia).

Raccomandazione: le misure della SNPC dovranno soddisfare nel modo più diretto possibile le esigenze dei gruppi di destinatari. I gruppi di destinatari dovranno essere coinvolti in modo adeguato (in particolare la popolazione) nei progetti di attuazione.

È necessario che nella pianificazione e nell'attuazione delle misure concrete Confederazione, Cantoni e città/Comuni operino in modo coordinato. Ad esempio, l'introduzione di un piano di attuazione cantonale da parte della RSS, che prevede anche lo sviluppo di un modulo di e-learning volto a sensibilizzare i collaboratori cantonali in merito ai ciber-rischi, ha promosso la realizzazione e la diffusione dei progetti di attuazione.

Raccomandazione: occorrerebbe valutare se fosse opportuno che la SNPC crei dei «progetti ponte» mirati che coinvolgono tutti e tre i livelli statali.

6.5 Piano di attuazione

Il piano di attuazione, creato insieme alla SNPC 2018–2022, si è rivelato un fattore importante per l'avvio rapido delle attività e il perseguimento degli obiettivi strategici. In molti lo considerano però troppo rigido. In tanti poi ritengono che la strategia alla base della visione della SNPC dovrebbe essere perseguita per un periodo più lungo rispetto ai

quattro anni previsti e che per l'attuazione potrebbe essere impiegato un piano di attuazione a rotazione. Alcuni, inoltre, ritengono che un piano di attuazione più flessibile potrebbe spingere un maggior numero di attori a partecipare.

Raccomandazione: la struttura e le modalità di esecuzione del piano di attuazione dovrebbero essere più flessibili e, se necessario, organizzate su cicli di durata maggiore.

All'introduzione di un piano di attuazione più flessibile o a rotazione dovrebbero però essere abbinati anche una misurazione dell'efficacia e un controlling maggiori (v. raccomandazione al successivo punto 6.6) nonché una gestione strategica (v. raccomandazione al punto 6.2).

6.6 Misure e misurazione dell'efficacia

Le 29 misure riflettono la varietà delle sfide e trattano quindi numerosissime tematiche. Il numero elevato di misure può anche far pensare che attraverso la SNPC si siano messe insieme in modo casuale tante idee diverse.

Organizzando le misure in modo più strutturato e classificandole per tipologia, ad esempio in misure chiave e misure accessorie, sarebbe più semplice sottolineare i punti essenziali e mettere in risalto le interazioni che si intendono ottenere. Un tipo di classificazione possibile potrebbe prevedere come categorie «misure immediate», «best practice», «progetti di regolamentazione», «progetti trasversali di base» e «progetti pilota». Inoltre bisogna tenere conto che esistono differenze sostanziali tra i progetti di durata limitata e i progetti che mirano alla creazione di un'attività operativa e al suo consolidamento. Per le misure chiave, infine, potrebbe essere definito anche un cosiddetto livello di ambizione e le misure accessorie potrebbero essere valutata in base a quanto contribuiscono all'attuazione delle misure chiave.

Raccomandazione: in futuro le misure e i rispettivi progetti di attuazione dovranno essere differenziati secondo criteri come il tipo di misura e gli obiettivi definiti, la loro scadenza e il livello di ambizione.

Diversi partner intervistati hanno sollevato altre tematiche e questioni che dovranno essere affrontate in modo mirato nel prossimo ciclo strategico attraverso specifiche misure.

— *Presa in considerazione dei rischi legati alla supply chain*: la Svizzera è molto dipendente dalle catene di fornitura globali. Le produzioni just in time, i rapporti di fornitura complessi e le giacenze di magazzino minime rendono le catene di approvvigionamento molto vulnerabili in caso di guasti, interruzioni o attacchi. La gestione sistematica dei rischi connessi alla supply chain deve essere trattata come un tema a se stante o considerata un ulteriore fattore che influisce sulle attuali misure. In aggiunta è necessario tenere conto anche di come questo sia legato agli sforzi nell'ambito della politica estera e del dialogo multilaterale, così da prendere in considerazione le catene di approvvigionamento nella loro dimensione globale.

— *Rafforzamento della formazione*: molti ritengono che fare in modo che tutte le persone coinvolte dei vari gruppi di destinatari siano in grado di affrontare in modo adeguato i ciber-rischi rappresenti un fattore chiave. Nel prossimo ciclo strategico dovrà quindi essere data maggiore importanza alla formazione e alla formazione continua.

— *«Ecosistema cyber» svizzero*: i ciber-rischi rappresentano una sfida di carattere globale che deve essere affrontata attraverso misure tecniche e organizzative. Un'economia adeguatamente protetta e con un'elevata integrità e capacità di agire in caso di incidenti informatici vanta un vantaggio competitivo a livello mondiale. Inoltre lo sviluppo sistematico delle conoscenze in un «ecosistema cyber» maturo permette di creare nuove opportunità di mercato per l'esportazione di tecnologie e servizi ad alta intensità di conoscenze. Integrando un «ecosistema cyber» nella SNPC si inseriscono al suo interno le opportunità create dalla strategia stessa.

Raccomandazione: la SNPC deve integrare nelle sue misure ulteriori temi. I più urgenti da trattare per potersi concentrare sulle relative opportunità sono i rischi legati alla supply chain, la formazione e l'«ecosistema cyber».

Le misure della SNPC 2018–2022 non hanno un sistema di misurazione dell'efficacia sistematico. La gestione strategica finora si è basata sul monitoraggio dell'attuazione. Inoltre, in alcuni casi misurare l'efficacia delle misure è anche più difficile perché gli obiettivi sono definiti in modo poco concreto e il loro livello di ambizione non è mai precisato. Vi sono però delle ragioni ben precise. Molti dei soggetti coinvolti ritengono che la definizione di obiettivi misurabili e la misurazione costante dell'efficacia delle misure sia un fattore di successo molto importante. La misurazione dell'efficacia rappresenta un aiuto per la gestione strategica e l'allocazione delle risorse della SNPC. La misurazione dell'efficacia di ognuna delle singole misure consente di avere sempre un quadro generale sull'efficacia complessiva della strategia.

Nell'ambito della Strategia Ciber DDPS le riflessioni sulla misurazione dell'efficacia, ad esempio, vengono formulate sulla base di gradi di maturità e un approccio simile viene utilizzato anche nella Cyber-Security Capacity Review per la Svizzera (University of Oxford, 2020). Questi approcci scientifici riconosciuti possono essere utilizzati anche per un confronto a livello internazionale.

Raccomandazione: in futuro la misurazione dell'efficacia dovrà essere un elemento fisso della pianificazione della strategia e delle misure. Nel pianificare i metodi di misurazione dell'efficacia si dovranno sfruttare i vantaggi di un processo di elaborazione collaborativo nonché le esperienze maturate nell'ambito delle strategie «speculari» dei dipartimenti coinvolti e del piano di attuazione della SNPC del Cantone.

6.7 Risorse

I punti 2.3 (Risorse) e 5.3 (Efficienza) dimostrano che le risorse impiegate per l'attuazione della SNPC 2018–2022 sono adeguate. Con le risorse disponibili finora è stato possibile svolgere i compiti principali della SNPC 2018–2022.

Tuttavia si sono verificate carenze di risorse e si auspica un aumento mirato del personale. Per poter rafforzare l'organico in breve tempo è necessario ripensare diverse condizioni quadro. Da un lato deve essere chiaro quale obiettivo e quale livello di ambizione si vuole raggiungere. Devono dunque essere stabiliti obiettivi chiari e misurabili, associati, se necessario, a indicatori di riferimento che permettano di monitorare le performance delle attività («key performance indicators»). In questo modo sarà più semplice capire quali competenze e qualifiche sono necessarie per raggiungere l'obiettivo.

Dall'altro deve essere possibile impiegare le risorse dove c'è maggior bisogno in modo più facile rispetto a oggi. I cicli di pianificazione pluriennali e la gestione decentralizzata del budget rendono più difficile l'allocazione flessibile e veloce delle risorse. A questo riguardo è necessario analizzare in modo critico i processi di pianificazione e preventivazione dell'Amministrazione federale nell'ambito della rete della SNPC. In particolare, si dovrà verificare se i mezzi fondamentali o i budget di progetto debbano essere gestiti in misura maggiore dal Comitato ristretto Ciber o dal CD.

Raccomandazione: gli obiettivi e i livelli di ambizione devono essere formulati in modo da essere costantemente misurabili, per poter individuare con maggiore precisione le risorse necessarie. Il Comitato ristretto Ciber o il CD dovranno occuparsi in misura maggiore della gestione dei budget di progetto, in modo tale che le risorse possano essere assegnate più facilmente.

In ogni caso vi è sicuramente bisogno di un maggior numero di esperti in materia in tutti i gruppi di destinatari e a tutti i livelli. L'elevato dinamismo con cui si evolve il settore informatico richiede una costante formazione continua. Anche nel prossimo ciclo strategico sarà quindi necessario concentrarsi in modo chiaro sulla formazione, sulla formazione continua e sul cosiddetto capacity building.

Raccomandazione: il pool di esperti dovrebbe essere ampliato attraverso programmi mirati di formazione e formazione continua.

Allegato

A-1 Dettagli sulla procedura

Analisi dei documenti e interviste ai responsabili delle misure

N.	Metodo/ fase di lavoro	Periodo	Dettagli	Informazioni/ conoscenze acquisite
1	Analisi dei documenti	settembre-novembre 2021	Procedura basata su una griglia di domande Classificazione dei documenti in sviluppo della strategia, pianificazione dell'attuazione e pianificazione delle risorse Analisi approfondita dei documenti specifici delle misure	Preparazione delle interviste brevi con i responsabili delle misure Applicazione di output, outcome e impact per ogni tappa fondamentale Suggerimenti sulle domande da porre a tutti i livelli di efficacia
Segreteria NCSC	*Controlling dell'attuazione da parte della segreteria*	*settembre-ottobre 2021*	*Rilevazione e valutazione in base all'andamento del controlling trimestrale all'attenzione del CD*	*Controlling dell'attuazione costante*
	Rilevazione delle risorse da parte della segreteria	settembre-novembre *2021*	*Rilevazione delle risorse richieste, assegnate e impiegate* *Interrogazione scritta da parte della segreteria NCSC*	*Panoramica delle risorse impiegate per misura*
2	Interviste sulla base di linee guida	*settembre-ottobre* 2021	Primo contatto con i responsabili delle misure come da accordi con il CD Organizzazione degli appuntamenti e, se necessario, consegna di documenti specifici 10-12 interviste telefoniche/video (max. 1 h) secondo le linee guida rivolte ai responsabili delle misure Verbale dell'intervista per motivi interni (non inviato all'NCSC)	Effetti della SNPC percepiti da una prospettiva interna Fattori che hanno promosso/frenato l'efficacia Sfide nell'attuazione delle misure Chiarimento di eventuali indicazioni nell'ambito del controlling dell'attuazione
3	*Rapporto intermedio*	*fino a metà novembre 2021*	– *Elaborazione della percezione dall'interno e dall'esterno da parte degli incaricati dell'elaborazione del rapporto intermedio*	*Risultati intermedi per gli incaricati* *Preparazione di possibili temi per i workshop*
4	Feedback NCSC e CD	*fine novembre 2021*	– Relazione al CD – Feedback consolidati da parte della segreteria NCSC – Riunione con econcept/EBP	Convalida dei risultati intermedi Suggerimenti su temi da approfondire/chiarire

Interviste/focus group rappresentanti gruppi di destinatari

N.	Metodo	Periodo	Dettagli	Informazioni/ conoscenze attese
1	Analisi del gruppo di destinatari	agosto 2021	Definizione del gruppo di destinatari Analisi degli attori per influenza Selezione degli attori (vedi sotto)	Selezione degli attori idonei tenendo conto della percezione dall'esterno da diverse prospettive
2	CD (presentazione/domande di chiarimento)	14.9.2021	Primo contatto con il CD Spiegazione/discussione/rappresentazione dell'analisi dei gruppi di destinatari e selezione dei partner per l'intervista Chiarimento sul supporto per i contatti da parte del CD	Accettazione del progetto Selezione finale dei rappresentanti dei gruppi di destinatari Referenti dei gruppi di destinatari
3	Interviste sulla base di linee guida	settembre-novembre 2021	Lettera di accompagnamento NCSC (bozza di econcept/EBP) Primo contatto con gli interlocutori, a seconda di persona/ufficio, tramite NCSC o econcept/EBP Contatto per definizione dell'appuntamento tramite econcept/EBP Invio delle linee guida per l'intervista, adattate in base all'attore Esecuzione/verbalizzazione dell'intervista (circa 45', telefonica/online) Verbale dell'intervista per motivi interni (non inviato all'NCSC)	Effetti della SNPC percepiti da una prospettiva esterna Fattori che hanno promosso/frenato l'efficacia Difficoltà nell'integrazione delle misure della SNPC all'interno delle proprie attività
4	Focus group commissione per la cibersicurezza di digitalswitzerland	novembre 2021	Pianificazione in collaborazione con digitalswitzerland Linee guida per la discussione Esecuzione (2 h, videoconferenza) Verbale dell'intervista per motivi interni (non inviato all'NCSC)	Effetti della SNPC percepiti da una prospettiva esterna Fattori che hanno promosso/frenato l'efficacia Difficoltà nell'integrazione delle misure della SNPC all'interno delle proprie attività
5	*Rapporto intermedio*	*fino a metà novembre 2021*	*Elaborazione della percezione dall'interno e dall'esterno da parte degli incaricati*	*Risultati intermedi per gli incaricati* *Preparazione di possibili temi per i workshop*
6	Feedback NCSC e CD	*fine novembre 2021*	– Relazione al CD – Feedback consolidati da parte della segreteria NCSC Riunione con econcept/EBP	Convalida dei risultati intermedi Suggerimenti su temi da approfondire/chiarire

A-2 Linee guida per le interviste

Linee guida per le interviste alle persone responsabili delle misure

Apertura

Funzione: per prima cosa potrebbe spiegarci quali sono la sua funzione e le sue responsabilità in relazione all'attuazione della SNPC 2018–2022?

Valutazione generale

Strategia e basi: in generale in che misura ritiene che la SNPC 2018–2022 sia adeguata a proteggere correttamente la Svizzera dai ciber-rischi? Le questioni base rilevanti sono state prese debitamente in considerazione? A suo avviso esistono delle lacune che, in futuro, dovranno essere colmate?

Misure in generale: in che misura ritiene che le 29 misure nel loro complesso siano adeguate per raggiungere gli obiettivi della strategia?

Effetti sui gruppi di destinatari: dal suo punto di vista la SNPC 2018–2022 ha permesso di ottenere gli effetti auspicati sui gruppi di destinatari? Perché sì/no?

Ulteriori effetti: secondo lei la SNPC 2018–2022 ha avuto altri effetti (non intenzionali)?

Attuazione della SNPC 2018–2022

Misure sotto la sua responsabilità: come valuta i seguenti aspetti in relazione all'obiettivo di proteggere la Svizzera contro i ciber-rischi? Quanto sono adeguati a raggiungere questo obiettivo?

Progetti di attuazione nell'ambito delle misure (cfr. pianificazione dell'attuazione)?

Livello di ambizione (stato previsto al 2022) in relazione alle misure?

Risorse: come valuta le risorse a disposizione per l'attuazione delle sue misure ed, eventualmente, anche per altri fini?

Strutture e processi: in che misura ritiene che le strutture e/o i processi siano efficaci ed efficienti in relazione:

all'attuazione delle sue misure?

alla collaborazione all'interno del suo servizio/della sua divisione?

alla collaborazione all'interno del CD/con l'NCSC?

altri eventuali argomenti?

Potenziali di ottimizzazione

Potenziali di ottimizzazione: dove a suo avviso vi è un possibile margine di (ulteriore) ottimizzazione per quanto riguarda:

la strategia SNPC 2018–2022 (p. es. obiettivi)?

i campi d’azione (p. es. coerenza reciproca)?

le misure (p. es. adeguatezza)?

i progetti di attuazione (p. es. ulteriori progetti)?

le tappe fondamentali?

altro?

Conclusione

Infine: ci sono altre osservazioni che vorrebbe fare?

Grazie per l’intervista!

Linee guida per le interviste ai rappresentanti dei gruppi di destinatari

Apertura

1 **Funzione**: per prima cosa potrebbe spiegarci le sue responsabilità per quanto riguarda la sicurezza informatica all'interno della sua organizzazione/della sua azienda/del suo servizio?

2 **Rischio e vulnerabilità**: come valuta i seguenti aspetti?

2.1 Rischio derivante dalle ciberminacce per la sua organizzazione/la sua azienda/il suo servizio [*solo per i rappresentanti di infrastrutture critiche/economia:* e per il suo ramo/settore] e

2.2 la vulnerabilità in caso di attacchi informatici?

Come è cambiata la sua valutazione dei rischi e della vulnerabilità dal 2018?

Rischi, vulnerabilità, strategia

3 **SNPC 2018–2022**: quali effetti o quale influenza ha la Strategia nazionale per la protezione della Svizzera contro i ciber-rischi (SNPC) 2018–2022 sulla sua organizzazione/la sua azienda/il suo servizio [*solo per i rappresentanti di infrastrutture critiche/economia:* e per il suo ramo/settore]? Utilizza la strategia come uno strumento di lavoro? Perché sì/no?

4 **Requisiti**: quali sono i requisiti che deve soddisfare una strategia per la protezione della Svizzera contro i ciber-rischi alla luce dei rischi e delle vulnerabilità specifiche? A suo avviso quali aspetti dovrebbero essere regolamentati e quali no?

5 **Valutazione SNPC 2018–2022**: alla luce di questo, come valuta in generale la SNPC 2018–2022?

6 **Valutazione dei campi d'azione e delle misure**: e come valuta i campi d'azione e le misure identificate per proteggere la Svizzera contro i ciber-rischi? [*solo per i rappresentanti di infrastrutture critiche/economia:* a suo avviso in che misura contribuiscono a proteggere il suo ramo/settore?]

Attuazione della strategia

7 **Effetti della SNPC 2018–2022**: la strategia 2018–2022 ha portato a cambiamenti concreti nella sua organizzazione/nella sua azienda/nel suo servizio [*solo per i rappresentanti di infrastrutture critiche/economia:* e nel suo ramo/settore]? Se sì, quali?

8 **Fattori di influenza (driver + freno)**: quali circostanze o condizioni quadro supportano, secondo lei, gli effetti della SNPC 2018–2022? E quali li ostacolano?

9 **Potenziali di ottimizzazione**: vi sono quindi delle esigenze concrete di miglioramento o ritiene vi sia la possibilità di migliorare la strategia stessa, i processi o le strutture? Se sì, quali?

Conclusione

10 **Aspettative**: cosa si aspetta da una strategia per la protezione della Svizzera contro i ciber-rischi in generale? Cosa si attende dagli organi responsabili?

11 **Infine**: ci sono altre osservazioni che vorrebbe fare?

Grazie per l’intervista!

A-3 Panoramica dei colloqui con i responsabili delle misure

N.	Nome	Cognome	Organizzazione	1	2	3	4	5	6	7	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29
1	Philipp	Kronig	SIC				X																	X	X						
2	Stefan	Brem	UFPP					X																							
	Giorgio	Ravioli	UFPP																												
3	André	Duvillard	DDPS							X																					
4	Daniel	Caduff	UFAE					X																							
	Christophe	Hauert	Cyber-Safe																												
5	René	Dönni Kuoni	UFCOM									X																			
	Nicolas	Rollier	UFCOM																												
6	Yanis	Callandret	fedpol																	X	X	X	X								
	Céline	Aubry	PGF/fedpol																												
7	Roger	Michlig	DDPS																							X					
8	Jonas	Grätz	DFAE																								X	X	X		
	Daniel	Seiler	DFF																												
9	Claudio	Stricker	CDDGP							X											X	X	X								
10	Robert	Flück	Cdo Cyber																						X	X					
11	Patrick	Schaller	PFZ		X	X		X	X	X		X	X											X							
	Imad	Aad	PFL		X	X		X	X	X		X	X											X							
12	Martin	Leuthold	SWITCH													X															
13	Pascal	Lamia	NCSC																												
	Manuel	Sutter	NCSC			X				X	X		X	X	X	X	X	X	X											X	
	Marco	Willisch	NCSC																												
14	Dominique	Trachsel	NCSC						X																						X
15	Monica	Ratté	NCSC							X																					

Tabella 13: elenco dei colloqui tenuti con i responsabili delle misure (*ancora da eseguire)

A-4 Panoramica dei colloqui con i gruppi di destinatari

N.	Nome	Cognome	Organizzazioni	Stato
1	Christoph	Niederberger	Associazione dei Comuni Svizzeri (ACS)	eseguito
2	Erich	Herzog	economiesuisse	eseguito
	Andreas W.	Kälin	digitalswitzerland	eseguito
	Christian	Grasser	Schweizerischer Verband der Telekommunikation (asut)	eseguito
	Thomas	Holderegger	UBS	eseguito
	Raphael	Reischuk	Zühlke	eseguito
2	Markus	Trutmann	H+ Gli ospedali svizzeri	eseguito
	Stefan	Trachsel	Servizio sanitario coordinato (SSC)	eseguito
4	Andy	Fluetsch	UPC/Salt	eseguito
5	Roger	Schneeberger	CDDGP	eseguito
6	Patric	Graber	Consiglio dei PF	eseguito
8	Philippe	Vuilleumier	Swisscom	eseguito
10	Serdar	Cünal Rütsche	Corpo di polizia del Cantone di Zurigo	eseguito
	Stefan	Walder	Ministero pubblico del Cantone di Zurigo	eseguito
11	Bertrand	Schnetz	Polizia criminale del Cantone del Jura	eseguito
12	Gunthard	Niederbäumer	Associazione Svizzera d'Assicurazioni (ASA)	eseguito
	Maya	Bundt	SwissRE	eseguito
13	Nicole	Wettstein	Accademia svizzera delle scienze tecniche (SATW)	eseguito
	Umberto	Annino	Presidente dell'Advisory Board Cybersecurity SATW	eseguito
14	Christophe	Hauert	Cyber-Safe	eseguito con respons. misure
15	Olivier	Crochat	C4DT	eseguito con respons. misure
	Imad	Aad		
16	Alain	Gut	IBM, presidente di Swiss Cyber Experts	eseguito

Tabella 14: lista delle organizzazioni rappresentanti dei gruppi di destinatari

A-5 Output in base alle tappe fondamentali

CA	Misura	Progetto di attuazione (output)	Outcome
Acquisizione di competenze e conoscenze	M1: Individuazione precoce di tendenze e tecnologie e acquisizione delle conoscenze	Creazione di un sistema di monitoraggio delle tecnologie e del mercato Valutazione degli sviluppi tecnologici e stesura di rapporti nel quadro dell'analisi delle tendenze	– Identificazione precoce di tendenze e tecnologie nel settore delle TIC – Identificazione precoce delle opportunità e dei rischi derivanti – Trasferimento delle informazioni agli attori di economia, politica e società
	M2: Ampliamento e promozione delle competenze di ricerca e formazione	Aggiornamento dell'analisi del fabbisogno di formazione ed eliminazione delle lacune esistenti nell'offerta Creazione di un centro comune di ricerca e di supporto per la cibersicurezza con i PFZ e PFL Attuazione dei progetti di ricerca del Cyber Defence Campus Promozione della ricerca interdisciplinare e della formazione in materia di cibersicurezza attraverso la creazione di una rete informale Promozione dell'«hackeraggio etico» mediante la promozione di eventi già consolidati	– Analisi del fabbisogno in termini di formazione delle competenze sui ciber-rischi – Valutazione dell'integrazione dei temi legati ai ciber-rischi nei percorsi formativi delle scuole universitarie e promozione dei talenti nel campo dell'«hackeraggio etico» – Rafforzamento della ricerca di base e applicata – Individuazione delle possibilità di promozione della ricerca interdisciplinare – Sviluppo di competenze e conoscenze nell'ambito della ciberdifesa del DDPS attraverso il campus CYD
	M3: Creazione di condizioni quadro vantaggiose per un'economia della sicurezza delle TIC innovativa in Svizzera	Creazione di un «Ecosistema della cibersicurezza» mediante il Centro di competenza per la cibersicurezza Approntamento di strumenti di promozione per progetti innovativi Creazione di centri di innovazione Creazione di un «think tank» per la cibersicurezza	– Promozione della Svizzera come sede interessante per le aziende nel campo della sicurezza delle TIC – Rafforzamento degli scambi tra economia e ricerca – Creazione di un ambiente favorevole allo sviluppo di innovazioni e start-up
Situazione di minaccia	M4: Rafforzamento delle capacità di valutazione e rappresentazione delle ciberminacce	Identificazione dei gruppi target e delle loro esigenze in relazione alla situazione di minaccia Definizione del catalogo di prodotti per ogni gruppo target Identificazione e creazione delle fonti e delle risorse produttive necessarie	– Preparazione di un quadro completo sulla situazione informatica con rappresentazione ed elaborazione della situazione di minaccia all'attenzione di autorità, gestori di infrastrutture critiche, imprese e popolazione – Sviluppo delle capacità per rilevare in modo sistematico e costante gli incidenti informatici – Sistematizzazione dell'OSINT, che serve da base per la raccolta delle informazioni – Intensificazione dello scambio di informazioni tra autorità preposte al perseguimento penale, esperti nell'ambito della cibersicurezza, esercito, SIC, economia e Cantoni
Gestione della resilienza	M5: Miglioramento della resilienza delle TIC delle infrastrutture critiche	Attuazione dei progetti previsti e in corso per rafforzare la resilienza nei sottosettori critici Aggiornamento delle analisi dei rischi e delle vulnerabilità Istituzione di un gruppo di lavoro accademico per la cibersicurezza	– Applicazione delle misure per migliorare la resilienza delle TIC dei sottosettori critici coinvolgendo le principali autorità di regolamentazione e gli uffici specializzati – Aggiornamento periodico delle analisi e delle misure

CA	Misura	Progetto di attuazione (output)	Outcome
	M6: Miglioramento della resilienza delle TIC all'interno dell'Amministrazione federale	Sviluppare disposizioni di sicurezza per metodi agili di progetto Campagna di sensibilizzazione nell'Amministrazione federale Sicurezza nella trasmissione dei dati attraverso tecnologie nuove: fase di test SCION Security Operations Center UFIT Creazione di un'interfaccia con il settore dei politecnici federali	– Miglioramento della resilienza delle TIC nell'Amministrazione federale
	M7: Scambio di conoscenze e creazione di basi per migliorare la resilienza delle TIC nei Cantoni	Scambi permanenti tra Cantoni e Centro di competenza per la cibersicurezza Svolgimento annuo della «Ciber-Landsgemeinde» Sviluppo e diffusione di disposizioni di sicurezza comuni alla Confederazione e ai Cantoni Creazione di un'interfaccia con il settore dei politecnici federali	– Creazione di una rete delle autorità al fine di effettuare uno scambio di esperienze e gettare basi comuni per rafforzare la resilienza delle TIC all'interno dei Cantoni – Supporto reciproco e individuazione di una procedura coordinata da parte delle autorità di Confederazione e Cantoni
Standardizzazione / regolamentazione	Valutazione e introduzione di standard minimi	Sviluppo e attuazione di standard minimi per migliorare la resilienza delle TIC Sviluppo e approntamento di ausili per le PMI	– Elaborazione e introduzione di standard minimi TIC verificabili – Verifica delle organizzazioni e delle attività per le quali gli standard dovrebbero essere vincolanti
	M9: Verifica dell'obbligo di notifica dei ciberincidenti e decisione in merito alla relativa introduzione	Studio dei modelli di massima degli obblighi di notifica Dibattito di principio con il mondo economico e le autorità	– Verifica dell'obbligo di notifica dei ciberincidenti e decisione in merito alla relativa introduzione
	M10: Internet governance globale	Gruppo di alto livello del Segretario generale delle Nazioni Unite per la cooperazione digitale Piattaforme di scambio multistakeholder per il coordinamento a livello nazionale	– Introduzione di un regolamento internazionale relativo all'utilizzo e allo sviluppo di Internet che sia conciliabile con gli ideali svizzeri di libertà, democrazia e responsabilità (individuale), servizio di base, pari opportunità, sicurezza, diritti umani e stato di diritto
	M11: Acquisizione di competenze da parte degli uffici specializzati e delle autorità di regolamentazione	Creazione di un pool di esperti interdipartimentale in materia di cibersicurezza a sostegno degli uffici specializzati Rafforzamento dei progetti di standardizzazione con il supporto delle scuole universitarie Contributo della Svizzera ad ancorare il tema della cibersicurezza nella politica finanziaria internazionale	– Rafforzamento della sicurezza informatica – Creazione di un pool di esperti per l'elaborazione di misure mirate, compresi eventuali interventi regolatori
Gestione degli incidenti	M12: Potenziamento di MELANI come partenariato pubblico-privato per i gestori di infrastrutture critiche	Ampliamento mirato della cerchia chiusa di clienti Sviluppo e ampliamento della gamma di servizi e prodotti Ampliamento dell'attuale piattaforma di scambio	– Potenziamento di MELANI (piattaforma per lo scambio di informazioni) – Coinvolgimento di tutti i settori nello scambio di informazioni – Garanzia delle qualità precedenti e definizione chiara dell'accesso
	M13: Creazione di servizi per tutte le imprese	Creazione di un punto di contatto nazionale per i ciber-rischi	– Sostegno all'economia svizzera tramite MELANI – Ampliamento dei gruppi di destinatari per MELANI

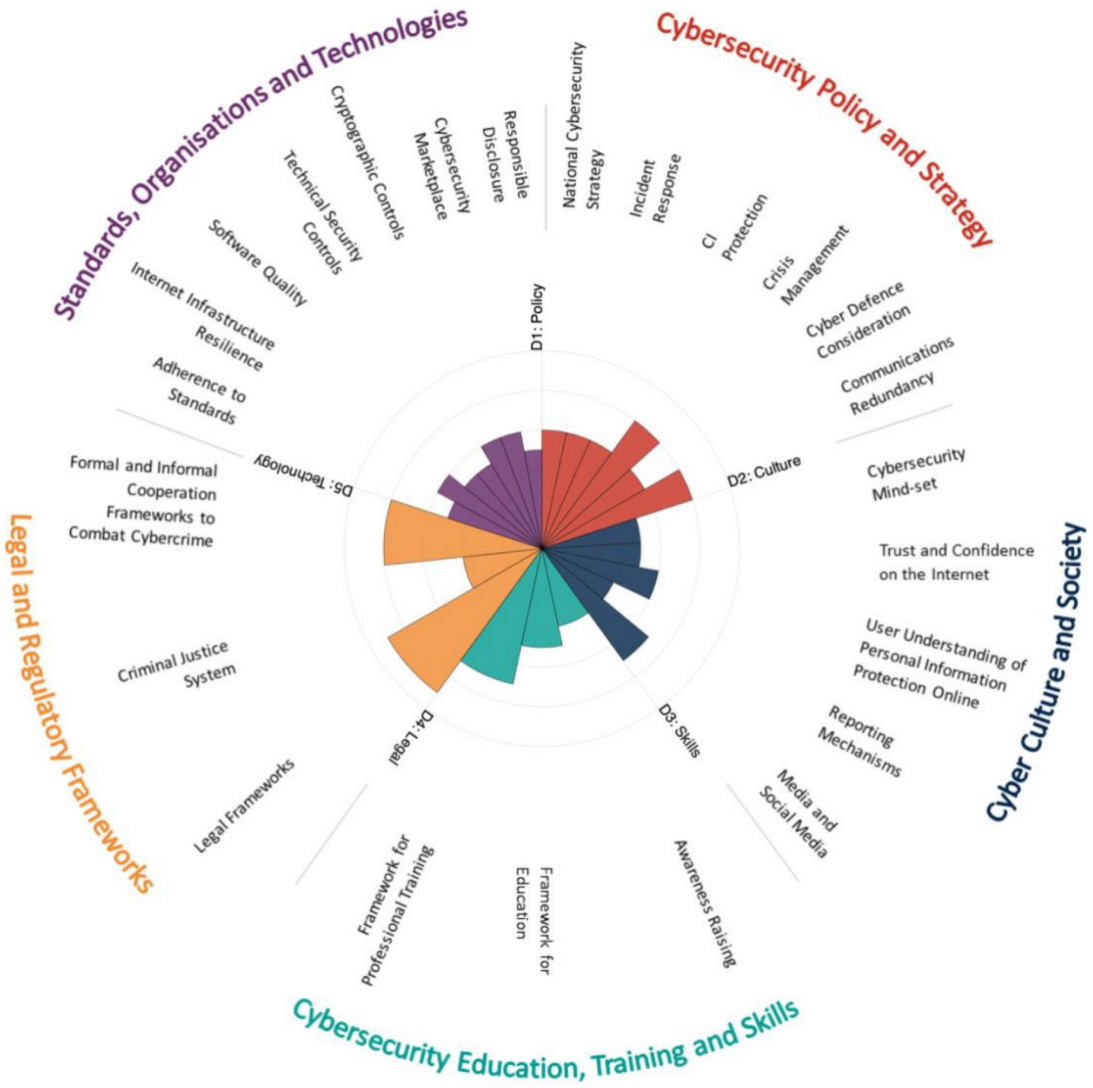
CA	Misura	Progetto di attuazione (output)	Outcome
		Pubblicazione di buone pratiche per la gestione degli incidenti e di valutazioni tecniche Informazione tempestiva mediante l'app Alertswiss in caso di incidente	– Sviluppo di un'offerta di servizi nell'ambito della prevenzione e della gestione degli incidenti
	M14: Collaborazione della Confederazione con uffici e centri di competenza rilevanti	Panoramica dei SOC attualmente operativi con i rispettivi interlocutori Scambio di informazioni con i CERT e i SOC	– Rafforzamento della collaborazione e dello scambio su MELANI tra gli organi interessati all'interno di Confederazione e Cantoni
	M15: Processi e basi della gestione degli incidenti	Elaborazione di un'ordinanza in materia di cibersicurezza Predisposizione di un processo di gestione degli incidenti per l'Amministrazione federale	– Standardizzazione delle modalità di gestione degli incidenti all'interno dell'Amministrazione federale
Gestione delle crisi	M16: Integrazione degli uffici competenti operanti nel settore della cibersicurezza negli stati maggiori di crisi della Confederazione	Definizione del ruolo del Centro di competenza per la cibersicurezza negli stati maggiori di crisi della Confederazione Arricchimento del lessico del ciberspazio	– Utilizzo degli attuali stati maggiori di crisi per la gestione delle crisi informatiche – Creazione di organizzazioni di crisi specifiche per settore ai fini della gestione delle crisi informatiche in ambito economico – Integrazione dei servizi deputati per la cibersicurezza negli stati maggiori
	M17: Esercizi congiunti di gestione delle crisi	Creazione delle basi per le esercitazioni di crisi che implicano aspetti inerenti al ciberspazio Svolgimento di esercitazioni di settore specifiche Introduzione di aspetti inerenti al ciberspazio nelle esercitazioni di crisi trasversali	– Verifica dei sistemi di gestione delle crisi – Ottimizzazione delle procedure e dei processi di gestione
Perseguimento penale	M18: Casistica della cibercriminalità	Sintesi dei dati della polizia cantonale in una casistica nazionale (PICSEL) Elaborazione di una casistica giudiziaria Presentazione degli sviluppi, degli scenari e delle ripercussioni della cibercriminalità	– Analisi e predisposizione delle condizioni quadro tecniche per l'elaborazione di un quadro nazionale della situazione della cibercriminalità
	M19: Rete di supporto alle indagini nella lotta alla criminalità digitale	Basi giuridiche concernenti la collaborazione e il computo delle prestazioni tra Confederazione e Cantoni nonché tra Cantoni	– Elaborazione delle condizioni quadro per la collaborazione con la polizia e il coordinamento tra i centri di competenze cantonali e nazionali per la cibersicurezza nella rete NEDIK
	M20: Formazione	Attuazione dei piani di formazione	– Sviluppo continuo delle competenze necessarie nell'ambito dei procedimenti penali
	M21: Ufficio centrale per la cibercriminalità	Modifica della legge sugli Uffici centrali di polizia giudiziaria	– Creazione di un ufficio centrale per la cibercriminalità e delle basi necessarie alla collaborazione con i Cantoni nella lotta contro la cibercriminalità

CA	Misura	Progetto di attuazione (output)	Outcome
Ciberdifesa	M22: Ampliamento delle capacità di acquisizione delle informazioni e di attribuzione degli attacchi informatici	Capacità di acquisizione delle informazioni e di attribuzione Svolgimento di una formazione specifica in ciberdifesa (esercito)	– Individuazione tempestiva di nuovi modelli d'attacco da parte del SIC – Sviluppo delle conoscenze specifiche e delle capacità del SIC per l'acquisizione di informazioni – Esecuzione di analisi approfondite degli attori e dell'ambiente – Utilizzo e sviluppo di strumenti tecnici – Elaborazione sistematica dei ciberattacchi
	M23: Capacità di eseguire misure attive nel ciberspazio secondo LAIn e LM	Utilizzo delle capacità del COE-BAC sviluppate nel quadro della LAIn	– Sviluppo di competenze e capacità qualitativamente e quantitativamente sufficienti per arrestare o rallentare attacchi contro le infrastrutture critiche
	M24: Garanzia della prontezza operativa dell'esercito nel ciberspazio in ogni circostanza e regolamentazione del suo ruolo sussidiario di supporto delle autorità civili	Progetto per lo sviluppo della ciberdifesa: abilitazione dell'esercito a fornire prestazioni nel ciberspazio Creazione di un centro nazionale di formazione per la cibersicurezza (Cyber Training Center) Formazioni per le organizzazioni di condotta nella gestione delle cibercrisi	– Gestione dei vari tipi di ciberminacce, sempre più gravi in termini di numero, intensità e complessità – Attuazione degli aspetti informatici della legge federale sulle attività informative e della legge militare – Supporto ai gestori delle infrastrutture critiche vittime di attacchi informatici
Posizionamento attivo della Svizzera nella politica di cibersicurezza internazionale	M25: Ruolo attivo nella definizione e partecipazione ai processi di politica in materia di cibersicurezza esterna	Partecipazione ai processi dell'ONU per la cibersicurezza internazionale Rappresentanza degli interessi nell'ambito dell'OSCE (consolidamento del clima di fiducia tra gli Stati) Creazione e istituzione dell'iniziativa «Geneva Dialogue on Responsible Behavior» Osservazione degli sviluppi in seno all'Unione europea (in particolare del Servizio europeo per l'azione esterna e dell'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione e di ENISA) Impegno per la promozione di un ciberspazio aperto e libero	– Sviluppo e attuazione di norme di comportamento statali e non statali nel ciberspazio – Riconoscimento del diritto internazionale e della tutela dei diritti dell'uomo nel ciberspazio – Costruzione di un clima di fiducia verso lo Stato nel ciberspazio – Applicazione di regimi di controllo delle esportazioni per quanto riguarda le tecnologie di monitoraggio
	M26: Cooperazione internazionale per la crescita e lo sviluppo delle capacità nel settore della cibersicurezza	Organizzazione di workshop con organizzazioni regionali Organizzazione di workshop per la creazione di istituzioni e strutture per la cibersicurezza esterna Supporto del Global Forum on Cyber-Expertise	– Confronto con organismi internazionali statali e non statali per l'acquisizione e lo sviluppo di competenze nazionali nell'ambito dei ciber-rischi – Acquisizione e sviluppo di capacità informatiche in Paesi terzi – Miglioramento della sicurezza informatica globale
	M27: Consultazioni politiche bilaterali e dialoghi multilaterali sulla politica estera di cibersicurezza	Consultazioni politiche bilaterali nel settore della cibersicurezza Sino-European Cyber Dialogue – Gruppo di lavoro «International Law»: consolidamento del clima di fiducia MENA Dialogue: quadro di discussione per gli Stati della regione MENA	– Organizzazione di consultazioni sulla cibersicurezza – Partecipazione a dialoghi multilaterali

CA	Misura	Progetto di attuazione (output)	Outcome
Visibilità e sensibilizzazione	M28: Creazione e attuazione di un piano per la comunicazione di informazioni sulla SNPC	Elaborazione di un piano per la comunicazione di informazioni sulla SNPC	– Creazione e attuazione di un piano per la comunicazione di informazioni sulla SNPC – Definizione di linee guida, competenze e processi di comunicazione
	M29: Sensibilizzazione del pubblico sui ciber-rischi («awareness»)	Sviluppo e svolgimento di una campagna nazionale di sensibilizzazione Piattaforma di informazione sui ciber-rischi gestita dal servizio nazionale di contatto per le questioni legate ai ciber-rischi	– Sensibilizzazione del pubblico sui ciber-rischi – Rafforzamento della comunicazione sui ciber-rischi

Tabella 15: output e outcome per ciascuna misura. CA = campo d'azione. Fonte: piano di attuazione della SNPC 2018–2022.

A-7 Security Capacity Switzerland: grado di maturità



Fonte: University of Oxford, 2020

Figura 4: Cyber-Security Capacity Switzerland: grado di maturità

Bibliografia

Center for Security Studies (CSS) PF Zurigo (2019): *Nationale Cyber-Sicherheitsstrategien im Vergleich – Herausforderungen für die Schweiz*. Zurigo.

Centro nazionale per la cibersicurezza NCSC (2021c): risultati della rilevazione interna delle risorse impiegate per l'attuazione della SNPC 2021; valutazione interna. Berna.

Centro nazionale per la cibersicurezza NCSC (2021a): *Rapporto semestrale 2020/2*. Berna.

Centro nazionale per la cibersicurezza NCSC (2021b): *Rapporto semestrale 2021/1*. Berna.

Confederazione Svizzera (2020a): strategia *Svizzera digitale*. Berna.

Confederazione Svizzera (2020b): *Strategia di politica estera digitale 2021–2024*. Berna.

Consiglio federale (2015): *Rete di dati sicura (SDVN)*. Comunicato stampa del 20 maggio 2015. Berna.

Consiglio federale (2017): *Strategia nazionale per la protezione delle infrastrutture critiche 2018–2022* (strategia PIC). Berna.

Consiglio federale (2018): *Strategia nazionale per la protezione della Svizzera contro i cyber-rischi (SNPC) 2018–2022*. Berna.

Consiglio federale (2021): *Rapporto sullo stato di attuazione della Strategia nazionale per la protezione della Svizzera contro i cyber-rischi 2018–2022*. Stato secondo trimestre 2021. Berna.

Dipartimento federale della difesa, della protezione della popolazione e dello sport DDPS (2021): *Strategia Ciber DDPS*. Berna.

European Union Agency for Network and Information Security ENISA (novembre 2016): *NCSS Good Practice Guide, Designing and Implementing National Cyber Security Strategies*. Attiki, Grecia.

gfs-Zürich (2021): *Auswirkungen der Corona-Krise auf die Digitalisierung und Cyber-Sicherheit in Schweizer KMU. Befragung von Geschäftsführenden kleiner Unternehmen in der Schweiz*. Studio su incarico di: digitalswitzerland et al. Zurigo.

Sotomo (2022): *Digitaler Staat in der Schweiz*. Studio commissionato da Swico. Zurigo.

Ufficio federale dell'energia (2021), *Cyber-Sicherheit und Cyber Resilienz für die Schweizer Stromversorgung*. Rapporto del 28 giugno 2021. Berna.

Università di Zurigo, Centro di gerontologia (2020): *Digital Seniors 2020*. Utilizzo delle tecnologie informatiche e di telecomunicazione da parte degli over 65 in Svizzera. Studio commissionato da Pro Senectute Svizzera. Zurigo.

University of Oxford (2020): *Cyber-Security Capacity Review. Switzerland. June 2020. Study at the invitation of the Swiss Federal Department of Foreign Affairs and the Swiss Federal Department of Finance*. Oxford.