AWK GROUP

Consulting
Engineering
Project Management

Rapporto

Verifica dell’efficacia della SNPC

Organo direzione informatica della Confederazione ODIC
Schwarztorstrasse 59
3003 Berna

30 novembre 2016, progetto n. 12.415.14.01

Informazioni sul presente documento

Titolo	Verifica dell’efficacia della SNPC	
Numero del progetto	12.415.14.01	
Pubblicazione	30 novembre 2016	
Salvataggio	2. aprile 2017	
Numero di pagine	89 esclusi gli allegati	
Nome del file	_Ber_161201_WiÜ_NCS_V1.0.docx	
Responsabile	Markus Meier, AWK	
Verifica a cura di	Correlatore/accompagnatore del progetto: Adrian Marti, AWK	Data: 18.11.2016

Gestione delle versioni

Versione	Data	Principali modifiche	Responsabile
V0.8	31.08.2016	Prima bozza completa all’attenzione del gruppo d’accompagnamento	Mem, Sep
V0.15	20.09.2016	Bozza da sottoporre a revisione da parte del CC SNPC	Mem
V0.25	16.11.2016	Versione dopo feedback WS SNPC II	Mem
V1.0	30.11.2016	Versione finale	Mem

Elenco delle abbreviazioni

Abbreviazione	Definizione
AEC	Associazione delle aziende elettriche svizzere
BAC	Base d’aiuto alla condotta
CaF	Cancelleria federale
CC SNPC	Comitato direttivo della SNPC
CCC	Cerchia chiusa di clienti
CdC	Conferenza dei governi cantonali
CDDGP	Conferenza delle direttrici e dei direttori dei dipartimenti cantonali di giustizia e polizia
CEO	Centro operazioni elettroniche
CERT	Computer Emergency Response Team
CIC	Consiglio informatico della Confederazione
CNO	Computer Network Operations
CoPIRFCyber	Comité de Pilotage Interdépartemental Recherche et Formation dans le domaine de la protection contre les Cyberrisques
CSI	Conferenza svizzera sull’informatica
CSIRT	Computer Security Incident Response Team
CTI	Commissione per la tecnologia e l’innovazione
CYD	Cyberdefence
DDoS	Distributed Denial-of-Service
DDPS	Dipartimento federale della difesa, della protezione della popolazione e dello sport
DEFR	Dipartimento federale dell’economia, della formazione e della ricerca
DFAE	Dipartimento federale degli affari esteri
DFGP	Dipartimento federale di giustizia e polizia
DPS	Divisione politica di sicurezza
DSC	Direzione dello sviluppo e della cooperazione
EGC	European Government CERTs Group
fedpol	Ufficio federale di polizia
FIRST	Forum of Incident Response and Security Teams
FTE	Full Time Equivalent
GCSP	Geneva Centre for Security Policy
GL	Gruppo di lavoro
GovCERT	Swiss Government CERT
ICANN	Internet Cooperation for Assigned Names and Numbers
IFSN	Ispettorato federale della sicurezza nucleare
iimt	International institute of management in technology
MELANI	Centrale d’annuncio e d’analisi per la sicurezza dell’informazione
MilCERT	Military Computer Emergency Response Team
MISP	Malware Information Sharing Platform
ODIC	Organo direzione informatica della Confederazione

Abbreviazione	Definizione
OIC	Operation Information Center
OSCE	Organizzazione per la Sicurezza e la Cooperazione in Europa
PPP	Partenariato pubblico privato
RSS	Rete integrata Svizzera per la sicurezza
SC SNPC	Servizio di coordinamento della SNPC
SCE	Swiss Cyber Experts
SCOCI	Servizio nazionale di coordinazione per la lotta contro la criminalità su Internet
SEFRI	Segreteria di Stato per la formazione, la ricerca e l'innovazione
SIC	Servizio delle attività informative della Confederazione
SIEM	Security Information and Event Management
SIGF	Swiss Internet Governance Forum
SIM	Servizio informazioni militare
Sipol	Politica di sicurezza (unità del DDPS)
SNPC	Strategia nazionale per la protezione della Svizzera contro i cyber-rischi
SOC	Security Operation Center
UFAE	Ufficio federale per l'approvvigionamento economico del Paese
UFCOM	Ufficio federale delle comunicazioni
UFE	Ufficio federale dell'energia
UFIT	Ufficio federale dell'informatica e della telecomunicazione
UFPP	Ufficio federale della protezione della popolazione
UO	Unità organizzativa
WSIS	World Summit of the Information Society

Indice

Compendio

Situazione iniziale e mandato

Il 27 giugno 2012 il Consiglio federale ha approvato la Strategia nazionale per la protezione della Svizzera contro i cyber-rischi (SNPC) e il 15 maggio 2013 il relativo piano di attuazione. Il piano prevede che, entro la primavera del 2017, debba essere presentata una verifica dell'efficacia della SNPC. Il presente rapporto adempie a questo mandato.

La SNPC definisce tre obiettivi strategici:

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

Si intende raggiungere questi obiettivi mediante 16 misure nei settori prevenzione e continuità, reazione, gestione delle crisi, collaborazione a livello internazionale, ricerca e formazione e basi legali.

Esposizione della verifica

Al fine di valutare in modo approfondito l'efficacia della SNPC è indispensabile effettuare un'analisi a tre livelli:

1) Misure della SNPC: le 16 misure sono state attuate come previsto? Cosa è stato raggiunto? In che misura hanno contribuito al raggiungimento degli obiettivi strategici?
2) Interfacce: i Cantoni e l'esercito sono stati coinvolti in modo adeguato nei lavori della SNPC?
3) Aspetti trasversali: le risorse della SNPC sono state pianificate in modo adeguato? I contenuti e la struttura dell'organizzazione della SNPC si sono dimostrati validi? La comunicazione interna ed esterna ha funzionato?

Metodo di valutazione

La verifica dell'efficacia si basa su un principio di valutazione completo che analizza l'efficacia su tre livelli (output, outcome e impact). Questi livelli sono definiti come segue:

- output: risultati dell'attuazione effettiva della strategia;
- outcome: gruppi di destinatari raggiunti, sviluppo delle conoscenze scaturito, sensibilizzazione e cambiamenti di comportamento raggiunti;
- impact: efficacia effettiva sugli obiettivi strategici della SNPC.

La valutazione dell'output e dell'outcome avviene in base agli obiettivi previsti nel piano di attuazione secondo una scala a quattro livelli (obiettivi raggiunti, obiettivi raggiunti soltanto in parte, obiettivi raggiunti in gran parte, obiettivi raggiunti). L'impact dimostra se un impatto è stato raggiunto o meno.

Rilevamento dei dati

I risultati della verifica effettuata si basano in primo luogo su un sondaggio condotta tra i responsabili dell'attuazione delle misure e i rappresentati delle interfacce, oltre che su un'analisi documentale a tutto tondo. Dove necessario e opportuno sono state condotte ulteriori inchieste. I partner da intervistare sono stati scelti in collaborazione con il servizio di coordinamento della SNPC. Il sondaggio si è svolto tra marzo e fine giugno 2016.

Poiché in tale periodo non tutte le misure erano state definite, la verifica effettuata riflette la situazione al momento del sondaggio.

Valutazione dell'attuazione delle misure

La Tabella 1 sintetizza i risultati della verifica a fronte delle singole misure.

Legenda			
✗✗	Obiettivi non raggiunti	✗	Obiettivi raggiunti soltanto in parte
✓✓	Obiettivi raggiunti in gran parte	✓	Obiettivi raggiunti
◎	Impact ottenuto	☐	Attualmente non misurabile, non valutabile

Misure	Ufficio competente, UO	Output	Outcome	Impact
M2/M12 Prevenzione e continuità: Analisi dei rischi e della vulnerabilità e continuità	UFPP, UFAE	✓✓	✓✓	☐
M3 Prevenzione e continuità: Analisi della vulnerabilità delle infrastrutture TIC	ODIC	✗	☐	☐
M4 Prevenzione e continuità: Elaborazione della rappresentazione e dell'evoluzione della situazione	MELANI, SIC	✓	✓	◎
M5 Reazione: Analisi ed elaborazione di eventi	MELANI, SIC	✓	✓	◎
M6 Reazione: Documento programmatico per una panoramica dei casi penali e il coordinamento dei casi di portata intercantonale	SCOCI	✓	✗	☐
M14 Reazione: Misure attive per l'identificazione degli autori	MELANI, SIC, ODIC	✓	✓	◎
M13 Gestione delle crisi: Coordinamento delle attività con gli attori direttamente interessati e supporto con perizie specializzate	MELANI, SIC	✓	☐	☐
M15 Gestione delle crisi: Documento programmatico per procedure e processi di condotta cibernetici	CaF	✓	✗	☐
M9 Collaborazione internazionale: Internet governance	UFCOM	✓✓	✓	☐
M10 Collaborazione internazionale: Cooperazione a livello della politica di sicurezza internazionale	DFAE	✓✓	✓✓	☐
M11 Collaborazione internazionale: Iniziative internazionali e processi di standardizzazione nel settore della sicurezza	UFCOM	✓	✗	☐
M1 Formazione e ricerca: Identificazione dei cyber-rischi attraverso la ricerca	SEFRI	✓✓	✓	☐
M7/M8 Formazione e ricerca: Panoramica delle offerte di formazione e incremento dell'impiego delle offerte di formazione in materia di creazione di competenze ed eliminazione delle lacune riscontrate nell'ambito delle offerte	SC SNPC	✓	✓✓	☐
M16 Basi legali: Necessità di modificare le basi legali	SC SNPC	✓✓	☐	☐

Tabella 1: Valutazione del raggiungimento degli obiettivi a fronte delle singole misure

Si può constatare che l'attuazione delle misure è avanzata in modo significativo. Le strutture e i processi previsti sono in gran parte stati implementati e diversi prodotti (rapporti e progetti) sono stati consegnati nei termini stabiliti. L'output prestato ha inoltre già determinato un importante outcome. Infatti, le capacità e le conoscenze sono state ampliate e la coordinazione è migliorata.

Risulta per contro più difficile valutare l'efficacia diretta (impact) dei lavori sugli obiettivi strategici. Nel contesto complesso e dinamico dei cyber-rischi è praticamente impossibile provare rapporti causali tra le misure adottate e il loro effetto sugli obiettivi della SNPC. Inoltre è troppo presto per effettuare una simile valutazione. Normalmente l'effetto delle misure adottate si manifesta soltanto dopo un determinato periodo. Pertanto è possibile dimostrare un impatto solo per tre delle 16 misure. Tuttavia, i modelli d'impatto elaborati per tutte le misure nel quadro della valutazione illustrano il previsto impatto concreto in base ai risultati finora ottenuti.

Valutazione delle interfacce
Ai fini dell'attuazione della SNPC due interfacce sono di fondamentale importanza: quella con le attività dei Cantoni e quella con la cyber-difesa dell'esercito. La verifica dell'efficacia della strategia ha valutato in che misura queste interfacce siano state ben utilizzate.

Interfaccia con i Cantoni

Livello	Obiettivi non raggiunti	Obiettivi raggiunti soltanto in parte	Obiettivi raggiunti in gran parte	Obiettivi raggiunti
Output				✓✓
Outcome			✓	
Impact	☐ attualmente non valutabile			

Tabella 2: Valutazione del raggiungimento degli obiettivi riguardanti le interfacce con i Cantoni – RSS

Interfaccia con l'esercito

Livello	Obiettivi non raggiunti	Obiettivi raggiunti soltanto in parte	Obiettivi raggiunti in gran parte	Obiettivi raggiunti
Output		✗		
Outcome		✗		
Impact nel contesto della CYD	☐ attualmente non valutabile			

Tabella 3: Valutazione del raggiungimento degli obiettivi riguardanti le interfacce con l'esercito

Valutazione degli aspetti trasversali
Per quanto riguarda gli aspetti trasversali, la valutazione mira ad accertare se la pianificazione delle risorse per la SNPC è stata fatta correttamente, se i contenuti e la struttura organizzativa della SNPC nel loro complesso si sono dimostrati validi e se la comunicazione, sia interna che esterna, ha funzionato. In questo contesto la valutazione è suddivisa in quattro livelli (aspettative non soddisfatte, aspettative soddisfatte soltanto

in parte, aspettative soddisfatte in gran parte, aspettative soddisfatte). I risultati di questa valutazione sono illustrati nella tabella 4:

Livello	Aspettative non soddisfatte	Aspettative soddisfatte soltanto in parte	Aspettative soddisfatte in gran parte	Aspettative soddisfatte
Pianificazione delle risorse			✓	
Contenuti				✓✓
Organizzazione			✓	
Comunicazione		✗		

Tabella 4: Valutazione degli aspetti trasversali

In generale anche gli aspetti trasversali ottengono un risultato positivo. I contenuti si sono rivelati efficaci, le risorse sono state appena sufficienti e la struttura organizzativa decentralizzata è accolta favorevolmente. È per contro stata criticata la comunicazione verso l'esterno che, secondo diversi partner intervistati, deve essere rafforzata.

1. Situazione iniziale e mandato

Il 27 giugno 2012 il Consiglio federale ha approvato la Strategia nazionale per la protezione della Svizzera contro i cyber-rischi (SNPC). D'intesa con le autorità, i rappresentanti dell'economia e i gestori di infrastrutture critiche, il Governo intende in tal modo minimizzare i cyber-rischi ai quali essi sono esposti quotidianamente. Il 15 maggio 2013 il Consiglio federale ha approvato il piano di attuazione della SNPC, in cui definisce le risorse in termini di personale necessarie per l'attuazione della SNPC e nomina un Comitato direttivo interdipartimentale della SNPC (CC SNPC) che controlli e coordini i lavori.

Il CC SNPC è incaricato di presentare al Consiglio federale, entro la primavera del 2017, una verifica dell'efficacia della strategia (pag. 10 del piano di attuazione). La verifica dovrebbe indicare se le misure decise siano riuscite a sortire gli effetti auspicati e se le risorse assegnate siano state impiegate in modo efficace.

Tale mandato costituisce la situazione iniziale per l'esecuzione della verifica dell'efficacia della strategia. Al riguardo bisogna però prima illustrare brevemente quali sono gli obiettivi e le misure contemplati dalla SNPC e chi è responsabile della loro attuazione. Nelle pagine successive sono descritti gli obiettivi e l'organizzazione del progetto di verifica dell'efficacia.

1.1. Situazione iniziale: contenuto e organizzazione della SNPC

1.1.1. Obiettivi e misure della SNPC

Il Consiglio federale ha individuato per la SNPC tre obiettivi strategici:

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

Per raggiungere questi obiettivi sono state definite 16 misure. Poiché i cyber-rischi interessano vari aspetti sociali, economici e politici, le misure sono differenziate di conseguenza. Tali misure comprendono l'esecuzione di analisi dei rischi, il rafforzamento della prevenzione, l'incentivazione della ricerca e la pianificazione della politica estera in materia di cyberspazio.

In sede di allestimento del piano di attuazione, le 16 misure sono state raggruppate e suddivise nei sei seguenti settori:

- <u>Prevenzione e continuità</u>
  - M2: Analisi dei rischi e della vulnerabilità in sottosettori critici
  - M3: Analisi della vulnerabilità delle infrastrutture TIC
  - M4: Elaborazione della rappresentazione e dell'evoluzione della situazione
  - M12: Gestione della continuità operativa: miglioramento della resilienza dei sottosettori critici
- <u>Reazione</u>
  - M5: Analisi ed elaborazione di eventi
  - M6: Documento programmatico per una panoramica dei casi penali e il coordinamento dei casi di portata intercantonale
  - M14: Misure attive per l'identificazione degli autori

- Gestione delle crisi
  - M13: Coordinamento delle attività con gli attori direttamente interessati e supporto con perizie specializzate
  - M15: Documento programmatico per procedure e processi di condotta cibernetici
- Formazione e ricerca
  - M1: Identificazione di cyber-rischi attraverso la ricerca
  - M7: Panoramica delle offerte di formazione
  - M8: Eliminazione delle lacune riscontrate nell'ambito delle offerte e incentivazione dell'utilizzo delle offerte esistenti
- Collaborazione internazionale
  - M9: Internet governance
  - M10: Cooperazione internazionale in materia di sicurezza cibernetica
  - M11: Iniziative internazionali e processi di standardizzazione nel settore della sicurezza
- Basi legali
  - M16: Necessità di modificare le basi legali

1.1.2. Organizzazione e responsabilità attuativa della SNPC

La responsabilità strategica per l'attuazione della SNPC compete al CC SNPC. In qualità di organo operativo del CC SNPC, il servizio di coordinamento della SNPC (SC SNPC) esegue il controlling strategico delle misure e il coordinamento dei responsabili delle misure. Il SC SNPC è parte dell'Organo direzione informatica della Confederazione (ODIC) e della Centrale d'annuncio e d'analisi per la sicurezza dell'informazione (MELANI).

Alle seguenti UO compete l'attuazione delle seguenti misure:

- SC SNPC (M7, M8, M16)
- MELANI (M4, M5, M13, M14)
- ODIC (M3)
- SIC (M4, M5, M14)
- UFPP e UFAE (M2, M12)
- UFCOM (M7, M9, M11)
- DFAE (M10)
- CaF (M15)
- SEFRI (M1)

1.2. Obiettivi della verifica dell'efficacia della strategia

Come indicato nel decreto del Consiglio federale concernente il piano di attuazione della SNPC, la verifica dell'efficacia della strategia deve innanzitutto analizzare i lavori fatti, le spese sostenute e i risultati raggiunti. Da ciò si evincono i tre obiettivi principali della verifica:

- Valutazione in merito all'attuazione delle misure: occorre verificare quali lavori sono stati fatti e a fronte di quali spese e quali risultati ed effetti è stato possibile ottenere.
- Valutazione delle interfacce: occorre analizzare se in sede di attuazione della SNPC si tengono sufficientemente in considerazione i Cantoni e se viene mantenuta attiva l'interfaccia con la cyber-difesa dell'esercito.
- Valutazione degli aspetti trasversali: occorre valutare se la pianificazione delle risorse per la SNPC è stata fatta correttamente, se i contenuti e la struttura prescelta

della SNPC si sono dimostrati validi e se la comunicazione interna ed esterna è stata soddisfacente.

2. Procedura

La base per l'attuazione della verifica dell'efficacia della strategia è costituita dal documento programmatico di dettaglio [3] redatto nell'autunno del 2015, in cui si stabiliva la procedura da seguire per effettuare la verifica in questione. Sulla base di tale documento è stata definita una procedura in tre fasi:

- Concezione
- Esecuzione
- Reporting

2.1. Concezione

Il documento programmatico di dettaglio di cui sopra articola la valutazione in tre parti:

1) Valutazione delle misure (cap. 3)
2) Verifica delle interfacce (cap. 4)
3) Analisi degli aspetti trasversali (cap. 5)

Questa struttura è utilizzata anche nel presente rapporto.

Le misure e le interfacce vengono verificate con l'ausilio di modelli di efficacia, in cui vengono illustrati gli effetti che le misure devono sortire e le relative modalità. Vi si distinguono i livelli documento programmatico, input, output, outcome e impact, come schematicamente rappresentato alla Figura 1:

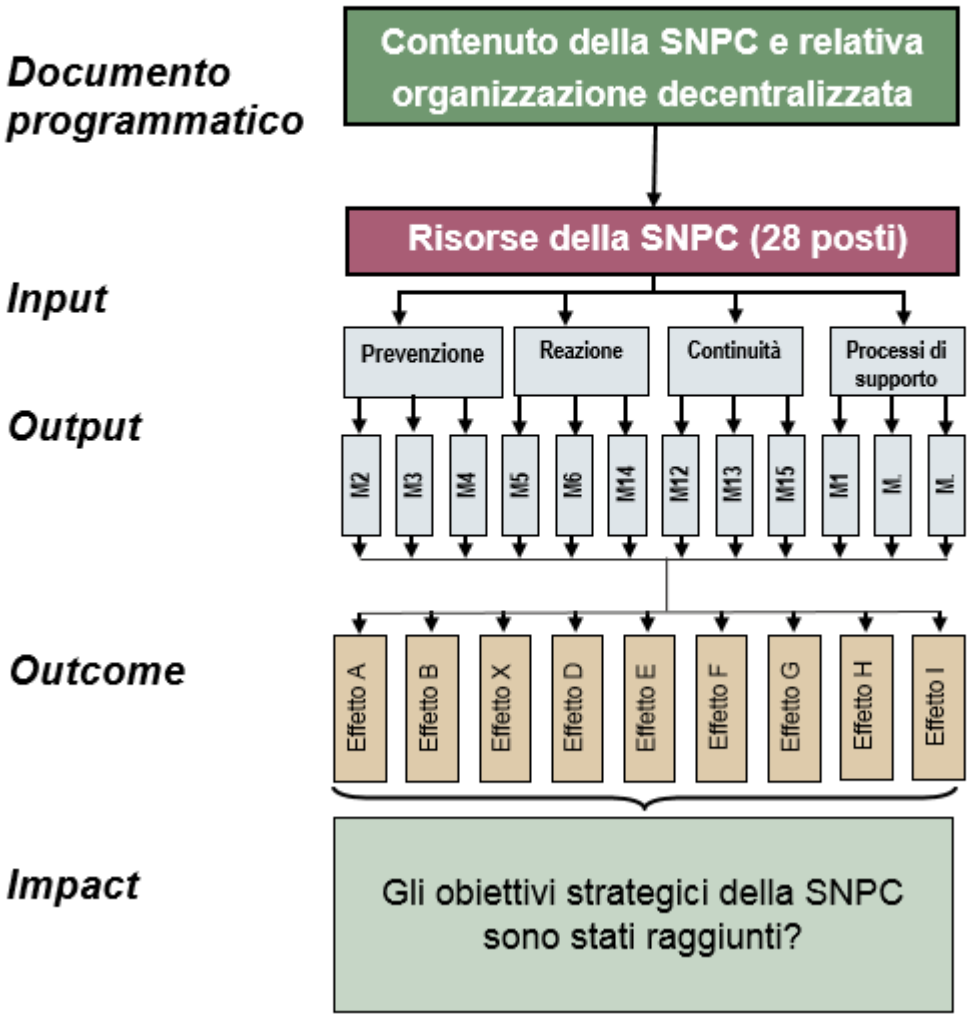

Figura 1: Livelli della verifica dell'efficacia della strategia

- **Documento programmatico:** questo livello ha rilevanza soprattutto per le questioni e le interfacce trasversali. Si valuta se, dal punto di vista contenutistico e organizzativo, la SNPC è ben strutturata e se c'è stata una buona collaborazione con i terzi. Per quanto riguarda le 16 misure, sono oggetto di analisi i livelli input, output, outcome e impact.
- **Input:** impiego di risorse finanziarie e di personale per l'attuazione della strategia. Viene valutato l'impiego delle risorse assegnate e se queste contribuiscono in maniera continuativa ai compiti previsti dalla SNPC.
- **Output:** risultati dell'attuazione effettiva della strategia: strutture organizzative consolidate, procedure implementate, prodotti e offerte di servizi realizzati ecc. Si tratta di valutare lo stato di attuazione delle misure nei diversi ambiti (raggiungimento di obiettivi intermedi).
- **Outcome:** gruppi di destinatari raggiunti, conoscenze acquisite, sensibilità toccate e comportamenti modificati. Al centro dell'attenzione c'è anche la valutazione della potenziale efficacia delle singole misure, ad esempio la loro capacità di sensibilizzare o modificare i comportamenti in relazione ai cyber-rischi.

- **Impact:** attuando le misure definite è possibile raggiungere gli obiettivi strategici della SNPC? L'attuazione delle misure è stata efficace? C'è stato un contributo alla resilienza e alla riduzione dei cyber-rischi? Se sì, di quale portata?

D'intesa con i responsabili delle misure, per ciascuna misura (e interfaccia) è stato sviluppato un modello di efficacia. Questo permette di capire quali erano l'idea di base, le modalità di esecuzione e i risultati di ciascuna misura. Ai fini della verifica delle misure sono importanti soprattutto i livelli output, outcome e impact, perché su questi livelli si può misurare direttamente l'avanzamento e il buon esito dei lavori dei responsabili dell'attuazione.

2.2. Esecuzione

2.2.1. Modalità di esecuzione del sondaggio

Come base per la valutazione è stato utilizzato un questionario generale ricavato dal documento programmatico [3].

Sulla base del questionario generale sono stati predisposti dei questionari individuali, da utilizzare nelle interviste e da inviare ai destinatari del sondaggio scritta.

I questionari specifici già precompilati mediante la documentazione messa a disposizione sono stati inviati ai partecipanti al sondaggio almeno cinque giorni lavorativi prima dell'intervista, affinché potessero prepararsi. I destinatari dei questionari scritti avevano circa dieci giorni lavorativi per rispondere. Dopo le interviste, i questionari interamente compilati sono stati trasmessi in visione ai partner intervistati per un'ultima verifica delle risposte fornite.

2.2.2. Scelta delle persone da intervistare

Le persone da intervistare sono state scelte d'intesa con il SC SNPC:

- **Interviste personali:** in totale sono state condotte 14 interviste con i rappresentanti di SEFRI, DFAE-DPS, ODIC-SEC, MELANI-ODIC, MELANI-OIC, SIC, fedpol, UFCOM, CaF, RSS, UFPP, UFAE, SIM, BAC e UFE.
- **Inchieste scritte:** sono state condotte inchieste scritte presso i rappresentanti di sei sottosettori critici: approvvigionamento di gas naturale, approvvigionamento di energia elettrica, traffico aereo, banche, media, sanità.

L'elenco dettagliato degli intervistati è riportato nell'allegato A.1.

Per ciascun ambito tematico il SC SNPC ha preparato per AWK i documenti necessari disponibili, i quali sono stati in parte integrati con ricerche condotte internamente da AWK (si vedano i riferimenti nell'allegato B).

2.2.3. Impressioni maturate durante il sondaggio

Il gran numero di domande (più di 280) previste nel documento programmatico [3] ha rappresentato una vera e propria sfida. Talvolta i partner intervistati, ad esempio quelli che erano responsabili di più misure, hanno dovuto rispondere anche a 100 domande. Le persone intervistate erano molto motivate e preparate. La modalità di esecuzione scelta è stata ben recepita e i partecipanti hanno partecipato attivamente. In alcuni casi hanno anche colto l'opportunità di riesaminare le risposte date durante l'intervista precisandone il contenuto per scritto.

Anche il sondaggio scritto condotto tra i rappresentanti dei sottosettori si è svolta in maniera ineccepibile. I questionari sono stati prontamente compilati e restituiti e in tal modo erano pronti per la valutazione.

2.3. Reporting

Nell'ultima fase si è proceduto al consolidamento dei risultati, che sono stati poi riassunti nel presente rapporto destinato al Consiglio federale. Il tutto è avvenuto in stretta collaborazione con il SC SNPC e i responsabili dell'attuazione, in modo da chiarire dubbi e contraddizioni nonché colmare eventuali lacune.

Osservazione: quanto affermato nel rapporto si basa sulle risposte fornite dai partner durante l'intervista. AWK ha elaborato tali risposte senza alterarne il senso e le ha utilizzate per redigere il presente rapporto.

2.4. Principali difficoltà in sede di valutazione

La valutazione dei dati acquisiti è il momento topico della verifica dell'efficacia della strategia. Allo stesso tempo, però, è anche la fase dell'intero processo la cui realizzazione rappresenta la sfida più grande. In nome della trasparenza, AWK descrive in questa sede alcune delle principali questioni con cui il team di valutazione ha dovuto confrontarsi e spiega quali soluzioni sono state adottate e per quali motivi.

2.4.1. Eterogeneità contenutistica delle misure

Come precedentemente spiegato, il contenuto delle 16 misure copre uno spettro estremamente vasto. La difficoltà insita nella verifica dell'efficacia sta soprattutto nel fatto che talune misure hanno prodotti finali chiaramente definiti, mentre per altre lo scopo è di dare inizio a nuovi processi o consolidare processi già in corso. Per la persona incaricata di effettuare la verifica è più semplice misurare prodotti che processi. Sussiste dunque il rischio che, nel confronto, le misure riferite ai prodotti siano valutate diversamente da quelle orientate ai processi.

Per ovviare a questa problematica, AWK considera le misure attenendosi rigorosamente agli obiettivi (obiettivi intermedi) secondo la roadmap della SNPC [6]. Solo così si può fare una valutazione equa, dato che le risorse assegnate si riferiscono alle misure definite. Questa soluzione comporta che, in sede di valutazione delle misure, AWK si astenga dall'effettuare confronti incrociati tra le misure, limitandosi a evidenziare per ciascuna misura se e fino a che punto sono stati raggiunti i corrispondenti obiettivi.

2.4.2. Verifica dell'efficacia delle misure in corso

Una grossa sfida posta dalla verifica dell'efficacia della strategia riguarda il momento in cui è stata effettuata. Normalmente questo genere di verifiche sono eseguite dopo la conclusione di un programma. Per contro, quando la verifica viene eseguita nel corso di un progetto sorgono due difficoltà sostanziali:

- eterogeneità nel grado di attuazione delle misure: poiché le varie misure sono ancora in corso, spesso si valuta un risultato intermedio e non la situazione finale;
- misurazione dell'impatto: per molte misure non è realistico misurare già adesso gli effetti a livello di impatto, visto che la loro efficacia sarà evidente solo in un secondo momento.

AWK era consapevole di questi problemi fin dall'inizio. Il primo problema può essere risolto valutando le misure esclusivamente in base agli obiettivi della roadmap della SNPC [6] già raggiunti nella primavera del 2016. Ai fini della valutazione non si tiene conto degli obiettivi prefissati dalla roadmap che devono essere conseguiti successivamente a tale data.

L'impatto delle misure viene valutato soltanto se si è in grado di dimostrare che c'è stato un effetto diretto o se si ha la certezza che non così non sarà. Per tutte le altre misure viene segnalata l'impossibilità di procedere a una valutazione, limitandosi a valutarle esclusivamente sotto il profilo dell'output e dell'outcome.

3. Verifica dell’efficacia delle misure

Ai fini della valutazione delle misure risulta determinante l’obiettivo definito per ognuna di esse nella roadmap della SNPC [6] e meglio precisato dagli stessi responsabili dell’attuazione.

Le 16 misure presentate al capitolo 1.1.1 vengono considerate a livello di input, output, outcome, impact e di documento programmatico. Si procede seguendo il documento programmatico illustrato al capitolo 2.1.

I capitoli in cui viene stilato il rapporto sulle singole misure sono strutturati in maniera identica per tutte e sedici le misure:

- Tabella con la descrizione delle misure, costituita da:
  - descrizione degli obiettivi;
  - ufficio responsabile;
  - fonti (documenti consultati);
  - rinvio alle interviste.
- Effetto atteso con il modello di efficacia estratto dal documento programmatico di dettaglio [3]
- Input (risorse assegnate)
- Tabella sul raggiungimento degli obiettivi e sulla loro efficacia
- Motivazione della valutazione suddivisa in output, outcome e impact

Gli aspetti riguardanti le interfacce sono riportati al capitolo 4, mentre gli aspetti trasversali sono riassunti al capitolo 5.

3.1. M2/M12 Prevenzione e continuità: Analisi dei rischi e della vulnerabilità nonché continuità

Titolo della misura	Analisi dei rischi e della vulnerabilità nonché gestione della continuità operativa al fine di migliorare la resilienza dei sottosettori critici
Obiettivi	Obiettivi della misura M2 Analisi dei rischi e della vulnerabilità • Nei 28 settori parziali critici vengono effettuate analisi dei rischi e della vulnerabilità in collaborazione con le autorità specializzate e con le associazioni come pure coinvolgendo i fornitori di prestazioni TIC e gli operatori di infrastrutture d’importanza critica. Tali analisi hanno avuto luogo secondo un approccio il più possibile unitario. – I risultati delle analisi dei rischi e della vulnerabilità sono consolidati in un’analisi globale della situazione di minaccia in collaborazione con la centrale MELANI. – I risultati fungono soprattutto da base per i lavori finalizzati alla realizzazione della misura 12. Obiettivi della misura M12 Gestione della continuità operativa • Miglioramento della resilienza dei sottosettori critici: sulla base dei risultati delle analisi dei rischi e della vulnerabilità, nei 28 sottosettori critici vengono elaborati i relativi documenti programmatici con le possibili misure di miglioramento della resilienza. – Questo lavoro viene fatto in collaborazione con il settore e, laddove opportuno, coinvolgendo le associazioni come anche le autorità specializzate e di regolazione competenti.

	– Il documento programmatico può contenere anche proposte riguardanti le misure di prevenzione, per la creazione di un sistema di gestione interaziendale della continuità operativa e delle crisi o per il miglioramento della resilienza delle imprese del rispettivo sottosettore critico.
Ufficio/UO responsabile	UFPP, UFAE
Documenti consultati per la verifica dell'efficacia	Fonti: [34], [35], [36], [37], [38], [39], [40], [41], [42], [43], [44], [45], [46], [47], [48], [49], [50], [51], [52], [53], [54], [55], [56], [57], [58], [59], [60], [61], [62], [63], [64]
Interviste, questionari	Si vedano l'allegato A.1, le interviste I 3, I 8 e le domande ai sottosettori A.2

Osservazioni

- L'UFPP e l'UFAE hanno proceduto a una ripartizione dei 28 sottosettori come segue.
  - Competenza UFPP: rappresentanze diplomatiche e sedi di organizzazioni internazionali, ricerca e insegnamento, beni culturali, Parlamento, Governo, giustizia e amministrazione, rifiuti, banche, assicurazioni, cure mediche e ospedaliere, laboratori, media, traffico postale, esercito, organizzazioni di primo intervento (polizia, pompieri, sanità), protezione civile.
  - Competenza UFAE: approvvigionamento di gas naturale, di petrolio e di energia elettrica; industria chimica e farmaceutica, industria meccanica, elettrotecnica e metallurgica (MEM), tecnologie dell'informazione, telecomunicazioni, approvvigionamento alimentare, traffico stradale, traffico navale, ferroviario e aereo, approvvigionamento idrico, acque di scarico.
- Per valutare i lavori concernenti le misure 2 e 12 sono stati intervistati complessivamente 13 rappresentanti dei seguenti sottosettori: cure mediche e ospedaliere, laboratori, banche, media, approvvigionamento di energia elettrica; gas; traffico aereo.

3.1.1. Effetto atteso: modello di efficacia M2/M12

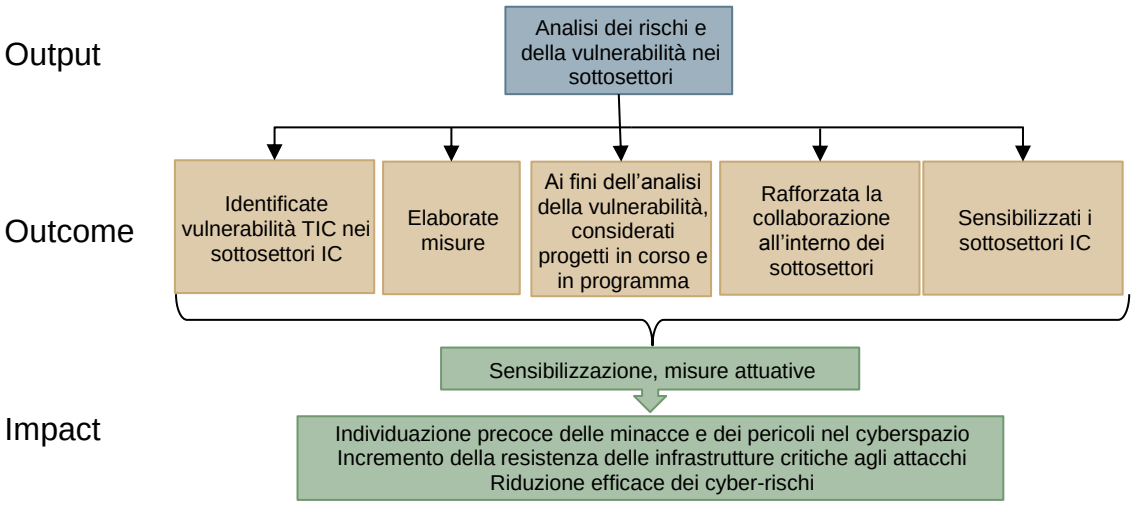

Figura 2: Modello di efficacia M2/M12

3.1.2. *Input: risorse assegnate*

Tipo di risorsa	Numero di risorse assegnate alla SNPC
Risorse in termini di personale	2 UFPP 2 UFAE 1 UFE
Risorse finanziarie	Nessuna risorsa aggiuntiva
Collaborazione di altri uffici/UO	Autorità specializzate/regolatori, MELANI, consultazioni con UFIT e BAC, associazioni professionali, rappresentanti delle infrastrutture critiche e altri attori di rilievo dei singoli sottosettori

All'UFPP e all'UFAE sono stati assegnate due FTE ciascuno per dirigere il progetto ed eseguire le analisi dei rischi e della vulnerabilità. Presso l'UFE è stato creato un posto, con il compito di analizzare i cyber-rischi specifici del settore energetico, supportare le misure di resilienza dell'economia energetica e, all'occorrenza, predisporre l'adeguamento delle condizioni quadro giuridiche. Senza questi posti non sarebbe stato possibile eseguire i lavori.

3.1.3. *Valutazione del raggiungimento degli obiettivi e della loro efficacia*

Livello	Obiettivi non raggiunti	Obiettivi raggiunti soltanto in parte	Obiettivi raggiunti in gran parte	Obiettivi raggiunti
Output				✓✓
Outcome				✓✓
Impact	☐ attualmente non valutabile			

Osservazione: alla data della verifica dell'efficacia, le analisi dei rischi e della vulnerabilità non erano ancora state interamente completate. I lavori proseguono come da programma fino al 2017 e le tempistiche sono rispettate. Alla data della verifica erano disponibili i rapporti conclusivi sulle analisi dei rischi e della vulnerabilità per i sottosettori seguenti:

- UFPP: protezione civile, laboratori, media, banche, cure mediche e ospedaliere. L'UFPP aveva inoltre fornito rapporti preliminari concernenti i settori: organizzazioni di primo intervento (polizia, pompieri, sanità), Parlamento, Governo, giustizia e amministrazione.
- UFAE: approvvigionamento di energia elettrica e di gas naturale, traffico aereo, traffico stradale, alimentari.

Oltre alle analisi dei rischi e della vulnerabilità era già disponibile un rapporto preliminare (M12) dell'UFAE sulle misure per il settore del gas naturale.

La valutazione si basa su questi rapporti.

3.1.4. Motivazione della valutazione

Output: gli obiettivi sono stati raggiunti

> Alla data della verifica dell'efficacia le analisi dei rischi e della vulnerabilità di vari sottosettori erano in parte già state eseguite, altre erano ancora in corso. La qualità dei rapporti e la metodica scelta sono state giudicate buone dagli esperti interrogati. Per le loro analisi l'UFPP e l'UFAE utilizzano approcci leggermente diversi, il che pregiudica un po' la coerenza e la trasparenza dell'intero progetto. Tuttavia al termine dei lavori sarà possibile avere un quadro generale dei rischi TIC e delle vulnerabilità dei sottosettori critici.

- **Valutazione delle analisi dei rischi e delle vulnerabilità nei sottosettori infrastrutturali critici:** le analisi dei rischi e della vulnerabilità e le analisi di mercato dei sottosettori critici sono in corso o sono già state completate. I rapporti sono stati stilati da gruppi di esperti sotto la guida dell'UFPP o dell'UFAE. I gruppi di esperti sono stati coadiuvati da rappresentanti dei settori (associazioni professionali e/o importanti imprese), rappresentanti delle autorità specializzate, regolatori e da altri specialisti TIC. I rapporti sono stati sottoposti a un processo di feedback multilivello, il che ha permesso di concordarne il contenuto con gli esperti dei vari settori. Tutti i rapporti sono infine approvati dall'UFPP, dall'UFAE o dall'ODIC.

  Dai rapporti già pronti alla data della verifica dell'efficacia emerge la valutazione sottostante.

  – Procedimento e struttura: la stretta collaborazione con gli esperti dei vari settori è da questi molto apprezzata. Il loro coinvolgimento consente di avere una rappresentazione completa delle strutture del mercato nei rispettivi settori, una stima realistica dei rischi e delle vulnerabilità nonché semplifica la definizione delle misure.
  – Metodica: per ciascun sottosettore si procede anzitutto a una descrizione generale del sottosettore. In seguito vengono identificati i processi critici e infine viene eseguita un'analisi dei rischi e della vulnerabilità. Per la valutazione dei rischi e delle vulnerabilità l'UFPP e l'UFAE hanno scelto approcci diversi (per ulteriori informazioni al riguardo si veda l'osservazione sottostante).
  – Trasparenza ed esposizione dei risultati: sulla base dei rapporti è prevista la preparazione di fogli informativi che possono essere resi accessibili al pubblico. Questo consente anche di ottenere una visione generale sulle analisi dei rischi e della vulnerabilità, contribuendo così a creare trasparenza.

- **Osservazione in merito alle diversità di approccio tra l'UFPP e l'UFAE:** per la valutazione dei rischi e delle vulnerabilità l'UFPP e l'UFAE hanno seguito un approccio diverso. L'UFPP, basandosi sui risultati delle analisi della vulnerabilità, effettua analisi dei rischi a fronte di vari scenari ed elabora una stima del rischio moltiplicando la probabilità che esso si verifichi per il potenziale danno. L'UFAE valuta le vulnerabilità TIC sulla base della criticità e della pericolosità dei sottoprocessi e rinuncia a effettuare un'analisi dei rischi sulla base di scenari. Il motivo di questo diverso modo di procedere risiede sia nelle differenti caratteristiche dei singoli sottosettori sia nella volontà di entrambi di riallacciarsi a lavori già in corso nei due uffici (per l'UFPP la strategia per la protezione delle infrastrutture critiche e l'analisi nazionale dei rischi «Catastrofi e situazioni di emergenza in Svizzera», per l'UFAE l'orientamento strategico dell'approvvigionamento economico del Paese). Ne consegue che l'UFPP analizza i cyber-rischi nel contesto di altri possibili pericoli, mentre l'UFAE fa un esame particolareggiato delle vulnerabilità TIC specifiche.

Malgrado la diversità di approccio, grazie alle analisi effettuate da entrambi gli uffici è comunque possibile farsi un quadro generale dei rischi e delle vulnerabilità dei diversi sottosettori. Inoltre anche il fatto di ricavare misure specifiche per le TIC per i sottosettori è un'attività da eseguire in modo analogo. Il diverso approccio non pregiudica quindi la possibilità di conseguire gli obiettivi riferiti alle misure.

Outcome: gli obiettivi sono stati raggiunti

Le vulnerabilità TIC dei sottosettori considerati sono state identificate e valutate chiaramente. Troviamo già delle prime proposte di misure nei rapporti conclusivi della M2, che vengono però ulteriormente elaborate in rapporti distinti nel quadro della M12. Dai documenti a disposizione si evince che le proposte formulate sono concrete e ben ancorate nei vari settori.
La difficoltà risiede nella supervisione delle attività di attuazione di tali misure e nell'aggiornamento delle analisi prodotte. A questo proposito resta ancora da definire l'ulteriore modo di procedere.

- **Identificazione delle vulnerabilità TIC nei sottosettori critici:** nei rapporti disponibili alla data della verifica dell'efficacia le vulnerabilità TIC sono state sistematicamente analizzate e chiaramente valutate. Poiché le vulnerabilità TIC non rivestono uguale importanza in tutti i sottosettori, anche i rapporti presentano un diverso grado di dettaglio.
- **Elaborazione delle misure:** le analisi contengono già una descrizione delle misure proposte. Anche in questo caso le misure vengono elaborate in stretta collaborazione con gli esperti dei vari settori e con le autorità e le associazioni responsabili, e vengono fissate nei rapporti relativi alla misura M12. Alla data della verifica dell'efficacia erano disponibili un solo rapporto di questo tipo (per il sottosettore Approvvigionamento di gas naturale) e un documento programmatico generale per la redazione dei rapporti. È evidente come, partendo dall'analisi dei rischi e della vulnerabilità e collaborando con i rappresentanti dei vari settori e i regolatori, sia possibile formulare misure concrete (p. es. il rollout della rete Polycom per garantire la sicurezza delle comunicazioni dei gestori di infrastrutture critiche). In alcuni sottosettori i lavori hanno portato all'ammissione di importanti gestori di infrastrutture critiche nella CCC di MELANI.
- **Considerazione dei progetti in corso:** la digitalizzazione determina l'insorgere di nuove vulnerabilità TIC in molti settori. In questo senso le analisi dei rischi e della vulnerabilità consentono anche di prevedere le possibili sfide da affrontare. È chiaro che tali analisi richiedono aggiornamenti costanti per seguire lo sviluppo tecnologico. Per questi aggiornamenti non vengono però definite scadenze.
- **Rafforzata la collaborazione all'interno dei sottosettori:** la collaborazione all'interno dei sottosettori funzionava bene già prima della SNPC (anche grazie ai lavori dell'UFPP nell'ambito della strategia PIC e dell'UFAE nell'ambito della sua organizzazione dei quadri) e oggi funziona ancora meglio. In particolare i lavori hanno contribuito a coinvolgere maggiormente nelle analisi dei rischi e della vulnerabilità i diversi attori dei singoli sottosettori.
- **Sensibilizzazione dei sottosettori infrastrutturali critici:** alcuni sottosettori (p. es. le banche) sono già fortemente sensibilizzati sul tema dei cyber-rischi, altri invece lo erano ancora poco (p. es. traffico stradale e media). In questi settori è stato apportato un valido contributo alla sensibilizzazione. Svariate richieste inviate all'UFPP e all'UFAE confermano che i gestori di infrastrutture critiche prestano maggiore attenzione a queste tematiche.

Impatto: attualmente non valutabile

Le misure M2 e M12 ottengono un impatto se i sottosettori attuano misure concrete di riduzione dei rischi TIC e delle vulnerabilità riducendo così i loro cyber-rischi. Talvolta questo avviene già (p. es. nel settore gas naturale). Tuttavia è ancora troppo presto per valutare l'effetto di questo impegno e di conseguenza l'impatto di queste misure nel loro insieme.

3.2. M3 Prevenzione e continuità: Analisi della vulnerabilità delle infrastrutture TIC

Titolo della misura	Analisi della vulnerabilità delle infrastrutture TIC
Settore	Prevenzione
Obiettivi	Ai responsabili delle segreterie generali e ai fornitori di prestazioni competenti viene fornito un piano di verifica che consenta loro di analizzare l'ambiente TIC dell'Amministrazione federale per rilevarne le vulnerabilità sistemiche, organizzative e tecniche e identificare i rischi informatici cui è esposto. Il piano di verifica è stato predisposto con il supporto dei fornitori di prestazioni UFIT e BAC e coordinato con i progetti in corso. I risultati sono consolidati in un'analisi globale della situazione di minaccia in collaborazione con la centrale MELANI. Il piano di verifica identifica i rischi informatici per ogni processo critico e definisce gli standard minimi di rilevanza sistemica. Se interessati, i Cantoni, l'economia e i gestori di infrastrutture critiche ricevono il piano di verifica delle infrastrutture TIC dell'Amministrazione federale per le proprie verifiche della vulnerabilità.
Ufficio/UO responsabile	ODIC
Documenti consultati per la verifica dell'efficacia	Fonti: [65], [66], [67], [68], [69], [70]
Interviste	Si veda l'allegato A.1, intervista I 7

3.2.1. Effetto atteso: modello di efficacia M3

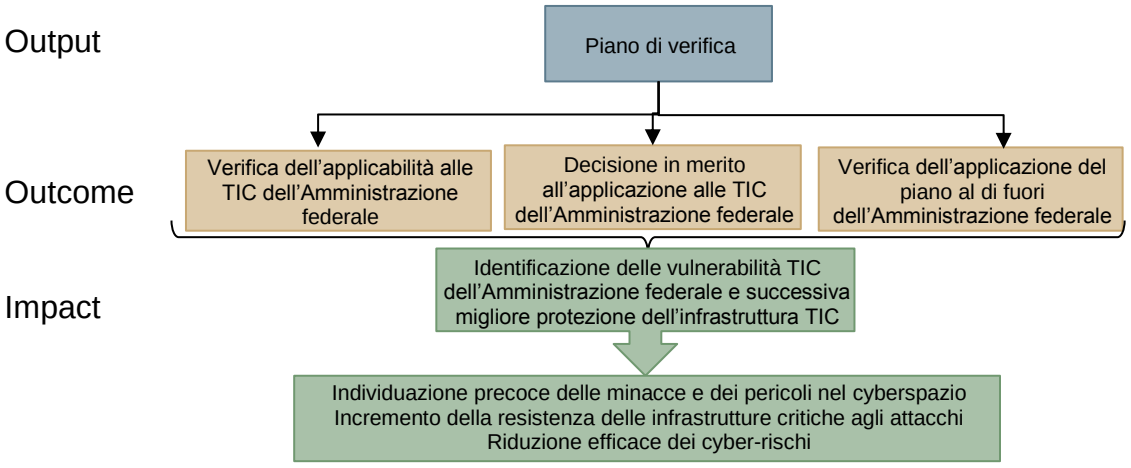

Figura 3: Modello di efficacia M3

3.2.2. Input: risorse assegnate

Tipo di risorsa	Numero di risorse assegnate alla SNPC
Risorse in termini di personale	Un posto a tempo determinato (100 %) presso l'ODIC fino al 31.12.2015
Risorse finanziarie	Nessuna risorsa aggiuntiva
Collaborazione di altri uffici/UO	Consultazioni con UFIT, BAC e CIC

Osservazioni

Per preparare il piano di verifica è stato creato un ulteriore posto a tempo determinato sino a fine 2015, occupato da una persona idonea alla funzione. Alla stesura del piano di verifica hanno partecipato i fornitori di prestazioni UFIT e BAC e il CIC. In generale il fabbisogno in termini di risorse, in particolare delle risorse per la verifica dell'attuabilità, è stato nettamente sottovalutato.

3.2.3. Valutazione del raggiungimento degli obiettivi e della loro efficacia

Livello	Obiettivi non raggiunti	Obiettivi raggiunti soltanto in parte	Obiettivi raggiunti in gran parte	Obiettivi raggiunti
Output		✖		
Outcome	☐ attualmente non valutabile			
Impact	☐ attualmente non valutabile			

3.2.4. Motivazione della valutazione

Output: gli obiettivi sono stati raggiunti soltanto in parte

> È stato predisposto un piano per analizzare le vulnerabilità TIC presenti nell'Amministrazione federale, Tuttavia esso non è stato recepito dal CC SNPC che ne ha ritenuta irrealistica l'attuazione in considerazione degli alti costi. Nella misura straordinaria successivamente decisa dal CC SNPC è stata sviluppata un'alternativa. Nel complesso i lavori non sono avanzati come inizialmente previsto.

Nel quadro della M3 è stato predisposto un piano di verifica che doveva servire al rilevamento e alla valutazione sistematica di tutte le vulnerabilità TIC presenti nell'Amministrazione federale. Il piano è basato sulla «Information Risk Assessment Methodology» (IRAM) riconosciuta a livello internazionale e sugli standard relativi all'analisi dei rischi TIC messi a punto dal «Bundesamt für Sicherheit in der Informationstechnik» (BSI) tedesco, l'ufficio preposto alla sicurezza informatica.

Già nella versione preliminare di questo piano veniva sostenuta la necessità, volendo rispettare in toto gli standard, di ampliare il compito originario dell'analisi delle vulnerabilità TIC, in quanto questo non imponeva di tenere sistematicamente in considerazione i processi interni, i pericoli e le minacce ma si limitava a considerare le vulnerabilità. Una successiva versione del piano di verifica ha però evidenziato che l'esecuzione di un'analisi dettagliata dei rischi TIC avrebbe comportato oneri eccessivi, sia finanziari che in termini di personale. Questo è quanto emerso anche dalle consultazioni previste dal compito con i fornitori di prestazioni UFIT e BAC, che hanno giudicato il piano senz'altro valido allo scopo ma estremamente oneroso in termini di risorse. Considerata l'impossibilità di aumentare le risorse a disposizione, pur giudicando il piano teoricamente corretto i membri del CIC ne hanno messo in dubbio la proporzionalità e l'effettivo valore aggiunto alla prova dei fatti.

In seno al CC SNPC il piano di verifica è stato oggetto di critiche [65]. I punti principali su cui si sono concentrate le critiche sono stati l'assenza di attenzione per l'identificazione delle vulnerabilità TIC, la mancanza di chiare indicazioni operative e i dubbi circa il valore aggiunto di un'analisi completa e fortemente standardizzata dei rischi TIC. Questi motivi hanno indotto il CC SNPC ad adottare una misura straordinaria per la M3, finalizzata allo sviluppo di un'alternativa al piano di verifica predisposto che delineasse un approccio pragmatico e di facile attuazione per il rilevamento delle vulnerabilità TIC. L'ODIC ha

predisposto quindi un piano con queste caratteristiche, la cui attuazione richiede risorse nettamente inferiori. Alla data della verifica dell'efficacia della strategia questo piano non era ancora stato recepito dal CC SNPC, ma nelle consultazioni preliminari aveva comunque riscontrato un ampio consenso. Trattandosi soltanto di una bozza preliminare sono necessari ulteriori lavori prima di poter introdurre sistematicamente l'analisi delle vulnerabilità TIC nell'Amministrazione federale. Nel complesso dobbiamo quindi dire che i lavori non sono avanzati come inizialmente previsto.

Outcome: attualmente non valutabile

> Alla data della verifica dell'efficacia della strategia esisteva solo una bozza preliminare del piano alternativo, la cui attuabilità verrà decretata in occasione dei primi pareri. Prima di un'eventuale decisione in merito all'adozione di questo approccio, il piano alternativo deve essere ulteriormente concretizzato. Una verifica dell'applicabilità del piano al di fuori dell'Amministrazione federale non è ancora avvenuta.

- Applicabilità del piano di verifica all'Amministrazione federale: la prevista verifica sistematica non ha avuto luogo in quanto la sua esecuzione è stata giudicata troppo onerosa in termini di risorse a fronte delle scarse disponibilità e nel quadro del budget stanziato. Solo dopo la finalizzazione del piano alternativo sarà possibile verificare in dettaglio l'applicabilità di un'analisi delle vulnerabilità TIC nell'Amministrazione federale.
- Decisione in merito all'applicazione al TIC dell'Amministrazione federale: non si è deciso ancora nulla, perché prima va verificato il piano alternativo.
- Verifica ai fini dell'applicazione del piano al di fuori dell'Amministrazione federale: una verifica in tal senso non ha ragione di essere se prima non viene presa una decisione in merito alla sua applicazione nell'Amministrazione federale.

Impact: attualmente non valutabile

> Considerando che non è stata presa una decisione in merito all'applicazione del piano di verifica e che il piano alternativo è in corso di elaborazione, l'impatto non può essere valutato. Finora la misura ha prodotto un unico effetto, ossia quello di sensibilizzare gli uffici responsabili dei vari dipartimenti sull'importanza delle analisi delle vulnerabilità.

3.3. M4 Prevenzione e continuità: Elaborazione della rappresentazione e dell'evoluzione della situazione

Titolo della misura	Elaborazione della rappresentazione e dell'evoluzione della situazione
Settore	Prevenzione
Obiettivi	Gli attori rilevanti e responsabili della politica, dell'economia e della società possono informarsi su eventi di importanza nazionale. Al riguardo, per i relativi ambiti di competenza vengono messe a loro disposizione delle analisi che informano sulla situazione e sulla sua evoluzione conformemente ai rispettivi livelli. Nel quadro del modello di PPP della centrale MELANI, tali informazioni sono centralizzate, valutate, analizzate e integrate al fine di fornire una rappresentazione della situazione. Le necessarie conoscenze specialistiche nel settore informatico e le capacità tecniche sono ampliate ed è rafforzata la piattaforma per lo scambio di informazioni su base volontaria con alcuni gestori di infrastrutture critiche e con l'economia.

Titolo della misura	Elaborazione della rappresentazione e dell'evoluzione della situazione
Ufficio/UO responsabile	MELANI, SIC
Documenti consultati per la verifica dell'efficacia	Fonti: [71], [72], [73], [74], [75], [76], [77], [78], [79]
Interviste	Si veda l'allegato A.1, intervista I 2

3.3.1. Effetto atteso: modello di efficacia

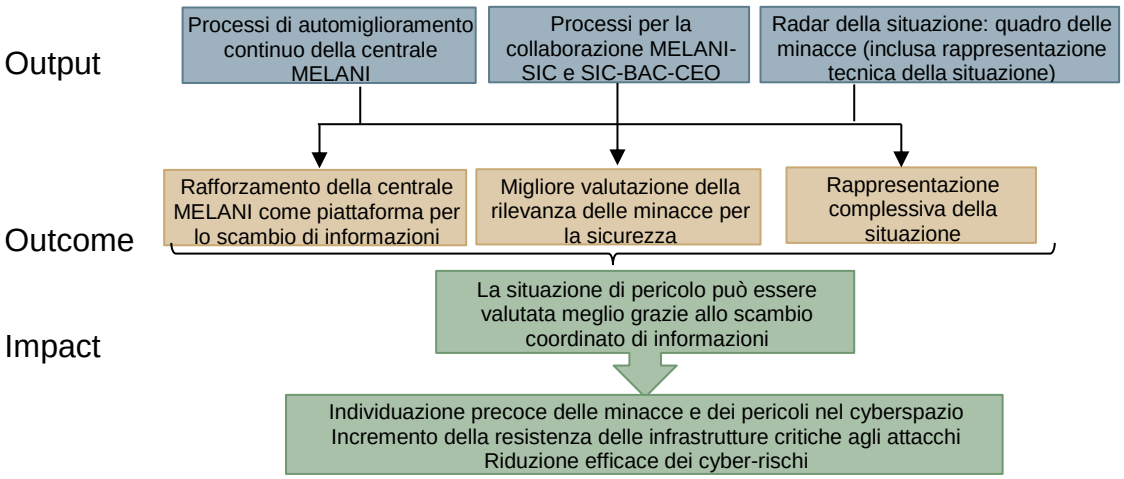

Figura 4: Modello di efficacia M4

3.3.2. Input: risorse assegnate

Tipo di risorsa	Numero di risorse assegnate alla SNPC
Risorse in termini di personale [Pool di risorse per M4, M5, M14]	3 MELANI-ODIC 3 MELANI-OIC (SIC) 7 SIC 1 SIM 4 BAC
Risorse finanziarie	Nessuna risorsa aggiuntiva
Collaborazione di altri uffici/UO	Uffici coinvolti oltre a MELANI, SIC, SIM e BAC: UFIT, SCOCI

Osservazioni sui posti nel SIC: i posti creati nel settore informatico (eccetto quelli nell'ambito dei servizi d'acquisto) vengono accorpati in una nuova UO (Cyber-SIC). Inoltre è stato creato il Commissariato informatico specializzato.

Tutti i collaboratori assunti hanno la qualifica necessaria per ricoprire questa posizione specialistica. Nello specifico dispongono non solo delle capacità tecniche ma anche delle necessarie soft skill. Meno utile ai fini del reclutamento è stato il fatto che si trattasse di contratti a tempo determinato.

L'entità delle risorse di personale richieste è stata valutata correttamente (le medesime risorse vengono utilizzate anche per M4 e M14, cfr. capitoli 3.4.2 e 3.6.2). Ciononostante

si stanno identificando nuove necessità, per esempio per l'elaborazione di nuovi prodotti o per analisi più specifiche e approfondite.

3.3.3. *Valutazione del raggiungimento degli obiettivi e della loro efficacia*

Livello	Obiettivi non raggiunti	Obiettivi raggiunti soltanto in parte	Obiettivi raggiunti in gran parte	Obiettivi raggiunti
Output			✓	
Outcome			✓	
Impact	◎ ottenuto			

3.3.4. *Motivazione della valutazione*

Output: gli obiettivi sono stati raggiunti in gran parte

I processi finalizzati all'automiglioramento della centrale MELANI e al rafforzamento della collaborazione MELANI-SIC e SIC-BAC-CEO sono già stati predisposti o i lavori in proposito sono in uno stadio avanzato. Un prototipo del radar della situazione è già disponibile. Il radar della situazione dovrà però essere ulteriormente sviluppato, così che possa fornire una rappresentazione complessiva della situazione.

Gli output definiti nel modello di efficacia sono stati conseguiti in gran parte.

- **Processi per l'automiglioramento continuo della centrale MELANI:** il programma di automiglioramento continuo della centrale MELANI è in corso di preparazione. Dovrà essere pronto entro fine 2016 ed essere esaminato separatamente da una società esterna. È basato sulle esigenze della clientela evidenziate nell'ambito della misura 13 e sul piano di rafforzamento della centrale MELANI come piattaforma per lo scambio di informazioni, piano peraltro già disponibile. I processi definiti nel programma di automiglioramento dovranno essere verificati nel corso di riunioni periodiche e all'occorrenza adeguati alla nuova situazione di pericolo.
- **Processi per la collaborazione MELANI-SIC e SIC-BAC-CEO:** i processi per la collaborazione tra MELANI e SIC, SIC e BAC-CEO nonché il coinvolgimento di partner internazionali sono definiti all'interno di una guida e messi in pratica. La collaborazione tra MELANI e SIC è ottima e ormai consolidata da molti anni. La collaborazione tra SIC e BAC-CEO è stata rafforzata grazie a una serie di opportune convenzioni sulle prestazioni.

  Dal punto di vista dei responsabili delle misure la collaborazione è buona anche perché nel settore informatico tutti si conoscono e possono avere uno scambio bilaterale di informazioni. La convenzione sulle prestazioni è ritenuta sufficiente, deve però essere costantemente verificata e all'occorrenza adeguata. All'interno della Confederazione gli attori rilevanti sono stati identificati e coinvolti; la loro collaborazione è sostanzialmente molto costruttiva e orientata ai compiti. Un aspetto non meno importante sono le riunioni di coordinamento, che si tengono a intervalli regolari sotto la direzione dell'MELANI-OIC tra i principali attori operativi e tecnici (GovCERT, BAC-CEO CNO, Cyber SIC, CSIRT-UFIT, MilCERT-DDPS e Cyber SIM), il cui scopo è fare un'analisi complessiva della situazione di pericolo e coordinare la gestione degli eventi.

- **Rappresentazione complessiva della situazione** (inclusa la rappresentazione tecnica): è stato creato un prototipo di rappresentazione della situazione di pericolo, il cosiddetto radar della situazione, presentato nella sua versione definitiva nell'autunno del 2016. Questo prodotto viene messo a disposizione delle infrastrutture critiche con informazioni specifiche per il settore e funge da strumento di monitoraggio. Le fonti di informazione per il radar sono le conoscenze del SIC, le analisi tecniche di GovCERT e le informazioni degli agenti di polizia, che confluiscono tramite SCOCI.

  Il radar della situazione dovrà però essere ulteriormente sviluppato, così che possa effettivamente fornire una rappresentazione complessiva della situazione. Al momento non si possono rappresentare casi complessi con tutti i relativi nessi. La qualità del radar della situazione dipende dal fatto che la centrale MELANI abbia risorse sufficienti per elaborare e inserire le informazioni rilevanti e dalla sua possibilità di rafforzare ulteriormente lo scambio di informazioni con le infrastrutture critiche.

Outcome: gli obiettivi sono stati raggiunti in gran parte

La creazione del radar della situazione ha reso disponibile uno strumento importante in grado di fornire una rappresentazione complessiva della situazione. Affinché la valutazione della situazione mostrata dal radar della situazione sia accurata e attuale, occorre incrementare maggiormente lo scambio di informazioni tra le persone coinvolte e i gestori di infrastrutture critiche.
Un primo passo in questa direzione è rappresentato dall'ulteriore ampliamento della CCC di MELANI. Ad oggi tuttavia manca un chiaro orientamento strategico per l'ulteriore sviluppo di questa cerchia.

- **Rafforzamento della centrale MELANI come piattaforma per lo scambio di informazioni:** dalla sua costituzione nel 2004 la centrale MELANI ha avuto una forte crescita ed è riuscita ad estendere maggiormente la sua CCC, costituita dai rappresentanti di infrastrutture critiche. Oggi aderiscono alla CCC più di 190 grandi imprese svizzere e unità amministrative, distribuite in dieci settori, che qui possono acquisire e condividere informazioni rilevanti ai fini della sicurezza. Per incrementare lo scambio di informazioni è necessario ampliare ulteriormente la CCC. Finora però non è ancora stata definita nessuna strategia che spieghi come si intende concretizzare tale ampliamento. Resta ancora da chiarire la questione della partecipazione allo scambio di informazioni di società che non fanno parte delle infrastrutture critiche. È necessario riflettere sulle idee per un «modello di cerchia» con varie CCC e i relativi diritti/doveri.
- **Migliore valutazione della rilevanza delle minacce per la sicurezza:** una volta ampliata la CCC si può migliorare anche la valutazione della rilevanza delle minacce per la sicurezza. Maggiore è il numero degli attori che partecipano allo scambio di informazioni, più precisa sarà la rappresentazione della situazione di pericolo. Le informazioni raccolte devono però essere anche interpretate con la dovuta cura, il che comporta spese supplementari. La portata e l'accuratezza dell'analisi sono limitate dalle risorse a disposizione [73]. Con le attuali risorse un ulteriore ampliamento è difficilmente realizzabile.
- **Rappresentazione complessiva ed evoluzione della situazione:** la creazione del radar della situazione ha permesso di avere uno strumento in grado di fornire un quadro d'insieme sempre attuale della situazione. Il radar fornisce infatti una rappresentazione in tempo reale. Inoltre si possono contattare gli attori interessati in breve tempo grazie al servizio di picchetto (incluso servizio SMS) attivo presso

l'MELANI-OIC 24 ore su 24, 7 giorni su 7. Le informazioni hanno già migliorato la capacità di azione, come mostrano gli esempi elencati di seguito.

– Attacchi DDoS: la collaborazione internazionale ha permesso allertare tempestivamente le aziende e di mettere in atto le opportune contromisure.
– Heartblead: la rappresentazione della situazione ha reso possibile una migliore valutazione delle minacce.
– Minaccia per il WEF annunciata dalla stampa: i chiari dati ottenuti con la rappresentazione della situazione hanno permesso di valutare correttamente che non vi è alcuna seria minaccia per il WEF.

L'ambizioso obiettivo di avere una rappresentazione complessiva della situazione può però essere raggiunto solo se vengono ulteriormente rafforzati lo scambio di informazioni e la collaborazione con tutti i partner coinvolti. Per adempiere pienamente al compito relativo alla misura 4 è stato necessario assegnare ulteriori risorse.

Impact: è stato ottenuto

Oggi la situazione di pericolo può essere oggetto di una migliore valutazione, in quanto lo scambio di informazioni tra gli attori SIC, MELANI, SIM, fornitori di prestazioni e gestori di infrastrutture critiche è coordinato. La creazione del Cyber SIC ha più volte consentito di individuare precocemente gli attacchi e le minacce. Il radar della situazione permette di avere una visione d'insieme delle minacce e di valutarne la rilevanza per la sicurezza della Svizzera.

Importante per valutare meglio la situazione è anche la maggiore capacità di attribuzione del SIC. Grazie all'intensa collaborazione degli attori e agli importanti contatti del SIC con i servizi partner sono sempre di più i casi in cui si riescono a identificare gli autori. Queste informazioni sono molto importanti per la valutazione della situazione (ulteriori informazioni cap. 3.6).

3.4. M5 Reazione: Analisi ed elaborazione di eventi

Titolo della misura	Analisi ed elaborazione di eventi
Settore	Reazione
Obiettivi	La Confederazione, i Cantoni e i gestori di infrastrutture critiche hanno verificato e sviluppato ulteriormente le rispettive misure di gestione di eventi. Le informazioni ottenute da eventi rilevanti (incidenti dovuti a malware, reti bot, cavalli di troia) vengono inoltrate a MELANI secondo i processi stabiliti sia all'interno che all'esterno della Confederazione. I gestori di infrastrutture critiche e i fornitori di prestazioni TIC ricevono, su richiesta, supporto tecnico da MELANI nell'elaborazione di eventi rilevanti. Le informazioni su eventi rilevanti per la protezione dello Stato in relazione ai cyber-rischi vengono inoltrate dal SIC a MELANI. I fornitori di prestazioni (CERT) sviluppano capacità tecniche per la sorveglianza delle reti della Confederazione. Le piattaforme e l'infrastruttura per riconoscere e contenere cyber minacce, come pure il supporto tecnico dei gestori di infrastrutture critiche sono allestiti. Presso i servizi federali rilevanti sono state anche ampliate le conoscenze specialistiche e le capacità forensi per riconoscere e contrastare le cyber minacce.
Ufficio/UO responsabile	MELANI e SIC
Documenti consultati per la verifica dell'efficacia	Fonti: [80], [81], [82], [83]

Interviste	Si veda l'allegato A.1, intervista I 10

3.4.1. *Effetto atteso: modello di efficacia M5*

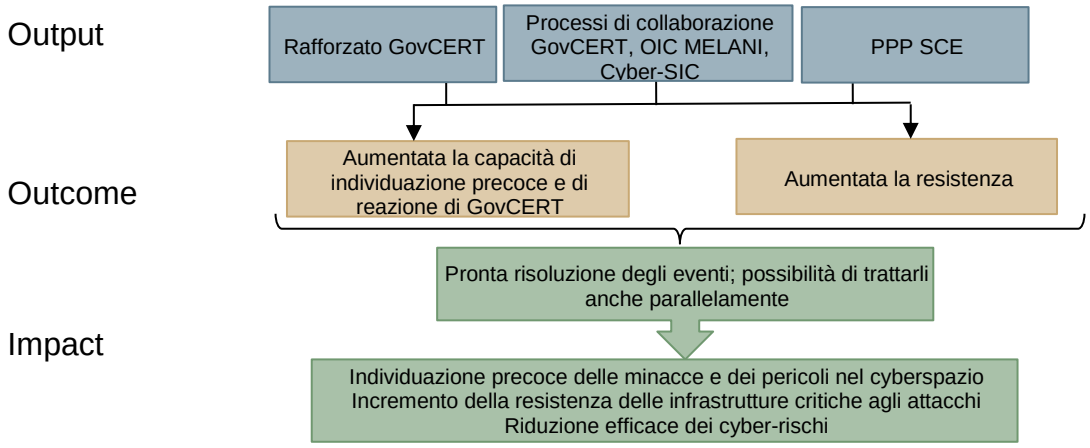

Figura 5: Modello di efficacia M5

3.4.2. *Input: risorse assegnate*

Tipo di risorsa	Numero di risorse assegnate alla SNPC
Risorse in termini di personale [Pool di risorse per M4, M5, M14]	3 MELANI-ODIC 3 MELANI-OIC (SIC) 7 SIC 1 SIM 4 BAC
Risorse finanziarie	Nessuna
Collaborazione di altri uffici/UO	Collaborazione con il CSIRT-UFIT

<u>Osservazioni sui posti in MELANI-ODIC e MELANI-OIC</u>

Per l'attuazione della SNPC è stata approvata la creazione di tre nuovi posti in GovCERT (MELANI-ODIC). Tre posti sono stati creati anche presso MELANI-OIC nel SIC. Attualmente (01.08.2016) GovCERT ha un tasso d'occupazione totale pari a 460 (il tasso previsto è 560). L'OIC occupa 8 FTE. Inizialmente veniva così garantita la normale gestione degli eventi. Oggi c'è anche la possibilità di gestire parallelamente due eventi di grandi dimensioni.

Grazie agli stretti contatti con uffici analoghi quali il CSIRT-UFIT e il CEO, per poter gestire un'eventuale crisi si può fare ricorso ad altre persone qualificate dell'Amministrazione federale.

Se dopo il 2017 le opportune risorse non fossero più disponibili, il compito principale della centrale MELANI (protezione delle infrastrutture critiche svizzere e supporto in caso di cyber-crisi) non potrebbe più essere assolto con la consueta qualità. Verrebbero a mancare le conoscenze tecniche e la qualità delle sinergie a livello nazionale e internazionale diminuirebbe in modo considerevole.

3.4.3. *Valutazione del raggiungimento degli obiettivi e della loro efficacia*

Livello	Obiettivi non raggiunti	Obiettivi raggiunti soltanto in parte	Obiettivi raggiunti in gran parte	Obiettivi raggiunti
Output			✓	
Outcome			✓	
Impact	◎ ottenuto			

3.4.4. *Motivazione della valutazione*

Output: gli obiettivi sono stati raggiunti in gran parte

Le capacità di gestione degli eventi sono state chiaramente incrementate. Questo grazie all'aumento delle risorse in GovCERT e presso MELANI-OIC e grazie a una migliore collaborazione di tutti gli attori. Perché la realizzazione sia completa manca ancora una piattaforma di comunicazione sicura per lo scambio di informazioni sugli eventi, la cui creazione è peraltro prevista.

- **Le unità operative di MELANI (GovCERT e MELANI-OIC) sono state rafforzate:** GovCERT ha potuto accrescere considerevolmente le proprie prestazioni grazie al miglioramento della situazione in termini di personale presso MELANI. Questo gli ha permesso di diventare oggi significativamente più resiliente di quanto non fosse solo qualche anno fa. Inoltre nel 2013 è stata definita la struttura organizzativa di GovCERT. Grazie al rafforzamento della sezione analitica di MELANI in seno al SIC (MELANI-OIC) è stato possibile gestire il maggior impegno lavorativo dedicato all'elaborazione delle informazioni in arrivo nell'ambito dell'analisi, della valutazione e della comunicazione con le infrastrutture critiche.
- **Il Cyber SIC è operativo:** la neocostituita unità Cyber SIC, aggregata al SIC, è molto attiva anche a livello internazionale. Analisi, fonti in rete e contatti internazionali hanno permesso di individuare precocemente gli eventi, di procedere ad attribuzioni e di classificare tempestivamente le minacce.
- **Sono stati definiti i processi per la collaborazione tra GovCERT, MELANI-OIC e Cyber SIC:** parallelamente al rafforzamento di GovCERT e MELANI-OIC, nell'ambito del Servizio delle attività informative sono stati ultimati i lavori di preparazione di un programma per la strutturazione delle cyber capacità del SIC e sono stati stabiliti i profili dei candidati per ricoprire la funzione di addetti all'analisi degli eventi. È stato anche organizzato e sviluppato il trasferimento di conoscenze su varie piattaforme di comunicazione, un sito web contenente un modulo di segnalazione di eventi e una MISP. Tra gli obiettivi raggiunti si segnalano anche il rafforzamento dei processi di condivisione delle conoscenze, l'aumento delle capacità di resistenza e di rilevazione e un migliore collegamento con i vari CERT nazionali e internazionali (grazie a contatti personali e all'adesione al FIRST e all'EGC). In caso di incident diventa così possibile analizzare e interpretare i dati in modo che l'organizzazione sotto attacco possa prendere contromisure tecniche. Grazie a piattaforme, strutture e processi ormai consolidati gli eventi trattati, che a quel punto possono essere considerati delle vere e proprie lezioni apprese, possono poi servire per attività di prevenzione, per aggiornare la rappresentazione delle minacce e in ultima analisi per ottimizzare la preparazione generale. Un obiettivo non ancora raggiunto è la prevista creazione di una piattaforma di comunicazione sicura, dove tutti gli attori rilevanti possono condividere in modo semplice e veloce informazioni sugli eventi.

- **È stata costituita la PPP SCE:** con questa PPP (un'associazione che riunisce i rappresentanti dell'industria TIC) è stata istituita una nuova organizzazione dotata di know-how specialistico a cui è possibile fare ricorso in caso di eventi gravi.

Outcome: gli obiettivi sono stati raggiunti in gran parte

Le aumentate capacità consentono di individuare più velocemente gli eventi e reagire più in fretta. Inoltre, si è riusciti anche a rafforzare le capacità di resistenza nel caso di minacce persistenti. Le risorse restano tuttavia ancora troppo esigue per riuscire a gestire le situazioni straordinarie. Bisogna altresì continuamente verificare quali ulteriori capacità specialistiche siano necessarie all'interno di GovCERT e di MELANI-OIC.

- **È stata incrementata la capacità di individuazione precoce e di reazione:** con l'approvazione della SNPC è stato allargato il compito di elaborazione degli eventi di MELANI. Affinché fosse possibile adempiere a questo compito, in GovCERT e in Cyber SIC sono state sviluppate sia le capacità di gestione delle minacce sia le capacità analitiche e forensi. Grazie a questo e alla rafforzata collaborazione tra GovCERT, CSIRT-UFIT e MELANI-OIC, unità aggregata al Servizio delle attività informative con funzioni di coordinamento, oggi è possibile individuare più velocemente gli eventi e rispondere con un'azione mirata. I gestori di infrastrutture critiche si dichiarano molto soddisfatti del supporto ricevuto dalla centrale MELANI (fonte: sondaggio nella CCC).

  Malgrado il potenziamento delle conoscenze acquisite, sono ravvisabili ancora lacune nelle conoscenze tecniche (in particolare l'aspetto della sicurezza dei sistemi SCADA). Qui la difficoltà risiede nel fatto che per ogni tipo di sistema sono necessarie conoscenze altamente specializzate. È pertanto indispensabile rafforzare ulteriormente la collaborazione con gli specialisti dei rispettivi settori.

- **La capacità di resistenza è stata aumentata:** in una situazione normale gli attuali posti sono sufficienti. Se dovessero verificarsi situazioni straordinarie che si protraggono per più giorni o settimane, le risorse disponibili sono insufficienti. In caso di contemporaneità di eventi, con le risorse attuali si arriverebbe presto al limite. Bisognerà quindi incrementare i contatti con i CERT dell'economia privata. Oltre ai buoni contatti esistenti con i CERT più grandi sarebbe opportuno inserire nella rete di MELANI anche dei team più piccoli, specialmente nel centro di competenze tecniche GovCERT.

Impact: è stato ottenuto

In vari casi in cui si sono dovute mettere alla prova le maggiori capacità di gestione degli eventi e si è visto che le misure adottate sono state pienamente efficaci.

Le conoscenze specifiche e le abilità delle sezioni operative di MELANI (GovCERT e MELANI-OIC) come pure la loro capacità di resistenza sono state impiegate per gestire eventi in maniera efficace. Grazie all'avvenuto incremento delle risorse oggi è possibile anche lavorare su più casi contemporaneamente. Migliorando l'individuazione precoce si riesce a reagire più prontamente agli eventi e a risolverli.

3.5. M6 Reazione: Documento programmatico per una panoramica dei casi penali e il coordinamento dei casi di portata intercantonale

Titolo della misura	Documento programmatico per una panoramica dei casi penali e il coordinamento dei casi di portata intercantonale
Obiettivi	Confederazione e Cantoni hanno fissato le modalità della loro futura collaborazione per il coordinamento dei casi di portata intercantonale in un documento programmatico che sarà sottoposto al Consiglio federale. Esso indica come ottenere, a livello nazionale, una panoramica per quanto possibile esaustiva dei casi (casi penali) e fornisce in tal modo informazioni sull'organizzazione delle interfacce con ulteriori attori nell'ambito della minimizzazione dei cyber-rischi e sui processi relativi al flusso di informazioni per la rappresentazione della situazione. Il coordinamento dei casi di portata intercantonale dovrà tenere conto degli sforzi internazionali già intrapresi per il perseguimento penale dei cyber-rischi. Il documento programmatico indica inoltre se a livello di Confederazione e Cantoni occorre adeguare le basi giuridiche e mettere a disposizione risorse per la sua realizzazione. Le informazioni evinte dalla panoramica dei casi (casi penali) e i dati concernenti casi risultanti dall'analisi tecnico-operativa del perseguimento penale nell'ambito dei procedimenti penali vengono trasmessi sistematicamente a MELANI. Per contro MELANI inoltra regolarmente a SCOCI informazioni rilevanti in ambito di diritto penale derivanti dalle sue conoscenze (informazioni del CERT e dei servizi di informazione). A tale scopo sono stati allestiti processi interni ed esterni alla Confederazione.
Ufficio/UO responsabile	SCOCI
Documenti consultati per la verifica dell'efficacia	Fonti: [84], [85], [86], [87], [88], [89]
Interviste	Si veda l'allegato A.1, intervista I 6

3.5.1. *Effetto atteso: modello di efficacia M6*

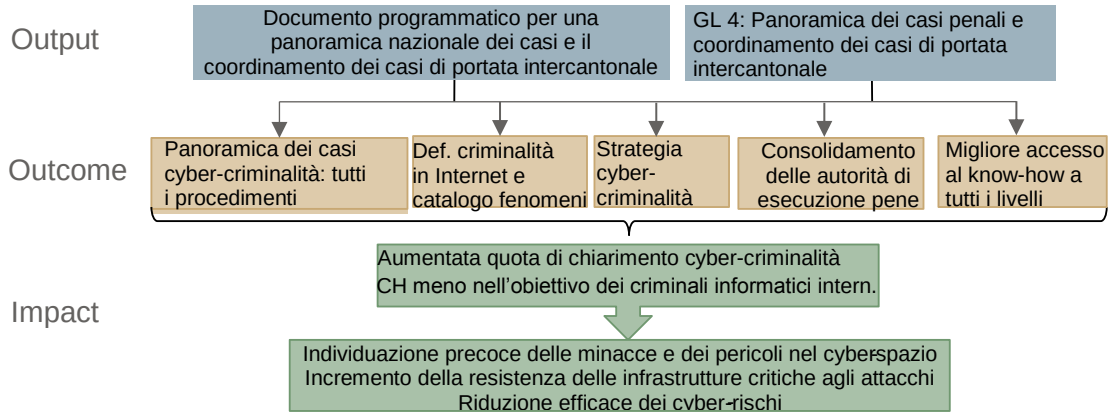

Figura 6: Modello di efficacia M6

3.5.2. *Input: risorse assegnate*

Tipo di risorsa	Numero di risorse assegnate alla SNPC
Risorse in termini di personale	Un posto (100 %) a tempo determinato per due anni.
Risorse finanziarie	Nessuna risorsa aggiuntiva
Collaborazione di altri uffici/UO	

Per l'attuazione della SNPC è stata approvata la creazione di un posto a tempo determinato (2 anni) con il compito di elaborare il documento programmatico. Il posto però è stato occupato solo per sei mesi. L'assunzione di personale idoneo per questo posto si è rivelata difficile.

3.5.3. *Valutazione del raggiungimento degli obiettivi e della loro efficacia*

Livello	Obiettivi non raggiunti	Obiettivi raggiunti soltanto in parte	Obiettivi raggiunti in gran parte	Obiettivi raggiunti
Output			✔	
Outcome		✖		
Impact	☐ attualmente non valutabile			

3.5.4. *Motivazione della valutazione*

<u>Output: gli obiettivi sono stati raggiunti in gran parte</u>

Il documento programmatico per la panoramica nazionale dei casi è pronto, ma deve ancora essere approvato. Nel corso dei lavori è emersa la necessità di avere una strategia globale sulla cyber-criminalità, che si estenda oltre il documento programmatico. Lo scambio con i Cantoni nel GL 4 è stato fruttuoso. Con SCOCI c'era già prima un buon coordinamento tra Confederazione e Cantoni nel settore della cyber-criminalità.

- **Documento programmatico «Panoramica nazionale dei casi e coordinamento dei casi di portata intercantonale»:** il documento esiste e nell'ottica odierna risulta completo. Nell'autunno del 2016 verrà sottoposto alla CDDGP e successivamente al Consiglio federale. Inizialmente il suo recepimento era previsto per la primavera del 2016; ma poi sono sopraggiunti ritardi in quanto gli accordi con i Cantoni, che fondamentalmente devono attuare il documento programmatico, hanno richiesto più tempo del previsto.

  Tutti gli addetti nelle funzioni interessate sono stati sufficientemente coinvolti nell'elaborazione del documento. MELANI ha contribuito con l'elenco dei requisiti per la rappresentazione della situazione e ha partecipato all'elaborazione del documento programmatico attraverso il GL 4 della RSS. All'inizio i Cantoni hanno assunto una posizione passiva, poiché per loro il significato e lo scopo di questa misura non erano chiari. Tuttavia, dopo aver ricevuto un catalogo dei fenomeni con una precisa definizione delle diverse forme di cyber-criminalità ne hanno capito l'utilità e hanno contribuito in modo fattivo all'elaborazione del documento programmatico.

  Il documento programmatico tuttavia non definisce nessuno dei processi necessari per il rilevamento dei casi e la redazione di una loro panoramica. In esso vengono solo illustrate varie possibilità su chi dovrebbe trasmettere quali informazioni e quando e dove consolidare tali informazioni per ottenere una panoramica dei casi. Queste questioni andranno chiarite una volta stabilita la strategia globale per il crimine informatico.

- **GL 4 Panoramica dei casi penali e coordinamento dei casi di portata intercantonale:** il GL 4 della RSS ha fornito un utile contributo alla preparazione del catalogo dei fenomeni, perché in quel contesto i Cantoni sono stati coinvolti direttamente nell'elaborazione delle definizioni di casi di cyber-criminalità. Il GL 4 è stato consultato nel quadro dei lavori di preparazione del documento programmatico

sulla panoramica dei casi, senza però una collaborazione diretta dei membri del gruppo. In linea di massima esiste già da molto tempo un'intensa collaborazione tra la Confederazione e i Cantoni tramite SCOCI. Per quanto riguarda il rafforzamento della collaborazione il GL 4 ha fornito un valore aggiunto solo limitato.

Outcome: gli obiettivi sono stati raggiunti soltanto in parte

Tuttora non esiste una panoramica completa dei casi riguardanti la cyber-criminalità in Svizzera, poiché non tutti i Cantoni rilevano i dati in proposito. Adesso però, grazie alle schede dei fenomeni preparate, abbiamo una descrizione dei diversi tipi di crimini informatici e una delimitazione degli uni rispetto agli altri. Per contro non si è riusciti a sciogliere il nodo della regolamentazione delle competenze, che resta una grossa criticità. La questione verrà affrontata nel corso dell'elaborazione della strategia globale sulla cyber-criminalità.

- **Panoramica nazionale dei casi:** in sede di preparazione del documento programmatico sulla panoramica dei casi sono stati consultati i Cantoni, che hanno espresso il loro parere anche in fase di consultazione. Attualmente non tutti i Cantoni effettuano una rilevazione dei dati relativi alla cyber-criminalità. Per questo motivo al momento non è possibile avere una panoramica esaustiva dei casi. La rilevazione dei dati avviene manualmente (SCOCI sta facendo un'azione proattiva nei confronti dei Cantoni). In merito alla procedura di coordinamento per la preparazione della panoramica dei casi si sta discutendo con i Cantoni e con il Ministero pubblico della Confederazione.
- **Definizione di criminalità su Internet e catalogo dei fenomeni di cyber-criminalità:** la creazione di un catalogo completo dei fenomeni relativi alle diverse forme di cyber-criminalità costituisce un importante passo in avanti verso la preparazione della panoramica dei casi e il rafforzamento della collaborazione nell'ambito dei procedimenti penali. Favorisce infatti la comprensione reciproca e aiuta a regolamentare le competenze. Un altro obiettivo riguarda la creazione di un'offerta di formazione per la polizia (moduli inseriti nell'offerta dell'Istituto svizzero di polizia).
- **Strategia sulla cyber-criminalità:** uno dei risultati dei lavori sulla M6 è stato quello di riconoscere la necessità di una strategia globale dei Cantoni sulla cyber-criminalità. Attualmente tale strategia è in fase di preparazione e sarà in linea con la SNPC. Il DFGP e la CDDGP verranno messi al corrente dei contenuti sia della M6 che della strategia globale, in modo che non ci siano divergenze. Tuttavia i lavori di elaborazione della strategia si trovano ancora in fase iniziale.
- **Consolidamento delle autorità di perseguimento penale:** i lavori relativi alla M6 hanno evidenziato il fatto che le competenze non sono sufficientemente definite. A questo proposito manca una giurisprudenza del Tribunale federale, per esempio in relazione ai casi di phishing. Comunque grazie a SCOCI la collaborazione tra Cantoni e Confederazione funziona.
- **Migliore accesso al know-how:** la formazione tecnica e analitica non è parte integrante della M6. Con le schede dei fenomeni si potrà migliorare la formazione dei poliziotti nell'ambito della cyber-criminalità.

Impact: non valutabile

Al momento l'obiettivo della riduzione della cyber-criminalità non è misurabile. Le autorità di perseguimento penale non dispongono ancora di una base di dati sufficiente per valutare questo aspetto. Considerato il forte aumento delle attività da parte dei criminali informatici, l'obiettivo più realistico è il contenimento dei casi di cyber-criminalità piuttosto che la loro effettiva riduzione.

3.6. M14 Reazione: Misure attive per l'identificazione degli autori

Titolo della misura	Misure attive per l'identificazione degli autori
Obiettivi	In caso di una minaccia specifica connessa a cyber-rischi, il SIC è in grado di identificare gli autori in collaborazione con partner esteri e con il sostegno di BAC e SIM in qualità di fornitori di prestazioni. Il Ministero pubblico della Confederazione riceve dal SIC informazioni sugli autori, sempreché ciò sia legale. Se non viene avviato un procedimento penale, il SIC prepara contromisure concrete conformemente alle basi legali vigenti.
Ufficio/UO responsabile	MELANI-OIC, SIC, ODIC
Documenti consultati per la verifica dell'efficacia	Fonti: [71], [72], [73], [74], [75], [76], [77], [78], [79]
Interviste	Si veda l'allegato A.1, intervista I 2

3.6.1. Effetto atteso: modello di efficacia M14

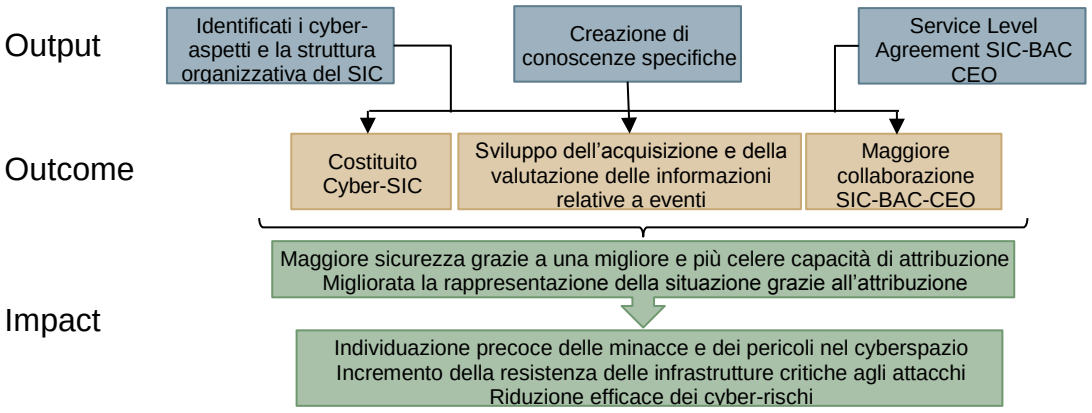

Figura 7: Modello di efficacia M14

3.6.2. *Input: risorse assegnate*

Tipo di risorsa	Numero di risorse assegnate alla SNPC
Risorse in termini di personale [Pool di risorse per M4, M5, M14]	3 MELANI-ODIC 3 MELANI-OIC (SIC) 7 SIC 1 SIM 4 BAC
Risorse finanziarie	Nessuna risorsa aggiuntiva
Collaborazione di altri uffici/UO	BAC, SIM, MELANI

Osservazioni

Si vedano le misure 4 (cap. 3.3) e 5 (cap. 3.4).

3.6.3. *Valutazione del raggiungimento degli obiettivi e della loro efficacia*

Livello	Obiettivi non raggiunti	Obiettivi raggiunti soltanto in parte	Obiettivi raggiunti in gran parte	Obiettivi raggiunti
Output			✓	
Outcome			✓	
Impact	◎ ottenuto			

3.6.4. *Motivazione della valutazione*

Output: gli obiettivi sono stati raggiunti in gran parte

> Il SIC ha definito le capacità di cui deve essere in possesso per identificare gli autori e ha creato e sviluppato le necessarie conoscenze specifiche al riguardo. La principale sfida resta l'analisi degli attori nelle più diverse regioni e del contesto in cui si muovono. In questo campo si devono acquisire ulteriori conoscenze specifiche.

- **Identificazione dei cyber-aspetti:** il SIC ha identificato le 8 capacità chiave seguenti per il lavoro che il Servizio delle attività informative deve svolgere nell'ambito dei crimini informatici [74]:
  - valutazione tecnica dei mezzi impiegati dagli autori degli attacchi;
  - acquisizione di informazioni finalizzata all'ottenimento di maggiori indicazioni sul modus operandi, gli obiettivi e il contesto in cui si muovono gli autori;
  - allineamento con le conoscenze già acquisite in merito agli attori e alle infrastrutture nell'ambito dei crimini informatici;
  - allineamento con le conoscenze già acquisite in merito a eventi simili occorsi in Svizzera e all'estero;
  - scambio situazionale di informazioni con servizi partner e coordinamento con le autorità di perseguimento penale;
  - valutazione e preparazione delle informazioni e delle conoscenze disponibili a livello strategico-operativo da sottoporre all'attenzione delle autorità decisionali politiche e adeguamento della stima della situazione di pericolo;
  - considerazione delle implicazioni di diritto internazionale;
  - concentrazione delle informazioni in rapporti di analisi e dei rischi.

Quando entrerà in vigore la nuova legge federale sulle attività informative (LAIn) si potranno rafforzare altre capacità nell'ambito delle contromisure attive.

- **Creazione di conoscenze specifiche:** in collaborazione con i partner MELANI-OIC, GovCERT e BAC-CEO, il SIC ha potuto raccogliere e sviluppare una serie di conoscenze specialistiche nei seguenti settori:
  – analisi dei dati di rete (analisi tecnica degli obiettivi di un attacco informatico e dei metodi utilizzati);
  – analisi dei malware (soprattutto l'ingegneria inversa e la correlazione con gli autori);
  – analisi degli attori (analisi dei rischi e correlazione con gli autori);
  – analisi contestuale (contesto e condizioni generali di un attacco informatico).

  Le capacità nel settore dell'analisi degli attori sono aggiornate ma ancora limitate a causa della scarsità di risorse.
- **Convenzione sulle prestazioni tra SIC e BAC-CEO:** per svolgere i propri compiti nell'ambito dei crimini informatici, il SIC si avvale talvolta del know-how tecnico di BAC-CEO. La convenzione sulle prestazioni tra le parti funge da base per questa collaborazione.

Outcome: gli obiettivi sono stati raggiunti in gran parte

La costituzione del Cyber SIC ha permesso di rafforzare e aggregare le competenze del SIC nell'ambito dei crimini informatici. L'acquisizione di informazioni funziona bene, ma la loro valutazione resta ancora difficile considerata la scarsità di risorse. Lo scambio di informazioni con il Ministero pubblico della Confederazione non è ancora ottimale.

- **Cyber SIC:** affinché il SIC fosse in grado di adempiere ai propri compiti nell'ambito dei crimini informatici è stata creata la nuova UO Cyber SIC. L'unità è ben consolidata nel suo ruolo e pienamente integrata nei processi del SIC. Ciò è avvalorato anche dai casi trattati nel 2015, quando furono scoperti e analizzati attacchi di Stato rilevanti per la Svizzera. Inoltre la Cyber SIC ha elaborato numerose analisi per il Consiglio federale e rapporti ufficiali per le autorità di perseguimento penale.
- **Acquisizione e valutazione delle informazioni:** MELANI-OIC è la piattaforma centrale per tutte le informazioni riguardanti i cyber-attacchi. L'acquisizione delle informazioni rilevanti per il tramite di Cyber SIC funziona bene. Le informazioni disponibili sono di qualità perlopiù sufficiente, non da ultimo grazie alla buona rete di fonti d'informazione nazionali e internazionali di Cyber SIC e di GovCERT in ambito tecnico. L'analisi, la valutazione e la contestualizzazione di queste informazioni è però onerosa in termini di risorse e resta ancora una grossa criticità. I processi per la trasmissione delle informazioni analizzate agli uffici competenti sono definiti.
- **Collaborazione tra SIC e Ministero pubblico della Confederazione:** il SIC invia rapporti al Ministero pubblico della Confederazione e si assicura che i dati necessari per il perseguimento penale siano correttamente raccolti e conservati. Il ritorno di informazioni dal Ministero pubblico della Confederazione è attualmente quasi ottimale. Talvolta succede che il Ministero pubblico della Confederazione non comunichi di aver chiuso un caso.

Impact: è stato ottenuto

L’impatto è stato illustrato con una serie di esempi che, per motivi di riservatezza, non possono essere ripresi nel presente rapporto. In ogni caso gli esempi documentano il fatto che gli autori sono stati identificati. Le informazioni riguardanti gli autori sono state utilizzate anche per preparare la valutazione della situazione, fornendo così un contributo sostanziale all’individuazione precoce dei rischi.

3.7. M13 Gestione delle crisi: Coordinamento delle attività con gli attori direttamente interessati e supporto con perizie specializzate

Titolo della misura	Coordinamento delle attività con gli attori direttamente interessati e supporto con perizie specializzate
Obiettivi	In caso di crisi gli attori interessati ricevono il supporto di MELANI che in via sussidiaria mette a loro disposizione conoscenze specialistiche. Lo scambio volontario di informazioni tra gestori di infrastrutture critiche, fornitori di prestazioni ICT e fornitori di sistemi è garantito, in modo da consolidare la continuità e la resistenza sulla base dell'autoaiuto. A tal fine sono stati ampliati i servizi attualmente disponibili. Se si verificano casi con possibili implicazioni di politica estera viene informato il DFAE, che viene così coinvolto nella pianificazione di opportune misure preventive.
Ufficio/UO responsabile	MELANI
Documenti consultati per la verifica dell'efficacia	Fonti: [117], [118], [119], [120], [121], [122], [123], [124], [125], [126]
Interviste	Si veda l'allegato A.1, intervista I 12

3.7.1. Effetto atteso: modello di efficacia M13

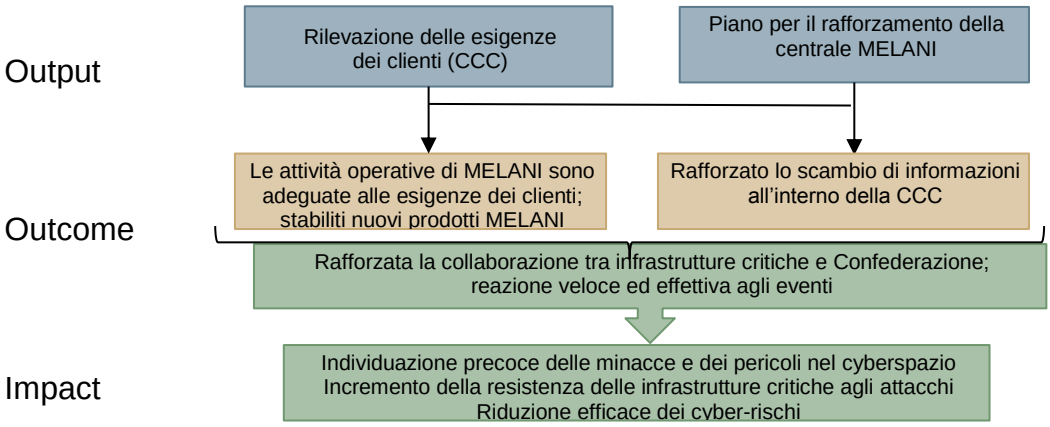

Figura 8: Modello di efficacia M13

3.7.2. Input: risorse assegnate

Tipo di risorsa	Numero di risorse assegnate alla SNPC
Risorse in termini di personale	Nessuna risorsa aggiuntiva
Risorse finanziarie	Nessuna risorsa aggiuntiva
Collaborazione di altri uffici/UO	SC SNPC

3.7.3. *Valutazione del raggiungimento degli obiettivi e della loro efficacia*

Livello	Obiettivi non raggiunti	Obiettivi raggiunti soltanto in parte	Obiettivi raggiunti in gran parte	Obiettivi raggiunti
Output			✔	
Outcome	☐ attualmente non misurabile			
Impact	☐ attualmente non misurabile			

3.7.4. *Motivazione della valutazione*

Output: gli obiettivi sono stati raggiunti in gran parte

Un sondaggio condotto all'interno della CCC ha permesso a MELANI di rilevare le esigenze dei gestori di infrastrutture critiche ivi rappresentati. Sulla base dei risultati ottenuti MELANI è ora in grado di adeguare i suoi servizi così da fornire un supporto ottimale ai gestori di infrastrutture critiche. Alla data della verifica dell'efficacia della strategia il sondaggio era terminato ma MELANI non aveva ancora formulato una strategia di adeguamento.

- **Rilevamento delle esigenze della CCC:** le esigenze dei gestori di infrastrutture critiche, che costituiscono la CCC di MELANI, sono state rilevate mediante un sondaggio online nel novembre 2015. Hanno risposto 260 su 424 membri. Il sondaggio evidenzia gli attuali punti di forza di MELANI, il potenziale di miglioramento e le esigenze dei membri della CCC. I risultati del sondaggio offrono a MELANI una buona base di partenza per le attività future.

  I membri della CCC sono sostanzialmente soddisfatti dei servizi che offre la centrale MELANI, da loro giudicata utile e importante. Le sfide future saranno il rafforzamento dei settori con meno membri, l'integrazione della CCC con gestori di infrastrutture critiche e altre informazioni ricavate dall'inventario per la protezione delle infrastrutture critiche, l'incentivazione della fiducia tra i membri della cerchia chiusa di clienti, il miglioramento della piattaforma per lo scambio di informazioni e la rapida diffusione di informazioni verificate su nuove minacce.

  L'analisi del sondaggio è terminata, tuttavia alla data della verifica dell'efficacia della strategia non erano ancora scaturite misure concrete.

- **Documento programmatico per il rafforzamento della centrale MELANI:** nell'ambito della misura 4 già nel febbraio del 2014 era stato elaborato un documento programmatico per il rafforzamento della centrale MELANI quale piattaforma per lo scambio di informazioni. Quel documento non tiene conto dei risultati del sondaggio, sulla base dei quali nell'estate 2016 il documento programmatico verrà modificato e quindi orientato alle esigenze della CCC. Stando a quanto comunicato dalla persona incaricata di elaborarlo, il documento programmatico considererà i seguenti temi:
  - garanzia dei servizi attualmente disponibili;
  - sviluppo dei settori già presenti;
  - ampliamento dei servizi di GovCERT.ch;
  - inclusione nella centrale MELANI di gestori di infrastrutture non critiche.

Outcome: attualmente non misurabile

Alla data della verifica dell'efficacia della strategia l'attuazione della misura 13 era appena cominciata. Di conseguenza non è possibile stabilire se MELANI abbia adeguato i suoi servizi alle esigenze della CCC e se lo scambio di informazioni abbia conseguentemente acquisito maggiore intensità.

Impact: attualmente non misurabile

Alla data della verifica dell'efficacia della strategia non si può ancora valutare l'impatto della misura 13.

3.8. M15 Gestione delle crisi: Documento programmatico per procedure e processi di condotta cibernetici

Titolo della misura	Documento programmatico per procedure e processi di condotta cibernetici
Obiettivi	È allestito un piano per procedure e processi di condotta volti alla soluzione tempestiva dei problemi, che tenga conto degli aspetti inerenti al cyberspazio. Anche la gestione delle crisi in generale è adeguata per i cyber-rischi e tiene conto degli aspetti inerenti al cyberspazio.
Ufficio/UO responsabile	CaF
Documenti consultati per la verifica dell'efficacia	Fonti: [117], [118], [119], [120], [121], [122], [123], [124], [125], [126]
Interviste	Si veda l'allegato A.1, intervista I 9

3.8.1. Effetto atteso: modello di efficacia M15

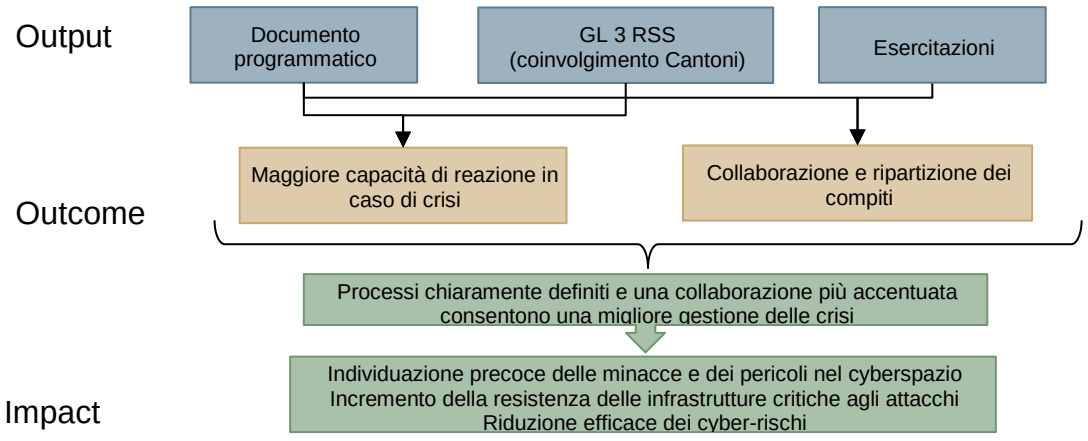

Figura 9: Modello di efficacia M15

3.8.2. *Input: risorse assegnate*

Tipo di risorsa	Numero di risorse assegnate alla SNPC
Risorse in termini di personale	Nessuna risorsa specifica per la SNPC
Risorse finanziarie	Nessuna risorsa aggiuntiva
Collaborazione di altri uffici/UO	SC SNPC

3.8.3. *Valutazione del raggiungimento degli obiettivi e della loro efficacia*

Livello	Obiettivi non raggiunti	Obiettivi raggiunti soltanto in parte	Obiettivi raggiunti in gran parte	Obiettivi raggiunti
Output			✔	
Outcome		✖		
Impact	☐ attualmente non valutabile			

3.8.4. *Motivazione della valutazione*

<u>Output: gli obiettivi sono stati raggiunti in gran parte</u>

La CaF ha preparato un documento programmatico per la gestione delle crisi che presentano aspetti inerenti al cyberspazio. Un elemento importante è stato riconosciuto, ovvero che gli aspetti inerenti al cyberspazio non rendono necessaria alcuna nuova forma di gestione delle crisi. L'attuale sistema di gestione delle crisi resta dunque valido. Per la gestione delle crisi nell'ambito dei crimini informatici occorre ampliare la rappresentazione della situazione e occorrono definizioni più chiare dei processi decisionali e delle responsabilità per la comunicazione. Il documento programmatico è stato ampliato durante i lavori del GL 3 della RSS e successivamente testato. Servono però ulteriori esercitazioni, di portata quanto più ampia possibile.

Documento programmatico: è stato allestito il documento programmatico per la gestione delle cyber-crisi che possono colpire la Confederazione. Un importante dato emerso durante i lavori di preparazione del documento è che la gestione delle crisi deve essere orientata ai processi e non agli scenari. Ciò significa che i processi decisionali e di condotta non devono cambiare se nella crisi sono coinvolti anche aspetti inerenti al cyberspazio. In caso di crisi di questo genere è fondamentale che gli attori aventi competenze nell'ambito dei crimini informatici (soprattutto MELANI) siano coinvolti nella gestione di queste crisi.

Il documento programmatico descrive due processi essenziali per la gestione delle crisi:

– **Rappresentazione unitaria della situazione:** la rappresentazione di un quadro aggiornato, unitario e completo della situazione è decisiva in caso di crisi. I relativi processi nell'ambito dei crimini informatici sono elaborati nel quadro della rappresentazione della situazione (misura 4).
– **Coordinamento:** non esiste a tutt'oggi un meccanismo decisionale chiaro e definito a livello strategico. Nella Confederazione vi sono numerosi stati maggiori di crisi. Spesso non c'è chiarezza su chi siano gli interlocutori competenti e manca una visione globale dei processi definiti. Ne consegue che

normalmente si utilizzano i canali di comunicazione privati (dove le persone si conoscono).

Esercitazioni: talvolta risulta difficile coinvolgere tutti gli attori interessati. Spesso questo avviene solo grazie a contatti personali, cosa che limita la cerchia delle parti interessate. Un'altra sfida è sensibilizzare i rappresentanti dei gruppi d'interesse affinché riescano a rendersi conto dei rischi. L'esercitazione più importante su come affrontare una crisi che presenta aspetti inerenti al cyberspazio è stata l'ECS 13, durante la quale è stata testata la gestione delle crisi a livello di Confederazione in presenza di uno scenario di attacco informatico su vasta scala contro la Svizzera. In quell'occasione la collaborazione tra i dipartimenti era prioritaria.

Outcome: gli obiettivi sono stati raggiunti soltanto in parte

La capacità di reazione non può essere giudicata soltanto in riferimento agli aspetti di una crisi inerenti al cyberspazio. In linea generale i piani di gestione delle crisi devono poggiare su basi più ampie, che prendano in considerazione la gestione di multi-crisi complesse. La collaborazione ha messo in evidenza il fatto che per svariati uffici i processi sono poco chiari. A complicare la situazione si aggiunge il fatto che in seno agli stati maggiori di crisi spesso si considerano ancora troppo poco gli aspetti inerenti al cyberspazio.

- **Maggiore capacità di reazione in caso di crisi:** durante i lavori si è capito che per valutare la capacità di reazione non si può focalizzare l'attenzione solo sull'aspetto della crisi inerente al cyberspazio. Le crisi fanno molto presto a colpire i settori più diversi (multi-crisi). Serve quindi un piano di gestione che poggi su basi più ampie e che si focalizzi anche su altri settori oltre a quello del cyberspazio (p. es. gestione della crisi in caso di perdita di infrastrutture critiche con ripercussioni sull'economia e sulla società).
- **Collaborazione:** per quanto riguarda la collaborazione ci sono ancora importanti sfide da affrontare. A livello di Confederazione va fatta chiarezza in merito al coordinamento tra i diversi stati maggiori di crisi. Benché a grandi linee le strutture di direzione della Confederazione per la gestione interdipartimentale delle crisi e i rispettivi ruoli e compiti siano definiti (si veda [117]), diverse questioni restano aperte.

  Spesso negli stati maggiori di condotta cantonali la tematica del cyberspazio non è stata ancora trattata. Di conseguenza anche l'integrazione di personale informatico specializzato all'interno degli organi cantonali di condotta non è ancora stata realizzata in toto. Nemmeno il supporto reciproco tra i Cantoni è disciplinato. Si ravvisa la necessità di creare un contenitore idoneo allo scambio delle informazioni, p. es. tramite il GL Sicurezza della CPS o la Conferenza dei capi cantonali di stato maggiore.

Impact: non valutabile

Nel corso dei lavori per la preparazione del documento programmatico e nel quadro delle esercitazioni la collaborazione è stata rafforzata. Ora i processi sono più chiari, ma resta da appurare se tutto ciò si traduce in una migliore gestione delle crisi. Pertanto al momento l'impatto non può essere valutato.

3.9. M9 Collaborazione internazionale: Internet governance

Titolo della misura	Internet governance
Obiettivi	Gli interessi delle autorità, dell'economia e della società svizzere sul tema Internet governance sono coordinati. Al riguardo sono stati definiti i relativi processi. La piattaforma di scambio ad approccio multistakeholder gestita dal DATEC sarà utilizzata dagli attori interessati per discutere tematiche riguardanti l'Internet governance. Gli interessi della Svizzera nel settore dell'Internet governance saranno rappresentati nei relativi organismi internazionali e nelle manifestazioni. La cooperazione con partner a livello internazionale è garantita.
Ufficio/UO responsabile	UFCOM
Documenti consultati per la verifica dell'efficacia	Fonti: [90], [91], [92]
Interviste	Si veda l'allegato A.1, intervista I 6

3.9.1. Effetto atteso: modello di efficacia M9

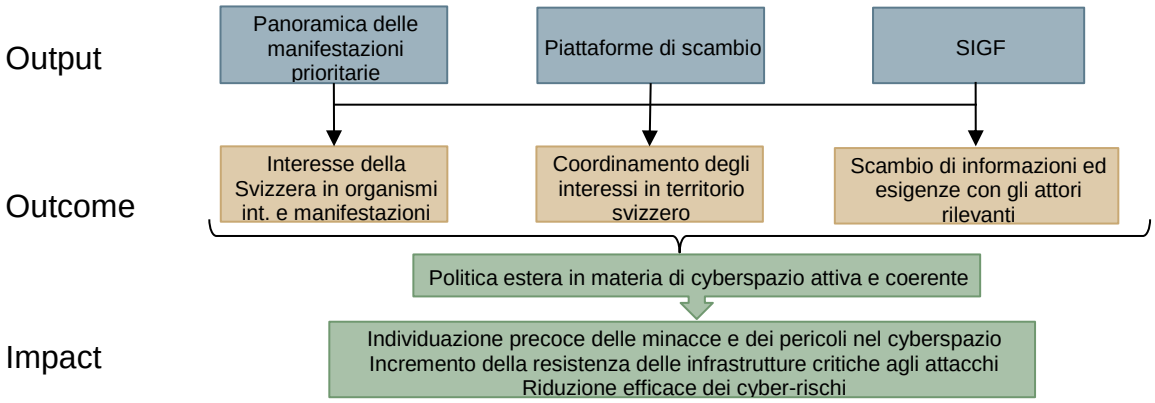

Figura 10: Modello di efficacia M9

3.9.2. Input: risorse assegnate

Tipo di risorsa	Numero di risorse assegnate alla SNPC
Risorse in termini di personale	Un posto nuovo (budget UFCOM)
Risorse finanziarie	Nessuna risorsa aggiuntiva (budget ordinario UFCOM)
Collaborazione di altri uffici/UO	DFAE, MELANI

3.9.3. Valutazione del raggiungimento degli obiettivi e della loro efficacia

Livello	Obiettivi non raggiunti	Obiettivi raggiunti soltanto in parte	Obiettivi raggiunti in gran parte	Obiettivi raggiunti
Output				✓✓
Outcome			✓	
Impact	☐ attualmente non valutabile			

3.9.4. *Motivazione della valutazione*

Output: gli obiettivi sono stati raggiunti

> Si è ottenuta una panoramica degli attori e delle manifestazioni più importanti nell'ambito della Internet governance. Grazie all'utilizzo di formati già disponibili e altri di nuova creazione si potrà garantire lo scambio con tutte le parti interessate della pubblica amministrazione, dell'economia e della società.

- **Internet governance e manifestazioni:** sono rappresentate tutte le istituzioni rilevanti che si occupano di Internet governance. La priorità 1 è stata assegnata alle organizzazioni e agli organismi internazionali che hanno un ruolo fondamentale nella Internet governance e che si occupano in primo luogo di questioni relative a Internet, siano esse di natura tecnica o politica. A tutte le altre istituzioni è stata assegnata la priorità 2 o 3. Una volta pronta, questa panoramica andrà aggiornata a intervalli regolari.
- **Piattaforme di scambio:** nell'elenco degli organismi sono definite le modalità di funzionamento dello scambio di informazioni (si veda [91]).
  - Scambio all'interno della Confederazione: come canale d'informazione interno alla Confederazione si utilizza la piattaforma ch@world, che consente di informare i vari uffici federali sulle consultazioni che li riguardano, così da poter far loro pervenire le informazioni nei termini previsti. Lo scambio avviene anche attraverso i canali tradizionali (e-mail, telefono) e sporadicamente approfondito in occasione di incontri informali durante la pausa pranzo.
  - Scambio con l'economia e la società civile: la piattaforma tripartita, creata nel 2003, viene utilizzata dall'UFCOM per discussioni sul tema della Internet governance e per la divulgazione di informazioni. La piattaforma prevede due riunioni annuali e una mailing list. Attualmente il gruppo dei destinatari comprende 100 persone, la metà delle quali appartiene all'Amministrazione federale.
  - SIGF: questo forum, creato quale nuova piattaforma di scambio, offre a tutti gli interessati la possibilità di divulgare informazioni sulle proprie attività nell'ambito della Internet governance (approccio bottom-up) e nella sua essenza è complementare alla piattaforma tripartita, dove le informazioni vengono fornite principalmente dall'UFCOM. Il formato si è dimostrato valido. Infatti nel 2016 circa 100 persone hanno partecipato alla manifestazione annuale del SIGF.

Outcome: gli obiettivi sono stati raggiunti in gran parte

> Gli interessi della Svizzera nell'ambito della Internet governance sono coordinati. Lo scambio funziona bene, soprattutto tra DFAE-DPS e UFCOM. Al momento la DSC e la SECO partecipano troppo poco a questo coordinamento.
> Gli interessi dell'economia e della società vengono recepiti, anche se la partecipazione dell'economia privata è stata finora modesta.

- **Coordinamento degli interessi della Svizzera presso organismi internazionali e conferenze:** all'interno dell'Amministrazione federale lo scambio di informazioni sulla Internet governance è intenso soprattutto tra UFCOM e DFAE, che fin da quando è iniziata l'attuazione della M9 hanno rinsaldato le già buone relazioni. Il risultato è avere una buona condivisione di informazioni già prima di partecipare alle conferenze internazionali, affinché le delegazioni svizzere vi possano arrivare forti di posizioni consolidate. Il coordinamento avviene nell'ambito del gruppo specialistico

Cyber-International (cfr. cap. 3.10), che opera sotto la guida della DPS. Esempi dei successi ottenuti dalla rappresentanza congiunta degli interessi sono: la presidenza del rappresentante svizzero al comitato consultivo governativo dell'ICANN, la partecipazione coordinata al processo WSIS dell'ONU e il lancio comune della Geneva Internet Platform da parte del DFAE e dell'UFCOM.

Oltre allo scambio tra UFCOM e DPS, partecipa al coordinamento anche MELANI. Per contro manca uno scambio regolare con la DSC e la SECO su questioni concernenti la Internet governance.

- **Coordinamento degli interessi in ambito svizzero e scambio di informazioni:** grazie all'utilizzo della piattaforma tripartita e del nuovo SIGF si possono recepire tempestivamente i diversi interessi, così da poterne tener conto. Inoltre l'UFCOM fornisce informazioni anche mediante newsletter e articoli in riviste specializzate. Resta comunque un compito difficile riuscire a coinvolgere un pubblico quanto più ampio possibile nelle attività riguardanti la Internet governance. Poiché i processi all'interno degli organismi internazionali sono spesso molto lunghi e si svolgono su un piano alquanto astratto, l'impegno dell'economia privata resta modesto. Ne consegue che i loro interessi sono considerati perlopiù solo indirettamente.

Impact: non valutabile

Lo stretto coordinamento ha generato una politica estera coerente in materia di cyberspazio. I principi di base della Svizzera riguardo alla Internet governance (approccio multistakeholder) sono noti e sono rappresentati in maniera unitaria. Tuttavia al momento non si può evincere se la posizione della Svizzera ne risulta rafforzata. Per questo motivo l'impatto non può ancora essere valutato.

3.10. M10 Collaborazione internazionale: Cooperazione a livello di politica internazionale di sicurezza

Titolo della misura	Cooperazione a livello di politica internazionale di sicurezza
Obiettivi	Gli interessi dell'economia, della società e delle autorità sono coordinati al livello della politica di sicurezza internazionale in materia di cyber-rischi. La cooperazione internazionale per far fronte alla minaccia presente nel cyberspazio in collaborazione con altri Stati e organizzazioni internazionali è garantita.
Ufficio/UO responsabile	DFAE
Documenti consultati per la verifica dell'efficacia	Fonti: [98], **Fehler! Verweisquelle konnte nicht gefunden werden.**, [100], [101], [102], [103], [104], [105], [106], [107], [108], [109], [110], [111], [112], [113], [114], [115], [116]
Interviste	Si veda l'allegato A.1, intervista I 4

3.10.1. *Effetto atteso: modello di efficacia M10*

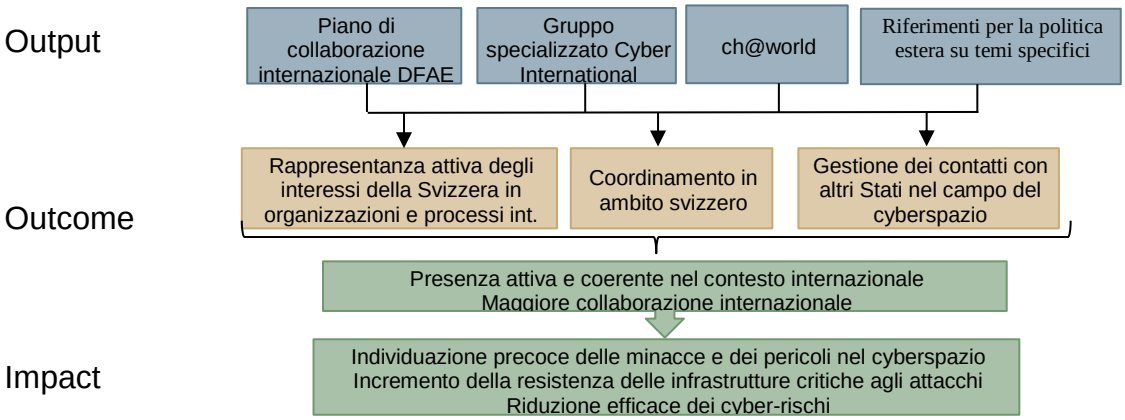

Figura 11: Modello di efficacia M10

3.10.2. *Input: risorse assegnate*

Tipo di risorsa	Numero di risorse assegnate alla SNPC
Risorse in termini di personale	2 collaboratori
Risorse finanziarie	CHF 150 000 all'anno
Collaborazione di altri uffici/UO	MELANI, SC SNPC, DFGP, DDPS, UFCOM, IFSN

3.10.3. *Valutazione del raggiungimento degli obiettivi e della loro efficacia*

Livello	Obiettivi non raggiunti	Obiettivi raggiunti soltanto in parte	Obiettivi raggiunti in gran parte	Obiettivi raggiunti
Output				✓✓
Outcome				✓✓
Impact	☐ attualmente non valutabile			

3.10.4. *Motivazione della valutazione*

<u>Output: gli obiettivi sono stati raggiunti</u>

È stata creata la base per una politica estera e di sicurezza in materia di cyberspazio coordinata e coerente. In un documento programmatico sulla collaborazione internazionale è chiaramente definito il ruolo della DPS del DFAE. Con la costituzione del gruppo specialistico Cyber International è stato istituito un organismo di scambio ed è stata intensificata la comunicazione sulla piattaforma ch@world. Sono stati anche predisposti riferimenti per la politica estera in materia di cyberspazio.

- **Piano di collaborazione internazionale:** il piano è pronto. Si tratta di un documento che illustra il ruolo, le attività e le iniziative in cui è coinvolto il DFAE, sia che operi in veste di responsabile o di supporto. Inoltre una volta all'anno la DPS prepara una panoramica delle principali attività, dei processi e delle iniziative nell'ambito del cyberspazio destinata al capodipartimento e al segretario di Stato del DFAE nonché

al comitato direttivo della SNPC per loro opportuno aggiornamento (si veda [98] per il 2014 e **Fehler! Verweisquelle konnte nicht gefunden werden.** per il 2015).

- **Gruppo specialistico Cyber International:** questo gruppo specialistico raggruppa i rappresentanti del DFAE (Direzione politica e Direzione del diritto internazionale pubblico), del DDPS (Sipol, UFPP, Aggruppamento Difesa e SIC), DATEC (UFCOM e UFE), DFF (ODIC) e DFGP (UFG e fedpol), a cui recentemente si è aggiunto quello dell'IFSN. Tutti i rappresentanti si impegnano attivamente. Questo organismo tiene un atteggiamento aperto nei confronti di altri uffici federali che si occupano delle tematiche cyber-sicurezza e Internet governance a livello internazionale. Il gruppo specialistico Cyber International è presieduto dalla DPS e si riunisce due volte all'anno. Se necessario, uno qualsiasi dei membri può convocare una riunione straordinaria.
- **ch@world:** per facilitare lo scambio di informazioni, su ch@world è stata creata una piattaforma per lo scambio delle informazioni tra i membri del gruppo specialistico Cyber International, dove i membri possono caricare documenti in totale autonomia. Questa piattaforma viene regolarmente utilizzata, in modo particolare per la partecipazione a consultazioni (p. es. per la «Geneva Declaration for Cyberspace»).
- **Riferimenti per la politica estera:** i riferimenti per la politica estera coprono i principali settori d'intervento, che vengono (ulteriormente) sviluppati in funzione della rilevanza per la politica estera e secondo le necessità. Un tema attuale riguarda la gestione dei contenuti legati all'estremismo violento in Internet e nei social media.

Outcome: gli obiettivi sono stati raggiunti

Nell'ambito della cyber-sicurezza la Svizzera rappresenta in maniera attiva e coerente i propri interessi nell'ambito degli organismi internazionali e intrattiene buoni contatti bilaterali. Il nostro Paese è reputato un attore attivo e affidabile.
Lo scambio tra tutti gli uffici federali coinvolti è ormai consolidato. Questo risultato è direttamente riconducibile alla creazione del gruppo specialistico Cyber International e all'utilizzo della piattaforma ch@world.

- **Rappresentanza attiva degli interessi della Svizzera presso organismi internazionali e gestione dei contatti con altri Stati nell'ambito del cyberspazio:** la DPS ha rappresentato la Svizzera in numerose negoziazioni internazionali e processi inerenti alla politica di cyber-sicurezza. Nel corso di queste attività si intrattengono anche rapporti bilaterali con diversi Paesi. La Svizzera è reputata un attore attivo e affidabile nell'ambito del cyberspazio, come dimostrano svariate richieste di supporto pervenute da altri Stati nell'elaborazione di strategie di cyber-sicurezza (p. es. partecipazione della Svizzera ad audizioni pubbliche in Armenia e Serbia, supporto per la creazione di CERT ecc.). Di seguito sono riassunte le principali attività e i risultati prodotti.
  - processo OSCE: consolidamento della fiducia nel cyberspazio. Promozione di misure volte a rafforzare la fiducia sotto la presidenza svizzera dell'OSCE nel 2014. Sono stati approvati due pacchetti di misure.
    - Partecipazione attiva della Svizzera alla «Global Conference on Cyberspace» e organizzazione del workshop «Mechanisms for Confidence-Building and Cooperation in Cyberspace» a Ginevra come contributo svizzero alla conferenza suddetta.
    - Partecipazione del GCSP al «Sino-European Cyber Dialog» (2014-2016) in occasione del quale è stato creato un gruppo di lavoro incaricato di esaminare la questione dell'applicabilità del diritto internazionale al cyberspazio.

  - ICT4Peace: progetti per lo sviluppo delle capacità nell'ambito del cyberspazio nei Paesi in sviluppo.
  - collaborazione alla stesura del Manuale Tallinn della NATO (studio sull'applicabilità del diritto internazionale nel cyberspazio).

- **Coordinamento degli interessi in ambito svizzero per una presenza più coerente nel contesto internazionale:** un importante valore aggiunto del gruppo specialistico Cyber International è lo scambio regolare di informazioni tra i servizi. Allo stesso scopo serve anche la piattaforma ch@world, diventata anche una banca dati completa dei principali documenti. Grazie a questi strumenti è stato possibile migliorare la coerenza della politica estera in materia di cyberspazio. All'occorrenza occorrerebbe aumentare la frequenza delle riunioni. Inoltre va precisato che, a seconda del tema trattato, occorre coinvolgere nel progetto partner che non aderiscono al gruppo specialistico Cyber International.

Impact: attualmente non valutabile

La Svizzera applica una politica estera attiva e coerente per quanto riguarda i cyber-rischi. Investe energie per consolidare i rapporti con altri Stati e si impegna a fornire un contributo alla cyber-sicurezza internazionale. Dato che questi sforzi esplicano il loro effetto nel lungo termine, al momento non è possibile misurarne l'impatto.

3.11. M11 Collaborazione internazionale: Iniziative internazionali e processi di standardizzazione nel settore della sicurezza

Titolo della misura	Iniziative internazionali e processi di standardizzazione nel settore della sicurezza
Obiettivi	Gli interessi della piazza economica svizzera vengono portati negli organismi internazionali privati e pubblici che operano nel settore della sicurezza, delle tutele e della standardizzazione dopo essere stati coordinati in ambito nazionale. A tal fine è stato intensificato lo scambio di informazioni tra gestori di infrastrutture critiche, fornitori di prestazioni TIC, fornitori di sistemi, associazioni, organizzazioni di standardizzazione nazionali, autorità specializzate e regolatori. È stato inoltre stabilito un processo al riguardo.
Ufficio/UO responsabile	UFCOM
Documenti consultati per la verifica dell'efficacia	Fonti: [93], [94], [95], [96], [97]
Interviste	Si veda l'allegato A.1, intervista I 6

3.11.1. *Effetto atteso: modello di efficacia M11*

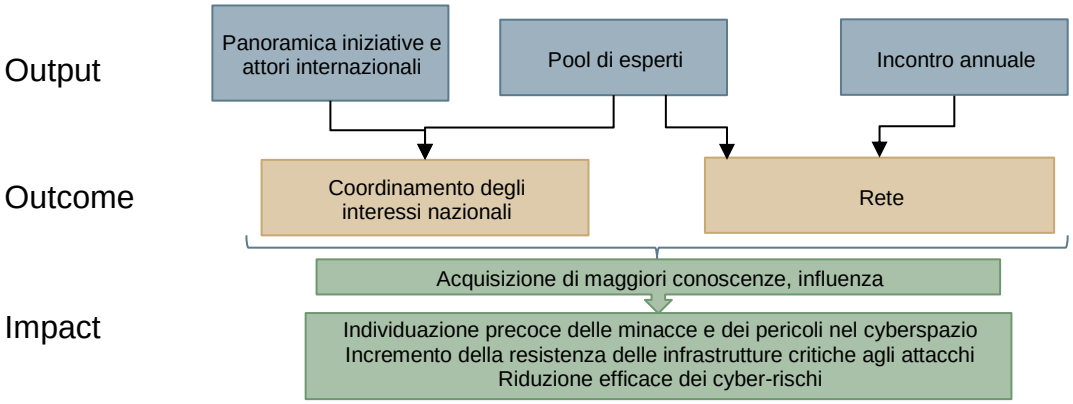

Figura 12: Modello di efficacia M11

3.11.2. *Input: risorse assegnate*

Tipo di risorsa	Numero di risorse assegnate alla SNPC
Risorse in termini di personale	Nessuna. L'UFCOM si è assunto questo compito senza bisogno di ulteriori risorse
Risorse finanziarie	Nessuna risorsa aggiuntiva
Collaborazione di altri uffici/UO	SC SNPC

3.11.3. *Valutazione del raggiungimento degli obiettivi e della loro efficacia*

Livello	Obiettivi non raggiunti	Obiettivi raggiunti soltanto in parte	Obiettivi raggiunti in gran parte	Obiettivi raggiunti
Output			✔	
Outcome		✖		
Impact	☐ attualmente non valutabile			

3.11.4. *Motivazione della valutazione*

<u>Output: gli obiettivi sono stati raggiunti in gran parte</u>

Sono stati definiti gli obiettivi intermedi della pianificazione strategica ed è stata creata una rete di attori disponibili a condividere informazioni sulle questioni riguardanti le iniziative internazionali e i processi di standardizzazione. Non vi è grande interesse dell'economia privata a una partecipazione diretta. Si è tenuto un primo workshop (a cadenza potenzialmente annuale) sul tema degli attuali sviluppi internazionali.
Tra gli attori della M11 non è stata identificata una concreta necessità di coordinamento, né altre parti hanno manifestato una tale necessità alla M11. Le conoscenze specialistiche in possesso degli attori della rete sono documentate da elenchi e relazioni. Resta però ancora da capire se possano essere utilizzate per la SNPC in un contesto più ampio.

- **Panoramica delle iniziative internazionali che vedono la partecipazione degli attori svizzeri:** la panoramica esiste ([96]) e va aggiornata una volta all'anno. Consiste in un elenco di attori che seguono ed esercitano la loro influenza su quanto avviene nell'ambito delle organizzazioni e delle iniziative internazionali sul tema della cyber-sicurezza. Questo elenco è suddiviso in due categorie, con intenzioni diverse:
  – attori che rappresentano autorità, servizi specializzati e regolatori;
  – attori che rappresentano organizzazioni dell'economia privata e istituti di formazione.

  L'elenco è basato sull'adesione volontaria. Di tutte le organizzazioni interpellate nell'ambito della M11 ha risposto solo un terzo. Mancano grosse aziende con succursali in Svizzera, che sono rappresentate in seno a organismi internazionali ma non si considerano attori svizzeri (p. es. Google, Microsoft, Cisco).
- **Pool di esperti su questioni inerenti alla standardizzazione nel settore della sicurezza:** tra i partecipanti ci sono anche esperti su questioni diverse riguardanti i processi internazionali nell'ambito dei cyber-rischi. D'intesa con i partecipanti occorre focalizzare maggiormente l'attenzione del gruppo. Un primo workshop verteva sulle questioni riguardanti la creazione di CERT. Non si ravvede l'esigenza di intensificare il coordinamento in relazione alla SNPC, in quanto lo scambio tra i rappresentanti in seno alle organizzazioni internazionali di standardizzazione è già proficuo.

Outcome: gli obiettivi sono stati raggiunti soltanto in parte

Nel corso di un primo workshop è stata potenziata la rete. Si è costituito un gruppo di 30-40 partecipanti interessati alle questioni della standardizzazione e delle buone prassi. Per contro non si sente l'esigenza di coordinare il tema della standardizzazione internazionale: gli interessi si concentrano piuttosto sugli sviluppi a livello nazionale.

- **Coordinamento degli interessi nazionali:** finora su questo tema non sono stati raccolti risultati né si ravvedono esigenze in tal senso. Per ora la priorità è la creazione e lo sviluppo della rete. La maggior parte dei partecipanti è interessata agli sviluppi sul piano nazionale, non al coordinamento sul piano internazionale.
- **Rete:** si è tenuto un primo workshop con circa 40 partecipanti, nel quale si è discusso principalmente dei controlli e delle conseguenti reazioni («Monitoring and response»). Il workshop è stato utile per consolidare la rete. Tuttavia non è chiaro se per i partecipanti il tema della standardizzazione è sufficientemente rilevante da indurli a continuare il loro impegno nell'ambito della M11.

Impact: attualmente non valutabile

È ancora troppo presto per valutare l'impatto in maniera completa. Gli esperti che fanno parte della rete hanno senz'altro dimostrato di possedere buone conoscenze e la capacità di esercitare un'influenza. Tuttavia sul fronte internazionale non si delinea alcuna un'azione coordinata in tal senso da parte dei rappresentanti della Svizzera.

3.12. M1 Formazione e ricerca: Identificazione di cyber-rischi attraverso la ricerca

Titolo della misura	Identificazione di cyber-rischi attraverso la ricerca
Obiettivi	I servizi federali responsabili intrattengono regolari scambi reciproci e con attori esterni all'Amministrazione federale riguardo agli sviluppi attuali e agli sviluppi da sottoporre a ricerca correlati ai cyber-rischi in Svizzera e all'estero. Inoltre, se necessario, eseguono pertinenti attività di ricerca intra muros o le assegnano all'esterno.
Ufficio/UO responsabile	SEFRI, SC SNPC
Documenti consultati per la verifica dell'efficacia	Fonti: [16], [17], [18], [19], [20], [21], [22], [23], [24], [25], [26], [27], [28], [29], [30], [31], [32]
Interviste	Si veda l'allegato A.1, intervista I 1

3.12.1. *Effetto atteso: modello di efficacia M1*

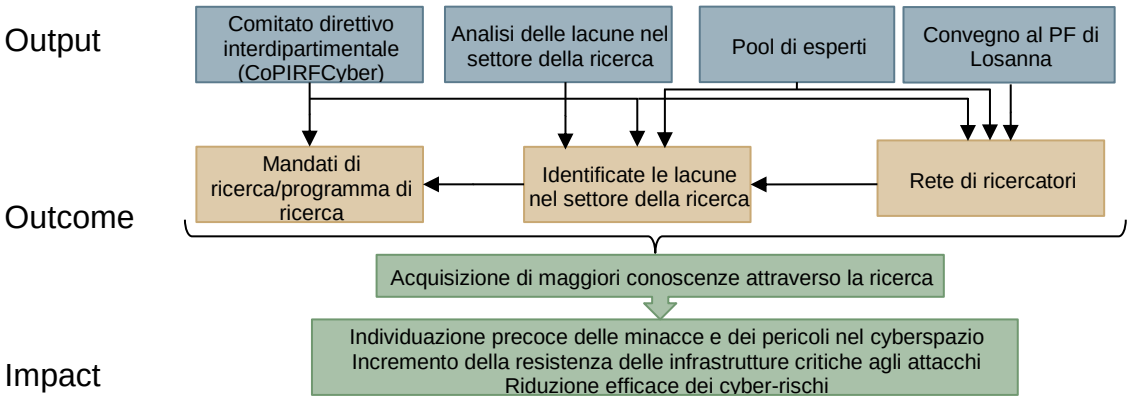

Figura 13: Modello di efficacia M1

3.12.2. *Input: risorse assegnate*

Tipo di risorsa	Numero di risorse assegnate alla SNPC
Risorse in termini di personale	Nessun posto nuovo creato.
Risorse finanziarie	Nessuna risorsa aggiuntiva; gli esperti provenienti dalle scuole universitarie offrono il loro impegno a titolo puramente onorifico.
Collaborazione di altri uffici/UO	DFAE SDP, UFCOM, BAC-CEO, SIM, CTI, UFAE, MELANI, RSS

La SEFRI si è assunta la responsabilità per l'attuazione della misura nel 2014 e sostiene in prima persona le spese per il personale.

3.12.3. *Valutazione del raggiungimento degli obiettivi e della loro efficacia*

Livello	Obiettivi non raggiunti	Obiettivi raggiunti soltanto in parte	Obiettivi raggiunti in gran parte	Obiettivi raggiunti
Output				✓✓
Outcome			✓	
Impact	☐ attualmente non valutabile			

3.12.4. *Motivazione della valutazione*

Output: gli obiettivi sono stati raggiunti

Grazie alla creazione di un comitato direttivo interdipartimentale per la ricerca e la formazione nell'ambito dei cyber-rischi, diretto dalla SEFRI, il coordinamento in questo settore è garantito. I primi passi verso il rafforzamento della ricerca sono fatti. È stato nominato un gruppo di esperti composto da rappresentanti delle scuole universitarie svizzere con il compito di identificare le esigenze prioritarie di ricerca in Svizzera. Con la prima «Swiss Cyber Risk Research Conference» è stata rafforzata la rete di ricercatori ed è stato lanciato un segnale all'esterno che manifestano l'intenzione della Confederazione di incentivare la ricerca nel settore dei cyber-rischi.

- **Creazione di un comitato direttivo interdipartimentale:** è stato creato il CoPIRFCyber diretto dalla SEFRI. Nel comitato sono rappresentati gli uffici federali interessati alle questioni riguardanti la formazione e la ricerca nell'ambito dei cyber-rischi. Il comitato si riunisce quattro volte all'anno (o in caso di necessità). In questo settore esso coordina le attività normative dell'Amministrazione federale.
- **Pool di esperti e analisi delle lacune nel settore della ricerca:** per garantire un supporto specialistico in particolare nell'identificazione delle esigenze di ricerca il CoPIRFCyber ha nominato un gruppo di esperti. Quattordici esperti provenienti dalle scuole universitarie svizzere si sono dichiarati disponibili a fornire la loro collaborazione all'interno di tale gruppo, che ha già identificato le principali tematiche di ricerca e che per fine 2016 redigerà un rapporto in cui saranno illustrate le maggiori sfide del momento nell'ambito della ricerca nazionale e internazionale.
- **Convegno sui cyber-rischi:** il 25 maggio 2016 presso il PF di Losanna si è tenuta la prima «Swiss Cyber Risk Research Conference», organizzata dal CoPIRFCyber sotto la direzione della SEFRI. Al convegno, cui hanno partecipato 350 esponenti del mondo della ricerca svizzero, ha ospitato relatori di fama internazionale. In futuro il convegno si terrà ogni due anni e contribuirà a rafforzare la rete di ricercatori nel settore dei cyber-rischi.

Outcome: gli obiettivi sono stati raggiunti in gran parte

Grazie alla «Swiss Cyber Risk Research Conference» è stato possibile rivolgersi a ricercatori dei settori più disparati e affrontare con loro il tema dei cyber-rischi. Il pool di esperti creato è riuscito a riunire una fitta rete di specialisti. Lo stesso pool di esperti ha identificato i più importanti temi di ricerca e le principali sfide, che saranno illustrati in dettaglio entro fine 2016. I lavori hanno lo scopo di aiutare la Confederazione a definire le priorità nella promozione della ricerca.

- **Rete di ricercatori:** la «Swiss Cyber Risk Research Conference» ha riunito per la prima volta ricercatori delle discipline più disparate provenienti da varie scuole universitarie, che si sono così confrontati sul tema dei cyber-rischi. L'evento rappresenta il primo passo verso la creazione della rete di ricercatori ma oltre a questo resta comunque importante l'interazione tra i ricercatori. Le modalità con cui ciò dovrà avvenire restano ancora da definire: il pool di esperti, composto da una fitta rete di specialisti, funge già da buona base di partenza.
- **Identificazione delle lacune nel settore della ricerca:** il gruppo di esperti ha identificato le principali tematiche e le sfide per la ricerca svizzera ed entro fine 2016 pubblicherà un rapporto al riguardo. Resta ancora da stabilire se i lavori saranno aggiornati con regolarità e in che modo.
- **Mandati di ricerca/programma di ricerca:** poiché ad oggi non esiste una descrizione dei principali temi di ricerca, non sono ancora stati formulati mandati concreti al riguardo. Nel quadro del programma «Big Data» del Fondo nazionale svizzero viene però già incentivata la ricerca nell'ambito dei cyber-rischi.

Impact: non può ancora essere valutato

Le strutture create sembrano essere idonee a tracciare un quadro dello stato attuale della ricerca e a identificare maggiori esigenze di ricerca nell'ambito dei cyber-rischi. Tuttavia ora è troppo presto per stabilire se la misura sarà in grado di produrre effetti.

3.13. M7/M8 Formazione e ricerca: Panoramica delle offerte di formazione e incremento dell'impiego delle offerte di formazione in materia di creazione di competenze ed eliminazione delle lacune riscontrate nell'ambito delle offerte

Titolo della misura	Formazione e ricerca: Panoramica delle offerte di formazione e incremento dell'impiego delle offerte di formazione in materia di creazione di competenze ed eliminazione delle lacune riscontrate nell'ambito delle offerte
Obiettivi	M7: Gli attori dell'economia, dell'amministrazione e della società civile possono informarsi, in maniera conforme alle esigenze, riguardo alle offerte in materia di creazione di competenze concernenti la gestione dei cyber-rischi. Le lacune nell'ambito delle offerte sono state identificate e servono da base per l'attuazione della misura 8. M8: D'intesa con i Cantoni e l'economia, in un piano di attuazione la Confederazione ha stabilito come intende ottenere un maggiore impiego delle offerte formative in materia di creazione di competenze per la gestione dei cyber-rischi. Il piano indica inoltre in che modo debbano essere eliminate le lacune esistenti e quali nuove offerte formative in materia di creazione di competenze debbano essere previste.
Ufficio/UO responsabile	SEFRI, SC SNPC
Documenti consultati per la verifica dell'efficacia	Fonti: [16], [17], [18], [19], [20], [21], [22], [23], [24], [25], [26], [27], [28], [29], [30], [31], [32]
Interviste	Si veda l'allegato A.1, intervista I 1

3.13.1. *Effetto atteso: modello di efficacia M7/M8*

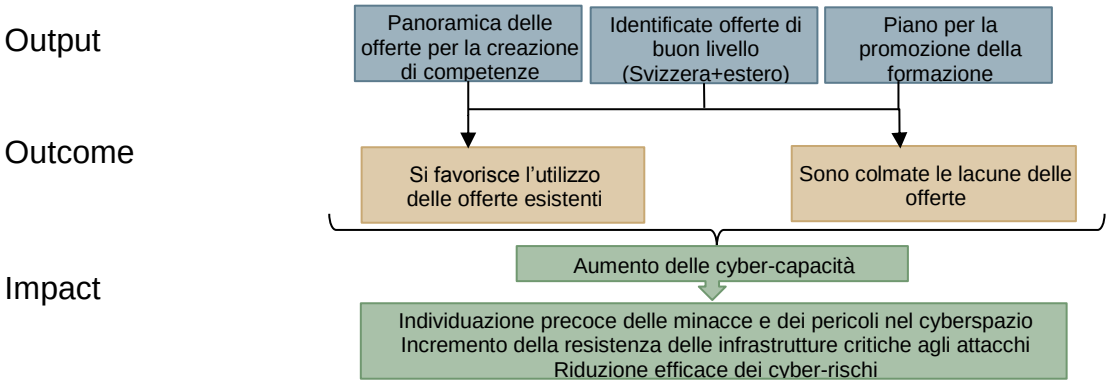

Figura 14: Modello di efficacia M7/M8

3.13.2. *Input: risorse assegnate*

Tipo di risorsa	Numero di risorse assegnate alla SNPC
Risorse in termini di personale	Nessun posto nuovo creato
Risorse finanziarie	Nessuna risorsa aggiuntiva
Collaborazione di altri uffici/UO	UFCOM, DFAE, DDPS

3.13.3. *Valutazione del raggiungimento degli obiettivi e della loro efficacia*

Livello	Obiettivi non raggiunti	Obiettivi raggiunti soltanto in parte	Obiettivi raggiunti in gran parte	Obiettivi raggiunti
Output			✓	
Outcome				✓✓
Impact	☐ attualmente non valutabile			

3.13.4. *Motivazione della valutazione*

Output: gli obiettivi sono stati raggiunti in gran parte

È stata preparata una panoramica delle offerte di formazione già disponibili in materia di creazione di competenze e, con l'aiuto di esperti, sono state identificate le offerte di elevato valore qualitativo. Questi lavori sono stati utili soprattutto per farsi un'idea di come la Confederazione possa incentivare la formazione per creare competenze nell'ambito dei cyber-rischi. Si è rinunciato a documentare specificatamente le offerte di elevato valore qualitativo perché una valutazione della Confederazione sarebbe ammessa solo nel quadro di un processo di certificazione completo.
Un piano di attuazione ha stabilito in che modo la Confederazione intende gestire lo sviluppo delle competenze nell'ambito dei cyber-rischi. Nello specifico vengono concretizzate le modalità di lavoro nei settori della formazione continua e della formazione professionale e a livello di scuole universitarie.

- **Panoramica delle offerte:** mediante un sondaggio condotto tra gli esperti sono state identificate le offerte formative già disponibili per la creazione di competenze in Svizzera e nei Paesi limitrofi. Viene fatta una distinzione tra le offerte per la popolazione, per l'amministrazione e per l'economia. Le esigenze dei gruppi mirati, le offerte identificate e le lacune riscontrate nell'ambito delle offerte sono state descritte in un rapporto. È chiaro che una panoramica di questo tipo non può essere esaustiva, considerando il fatto che il mercato della formazione è una realtà molto dinamica. L'aggiornamento a intervalli regolari non è previsto, visto che anche le varie unioni e associazioni pubblicano sui rispettivi siti web delle panoramiche su queste offerte.
- **Identificazione delle offerte di elevato valore qualitativo:** sempre avvalendosi del suddetto sondaggio si è cercato di identificare degli esempi di offerte formative adeguate in materia di creazione di competenze. Alla fine si è rinunciato a fornire una valutazione qualitativa sistematica delle varie offerte e a pubblicare quelle migliori. Per ragioni di natura politico-istituzionale non è opportuno che la Confederazione si intrometta nel mercato delle offerte formative disponibili. Una valutazione globale sarebbe ammessa solo nel quadro di una procedura di certificazione, ma questo esula dagli obiettivi previsti dalle misure 7 e 8.
- **Documento programmatico per l'incentivazione della formazione:** il documento programmatico per l'incentivazione della formazione nell'ambito dei cyber-rischi è stato approntato. È frutto del lavoro del CoPIRFCyber (cfr. cap. 3.12) e spiega le misure che la Confederazione adotterà per promuovere la formazione nell'ambito dei cyber-rischi. Anzitutto la Confederazione incentiverà la creazione di competenze a livello di formazione continua, formazione professionale e scuole universitarie. Al riguardo, il documento programmatico descrive già alcuni interventi concreti. La formazione di base rientra in misura determinante nelle competenze dei Cantoni, perciò finora l'argomento non è stato affrontato.

Outcome: gli obiettivi sono stati raggiunti

L'istituzione del diploma federale di ICT Security Expert, un progetto realizzato in collaborazione con l'associazione ICT Formazione professionale, ha permesso di compiere un importante passo in avanti per incentivare la creazione di competenze a livello di formazione continua e formazione professionale. A livello di scuole universitarie la formazione è stata incrementata indirettamente, soprattutto con la promozione della ricerca (cfr. M1, cap. 3.12).

Incentivazione dell'impiego delle offerte disponibili ed eliminazione delle lacune riscontrate nell'ambito delle offerte: per incentivare l'impiego delle offerte disponibili e per eliminare le lacune riscontrate nelle offerte nell'ambito dei cyber-rischi, in collaborazione con l'associazione ICT Formazione professionale è stato creato il nuovo profilo professionale di «ICT Security Expert» (si veda [32]). I primi diplomi saranno presumibilmente conferiti nell'autunno 2018. Il progetto ha suscitato vivo interesse nell'economia privata ed è co-finanziato da numerose aziende. Basato sulle offerte formative preesistenti, completa queste ultime dove sussistono delle lacune. Il profilo di qualificazione viene definito insieme ai rappresentanti dell'economia privata.

La Confederazione promuove la formazione nel settore della ricerca a livello di scuole universitarie. L'attuazione di questa misura è dunque strettamente connessa alla misura 1 ed è coordinata dal CoPIRFCyber (cfr. M1, cap. 3.12). Con la promozione mirata dei progetti di ricerca si intende migliorare la formazione nelle scuole universitarie. In tal senso, una particolare attenzione viene rivolta alla promozione dei corsi di formazione interdisciplinari.

Impact: attualmente non valutabile

> Quello della formazione è un impegno a lungo termine. Adesso è troppo presto per riuscire a valutare un impatto concreto.

3.14. M16 Basi legali: Necessità di modificare le basi legali

Titolo della misura	Necessità di modificare le basi legali
Obiettivi	I dipartimenti competenti hanno identificato come prioritarie le lacune legislative esistenti, effettuato i necessari adeguamenti giuridici ed elaborato i relativi progetti ai livelli normativi interessati. Un piano di regolamentazione sarà sottoposto al Consiglio federale.
Ufficio/UO responsabile	ODIC
Documenti consultati per la verifica dell'efficacia	Fonti: [127]
Interviste	Si veda l'allegato A.1, intervista I 13

3.14.1. Effetto atteso: modello di efficacia M16

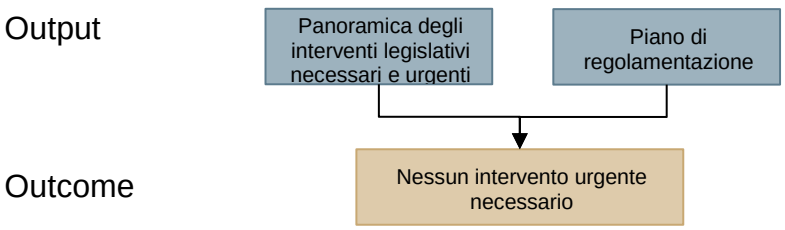

Figura 15: Modello di efficacia M16

3.14.2. *Input: risorse assegnate*

Tipo di risorsa	Numero di risorse assegnate alla SNPC
Risorse in termini di personale	Gestito dal SC SNPC
Risorse finanziarie	Nessuna
Collaborazione di altri uffici/UO	Sono stati coinvolti gli uffici federali competenti (si veda l'elenco nell'allegato M16 1).

3.14.3. *Valutazione del raggiungimento degli obiettivi e della loro efficacia*

Livello	Obiettivi non raggiunti	Obiettivi raggiunti soltanto in parte	Obiettivi raggiunti in gran parte	Obiettivi raggiunti
Output				✓✓
Outcome	☐ attualmente non valutabile			
Impact	☐ attualmente non valutabile			

3.14.4. *Motivazione della valutazione*

<u>Output: gli obiettivi sono stati raggiunti</u>

> È stata predisposta una panoramica degli interventi legislativi necessari e urgenti. Per farlo sono stati consultati tutti gli uffici federali competenti. Non è stata rilevata alcuna necessità di interventi legislativi o modifiche urgenti.

- **Panoramica degli interventi legislativi necessari e urgenti:** il compendio sulle necessità prioritarie di legiferazione e revisione nel settore cibernetico per l'obiettivo intermedio 16.1 (si veda [127]) contiene la panoramica richiesta. È stato accolto il contributo di tutti gli uffici federali competenti. Il SC SNPC, tramite le segreterie generali e la CaF, ha preparato insieme a tutti gli uffici federali competenti una panoramica delle basi legali rilevanti per i settori che presentano aspetti inerenti al cyberspazio e in quell'occasione ha chiarito se vi fossero necessità di interventi legislativi o modifiche urgenti.
- **Piano di regolamentazione:** l'Aggruppamento Difesa del DDPS è stato l'unico ufficio federale a segnalare una necessità di intervento urgente. Nel frattempo questo punto è stato regolamentato all'art. 100 della nuova legge militare, la cui relativa ordinanza è in fase di preparazione.

Il CC SNPC ha preso visione della panoramica degli interventi legislativi necessari e ha deciso di sospendere l'attuazione della misura 16. Non spetta alla SNPC, bensì agli uffici federali competenti, accertare il fabbisogno in questo senso.

<u>L'outcome non può essere valutato</u>

> Non è stata rilevata alcuna necessità di interventi urgenti. Pertanto la fase di elaborazione degli adeguamenti giuridici non ha luogo. Di conseguenza non è possibile valutare il risultato prodotto dalla misura 16.

- **Non servono interventi urgenti:** la misura è attuata, ma come qualsiasi altra misura di SNPC richiede una verifica a intervalli regolari. La panoramica descritta rappresenta solo una prima analisi. La situazione giuridica deve adeguarsi alle

sempre nuove forme di cyber-minacce. Al proposito si rimanda, ad esempio, ai lavori in corso relativi alla legge sulla protezione delle informazioni o la direttiva (UE) 2016/1148 del 6 luglio 2016 recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione.

Impact: nulla da valutare

Poiché la misura si è conclusa con la creazione della panoramica, non c'è nessun impatto da poter misurare.

4. Interfacce

Le misure previste dalla SNPC si focalizzano sui compiti dell'Amministrazione federale civile e si prefiggono di contribuire a garantire una maggiore protezione delle infrastrutture critiche. Per svolgere questi compiti non si può prescindere dall'interfacciarsi con due realtà fondamentali: i Cantoni con le loro attività e l'esercito con le sue attività nell'ambito della cyber-difesa. Per poter fare una valutazione globale degli effetti della SNPC sono state analizzate anche queste due interfacce.

4.1. Interfaccia con i Cantoni – Lavori della RSS

Tipo di interfaccia	Interfaccia per l'attuazione della SNPC nei Cantoni
Obiettivi	Coinvolgimento dei Cantoni in tutte le misure di attuazione della SNPC che li riguardano, coordinamento delle attività correnti dei Cantoni per la protezione dai cyber-rischi, scambio di informazioni e conoscenze.
Ufficio/UO responsabile	RSS
Documenti consultati per la verifica dell'efficacia	Fonti: [128], [129], [130]
Interviste	

4.1.1. Effetto atteso: modello di efficacia Interfaccia Cantoni

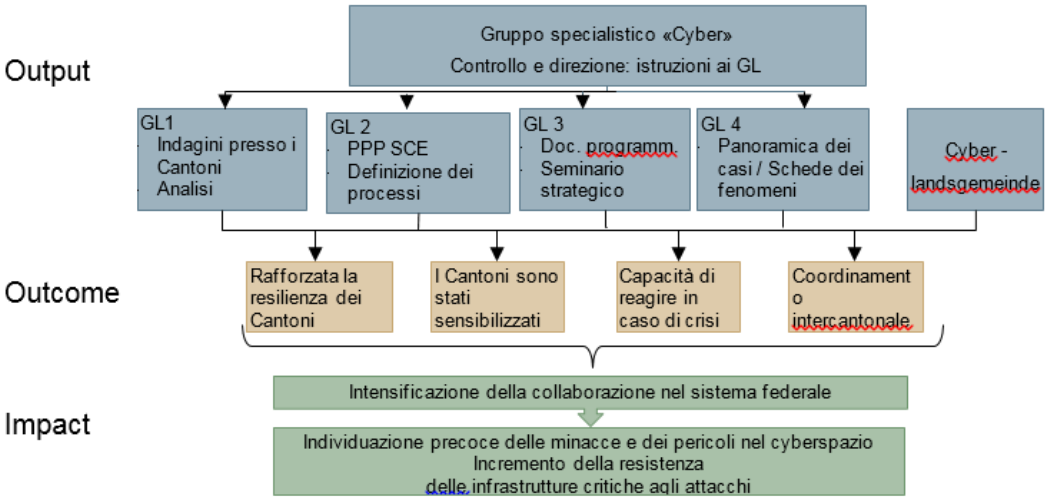

Figura 16: Modello di efficacia RSS

4.1.2. *Input: risorse assegnate*

Tipo di risorsa	Numero di risorse assegnate alla SNPC
Risorse in termini di personale	I lavori di coordinamento vengono svolti interamente dalla RSS senza ricorrere a risorse aggiuntive.
Risorse finanziarie	A carico della RSS
Collaborazione di altri uffici/UO	Sono coinvolti in primis i seguenti uffici dell'Amministrazione federale: SC SNPC, MELANI, SCOCI, CaF, UFPP, esercito.

4.1.3. *Valutazione del raggiungimento degli obiettivi e della loro efficacia*

Livello	Obiettivi non raggiunti	Obiettivi raggiunti soltanto in parte	Obiettivi raggiunti in gran parte	Obiettivi raggiunti
Output				✓✓
Outcome			✓	
Impact	☐ attualmente non valutabile			

4.1.4. *Motivazione della valutazione*

<u>Output: gli obiettivi sono stati raggiunti</u>

Il gruppo specialistico «Cyber» e i 4 GL a esso aggregato hanno consolidato la loro posizione e fornito un importante contributo al radicamento della SNPC nei Cantoni. Lo scambio reciproco è garantito dall'incontro nazionale «Cyber-Landsgemeinde» che si tiene una volta all'anno.

- **Gruppo specialistico «Cyber»:** nel piano di attuazione della SNPC, la RSS è stata incaricata di costituire un gruppo specialistico «Cyber» che funga da interfaccia tra l'attuazione della SNPC e le attività dei Cantoni.

  Il gruppo specialistico «Cyber» è stato creato nel 2013. Ne fanno parte le seguenti organizzazioni: RSS, CDDGP, SC SNPC, Conferenza dei cancellieri di Stato, MELANI, CSI, esercito, CdC, Unione delle città svizzere e Associazione dei comuni svizzeri. Il gruppo specialistico si riunisce due volte all'anno, garantendo in tal modo il coordinamento di tutti i lavori in corso. Per la salvaguardia operativa delle interfacce con la SNPC il gruppo specialistico «Cyber» ha costituito 4 GL, i cui capi sono anch'essi rappresentati in seno al gruppo specialistico.

  GL: i GL riflettono le principali interfacce della SNPC con i Cantoni. I 4 GL hanno conseguito gli obiettivi seguenti:

  – **GL1 Analisi dei rischi e misure di prevenzione** (interfaccia con le misure 2 e 3 della SNPC): ai Cantoni è stato distribuito un questionario da usare come strumento di autovalutazione sulla gestione dei cyber-rischi. Il GL ha analizzato le risposte e sottoposto ai Cantoni delle proposte su come ridurre i cyber-rischi identificati. Come prossimo passo, il GL fornirà ai Cantoni un supporto finalizzato all'integrazione dei cyber-rischi nella gestione dei rischi generica.
  – **GL2 Incident Management** (interfaccia con le misure 4 e 5 della SNPC): questo GL ha preparato una serie di documenti dove sono descritti i processi di gestione dei cyber-eventi, ad esempio i processi che regolano la collaborazione tra MELANI e i Cantoni nel caso si verifichi un incidente (documento IMTP6 [130]). All'interno del GL2 i Cantoni hanno manifestato il desiderio di poter

usufruire delle vaste conoscenze degli esperti. Per soddisfare questo loro desiderio è stato costituito il PPP SCE.

– **GL3 Gestione delle crisi di Confederazione e Cantoni** (interfaccia con la misura 15 della SNPC): questo GL ha portato l'attenzione della gestione delle crisi alla dimensione dei Cantoni, coinvolgendo anche le infrastrutture critiche. Il piano è stato testato in occasione di due manifestazioni: al seminario strategico dell'11 giugno 2015 e durante un test effettuato alla RUAG Cyber Range il 23 febbraio 2016. Il seminario strategico ha evidenziato gli aspetti ancora poco chiari. A titolo di esempio è stato simulato un attacco al sistema pensionistico svizzero. L'integrazione dei settori specialistici coinvolti nella gestione delle crisi è stata analizzata. Al centro dell'attenzione è stato messo il coordinamento tra Confederazione e Cantoni come principali partner nella RSS. I singoli attori hanno così potuto affrontare i punti deboli e le incertezze riscontrati e discuterne all'interno delle rispettive organizzazioni.
– **GL4 Panoramica dei casi penali e il coordinamento dei casi di portata intercantonale** (interfaccia con la misura 6 della SNPC): questo GL ha elaborato, sotto la direzione di SCOCI e con la partecipazione dei Cantoni, un documento programmatico per ottenere una panoramica nazionale dei casi (casi penali) e il coordinamento dei casi di portata intercantonale. Per i Cantoni sono importanti anche le schede dei fenomeni che descrivono i vari tipi di cyber-criminalità. I Cantoni sono stati coinvolti nella compilazione delle schede, ne hanno ricevuta una copia per esprimere la loro opinione al riguardo e ne hanno approvato il contenuto in fase di consultazione. Per contro non è ancora stato possibile regolare la questione della competenza del Ministero pubblico. Poiché SCOCI è un'UO gestita da Confederazione e Cantoni, ha potuto svolgere direttamente molta parte del lavoro di coordinamento.
– **Cyber-Landsgemeinde:** il primo incontro nazionale «Cyber-Landsgemeinde» si è svolto nel 2013 e da allora si ripete ogni anno. Ormai è diventato un appuntamento fisso e vanta la partecipazione di numerosi rappresentanti dei Cantoni, fornendo così un importante contributo allo scambio di informazioni tra la Confederazione e i Cantoni nell'ambito dei cyber-rischi.

Outcome: gli obiettivi sono stati raggiunti in gran parte

La collaborazione tra Confederazione e Cantoni e tra gli stessi Cantoni è stata intensificata. Dato che ora tutti i Cantoni sono membri di MELANI, la capacità di reazione è migliorata. Il coinvolgimento dei Cantoni nelle esercitazioni di gestione delle crisi aiuta a identificare e a eliminare i punti deboli nella gestione della resilienza. Tuttavia in tutti i settori la collaborazione è ancora migliorabile.

- **Collaborazione**: i GL e il «Cyber-Landsgemeinde» hanno migliorato sensibilmente la collaborazione e l'interazione tra Cantoni e Confederazione. Un esempio è dato da un più forte coinvolgimento dei Cantoni nella centrale MELANI. All'inizio dell'attuazione della SNPC, 10 Cantoni non partecipavano alle attività di MELANI. Grazie al supporto della RSS, da fine 2015 tutti i Cantoni aderiscono alla CCC di MELANI.

  I lavori però anche hanno evidenziato la necessità di un maggiore coordinamento tra la Confederazione e i Cantoni. Nei settori seguenti si ravvisa un potenziale di miglioramento nel grado di collaborazione:
  - rappresentazione comune e valutazione della situazione;
  - armonizzazione delle opzioni d'intervento e sincronizzazione delle decisioni;
  - panoramica e gestione delle risorse;
  - coordinamento della gestione della continuità;
  - elaborazione di messaggi comuni e loro comunicazione.
- **Gestione della resilienza:** grazie all'autovalutazione del GL1 è stato possibile dare un contributo al rafforzamento della resilienza dei Cantoni in materia di cyber-rischi. Adesso i Cantoni sono più consapevoli della situazione in cui si trovano e delle ulteriori misure da adottare. È stato altresì importante svolgere le esercitazioni sulla gestione delle crisi, coinvolgendo i Cantoni e le infrastrutture critiche. Solo durante queste esercitazioni si è capito quali processi non sono ancora stati sufficientemente sviluppati.
- **Capacità di reazione:** essendo membri di MELANI, adesso tutti i Cantoni hanno accesso diretto al suo servizio di picchetto, attivo 7 giorni su 7, 24 ore su 24. Inoltre alcuni Cantoni prendono parte alla creazione dei SOC (nel Cantone di Vaud un centro di questo genere è già operativo). Lo scambio reciproco permette di beneficiare delle esperienze altrui e di identificare le soluzioni più idonee. La definizione dei processi da mettere in atto in caso di cyber-incidente permette di gestire correttamente gli eventi e di reagire in fretta.
- **Coordinamento internazionale:** le discussioni che si fanno nei GL, a cui partecipano diversi Cantoni, favoriscono la condivisione delle conoscenze e delle esperienze. I prodotti che ne risultano vengono poi messi a disposizione di tutti i Cantoni. Conoscersi gli uni con gli altri contribuisce a creare un rapporto di fiducia e a facilitare lo scambio di informazioni.

Impact: non valutabile

La collaborazione con i Cantoni è nettamente migliorata. È difficile dire fino a che punto ciò abbia contribuito a creare una struttura consolidata della collaborazione federale nell'ambito dei cyber-rischi, in quanto la maggior parte dei lavori non è ancora conclusa. Attualmente il lavoro all'interno dei GL dipende molto dall'impegno volontario delle singole persone.

4.2. Interfaccia con l'esercito

Tipo di interfaccia	Interfaccia per attuazione della SNPC nei Cantoni
Obiettivi	All'occorrenza le capacità di cui dispone l'esercito devono poter essere accessibili e usufruibili dagli uffici responsabili nei loro processi attuativi. È quello che si definisce il principio di sussidiarietà dell'esercito, ad esempio in caso di catastrofi naturali.
Ufficio/UO responsabile	CYD SIM, SC SNPC
Documenti consultati per la verifica dell'efficacia	Fonti: interviste, documenti riservati
Interviste	I 10

L'esercito fa parte delle infrastrutture critiche del Paese. In ragione del suo mandato, l'uso del cyberspazio in generale e le cyber-minacce in particolare sono diventati temi essenziali. Uno dei compiti immediati più importanti dell'esercito è proteggere i propri sistemi e le proprie infrastrutture TIC in tutte le situazioni, così da garantire sempre la loro disponibilità e la libertà d'azione.

La SNPC esclude esplicitamente i casi di guerra e di conflitto, delegando all'esercito la competenza in caso di un relativo cyber-attacco. Non c'è nulla però che definisca come e quando la competenza passa dalle autorità civili all'esercito o come debba funzionare la collaborazione formale in caso di crisi.

In presenza di una crisi che non arriva a varcare la soglia del conflitto l'esercito svolge un ruolo sussidiario. Il presupposto per coinvolgere in via sussidiaria l'esercito nel quadro della SNPC è identificare e utilizzare in modo tempestivo le sinergie. Il coinvolgimento precoce dell'esercito deve anche servire a conciliare lo studio concettuale «Cyber Defence», elaborato dall'esercito nel 2013, con il sistema globale Svizzera.

4.2.1. Effetto atteso: modello di efficacia Interfaccia con l'esercito

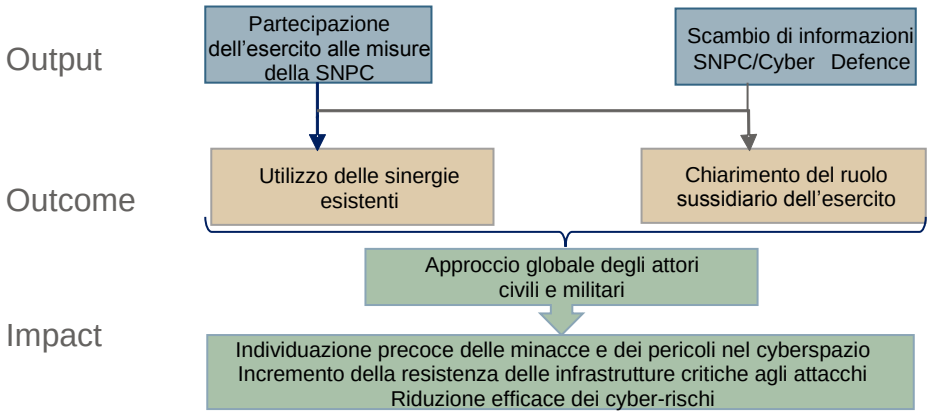

Figura 17: Modello di efficacia Interfaccia con l'esercito

4.2.2. Input: risorse assegnate

Tipo di risorsa	Numero di risorse assegnate alla SNPC
Risorse in termini di personale	Nessuna risorsa aggiuntiva. Per l'esercito, l'UO CYD si assume il lavoro di coordinamento con la SNPC, per la SNPC questo ruolo è svolto dal SC.
Risorse finanziarie	Nessuna

Collaborazione di altri uffici/UO	UO coinvolte nella collaborazione: MELANI, SIC, SEFRI, DFAE, CaF

4.2.3. Valutazione del raggiungimento degli obiettivi e della loro efficacia

Livello	Obiettivi non raggiunti	Obiettivi raggiunti soltanto in parte	Obiettivi raggiunti in gran parte	Obiettivi raggiunti
Output		✖		
Outcome		✖		
Impact	☐ attualmente non valutabile			

4.2.4. Motivazione della valutazione

<u>Output: gli obiettivi sono stati raggiunti soltanto in parte</u>

L'esercito collabora a buona parte della SNPC, quindi a livello operativo vi è anche un proficuo scambio di informazioni. Tuttavia, considerata la scarsità di risorse la collaborazione si riduce ai compiti più importanti, per cui le competenze sono molto limitate. I responsabili di entrambe le parti conoscono le rispettive capacità e attività. A livello strategico però lo scambio è insufficiente. Di conseguenza, varie questioni riguardanti la competenza e le aspettative nei confronti dell'esercito non sono sufficientemente chiare.

- **Collaborazione dell'esercito alle misure della SNPC:** l'esercito è coinvolto direttamente o indirettamente in diverse misure, segnatamente nelle seguenti:
  - M1, M7, M8: l'esercito si è fortemente impegnato in queste misure e ha finanziato la prima acquisizione di informazioni. Ha dato il via alla costituzione del CoPIRFCyber (cfr. cap. 3.12), attualmente diretto dalla SEFRI. I rappresentanti dell'esercito sono tuttora coinvolti.
  - M4, M5, M14: l'esercito è direttamente coinvolto, in particolare mediante la convenzione sulle prestazioni tra SIC e BAC-CEO. Alla rappresentazione della situazione l'esercito dà solo un contributo limitato, in quanto è ancora poco consolidata. Ciononostante, le poche informazioni disponibili vengono condivise settimanalmente con il SIC. Con MELANI lo scambio a livello operativo è intenso; le informazioni provenienti dalla rete MELANI non vengono inviate all'UO CYD SIM. A livello strategico lo scambio è insufficiente e la comprensione reciproca dei ruoli e delle competenze non è stata totalmente chiarita.
  - M2/12: l'esercito ha partecipato in maniera determinante all'elaborazione dell'analisi dei rischi e della vulnerabilità del sottosettore critico Esercito e nell'ambito di propri progetti effettua già varie analisi e adotta misure (piano integrale per la sicurezza del DDPS) atte a migliorare la resilienza delle proprie infrastrutture.
  - M10: l'esercito partecipa alle riunioni del gruppo specialistico Cyber International ed è quindi ben informato. A sua volta informa il gruppo in merito agli aspetti di portata internazionale delle attività nell'ambito della cyber-difesa.
  - M15: l'esercito è coinvolto. Non è stato tuttavia completamente chiarito fino a che punto, nel caso di una crisi che presenta aspetti inerenti al cyberspazio,

l’esercito possa fornire un contributo sussidiario alla gestione della stessa. In ogni caso il DDPS deve chiarire la questione entro fine 2016.

  - M6: lo scambio a questo proposito è informale. Gli aspetti su cui si focalizzano i militari nel valutare le situazioni sono però diversi, per natura, da quelli degli agenti di polizia.
  - Altre misure: l’esercito viene talvolta informato ma non è direttamente coinvolto. Pur essendo un grosso fornitore di prestazioni, l’esercito non è stato invitato nel CC SNPC; il problema però va ricercato internamente al DDPS.

- **Scambio di informazioni SNPC/CYD dell’esercito**: Lo scambio di informazioni tra l’esercito e i responsabili della SNPC a livello operativo è di tipo informale ed è consolidato ormai da anni. L’esercito è generalmente informato sui contenuti e sul grado di realizzazione della SNPC e viceversa gli uffici interessati sanno quali sono le capacità dell’esercito. Si deplora invece il fatto che lo scambio avvenga solo a livello operativo, mentre a livello strategico è irregolare e poco strutturato. Per quanto riguarda la necessità di chiarire i ruoli in caso di guerra o conflitto, l’esercito la promuove con le esercitazioni (p.es. Cyber Coalition, Cyber Pakt, Locked Shield).

Outcome: gli obiettivi sono stati raggiunti soltanto in parte

Il coinvolgimento dell'esercito in una serie di misure della SNPC ha reso possibile l'utilizzo delle sinergie. Per contro resta da chiarire il ruolo sussidiario dell'esercito. Non c'è nulla infatti che definisca quali siano le sue competenze in caso di escalation di una cyber-crisi e quando deve essere messo in allarme. Senza una chiara definizione di questi aspetti l'esercito non può fornire il suo supporto sussidiario in caso di crisi, in particolare se le sue risorse sono impegnate primariamente in attività di autodifesa e non vengono adibite a interventi esterni.

- **Utilizzo delle sinergie esistenti:** attualmente l'esercito offre il proprio supporto alle misure sopra citate. In quei casi le sinergie sono ben utilizzate. La collaborazione si esplica principalmente attraverso i rapporti personali e in misura minore attraverso processi formali (eccetto la convenzione sulle prestazioni tra BAC CEO e SIC). Una buona collaborazione si è instaurata tra i CERT, anche se occorre definire meglio le competenze. È stato invece incrementato il coinvolgimento del SIM nella preparazione della rappresentazione della situazione.
- **Chiarimento sul ruolo sussidiario dell'esercito:** il supporto sussidiario dell'esercito non è disciplinato. La SNPC, a questo proposito, non contiene nessuna indicazione chiara. Inoltre l'esercito non dispone attualmente di risorse sufficienti per assicurare un supporto sussidiario nell'ambito di tutte le misure e dà la precedenza alla protezione dei propri sistemi.

  In particolare resta da chiarire la questione di chi si assume la responsabilità di gestire un'eventuale escalation di una cyber-crisi nel momento in cui rischia di sfociare in un cyberconflitto. In tal senso occorre modificare la SNPC integrandola con indicazioni più precise. Sarebbe importante condurre esercitazioni su questi casi coinvolgendo tutte le parti interessate. In tal modo si potrebbe verificare concretamente se in caso di necessità vengono messe in allarme le persone giuste al momento giusto e se la resistenza agli attacchi è sufficiente. Un supporto sussidiario è possibile soltanto se si è deciso chiaramente quali prestazioni attendersi dall'esercito in quale momento di un'eventuale crisi.

Impact: attualmente non valutabile

Solo dopo la modifica della SNPC si potrà valutare se è possibile intensificare la collaborazione tra l'esercito e i responsabili della SNPC al punto da avere in futuro un approccio globale alla gestione dei cyber-rischi. Bisogna quindi riuscire a definire con maggiore precisione quale sia il ruolo dell'esercito nelle questioni inerenti i cyber-rischi.

5. Questioni trasversali a tutte le misure

Fatta la valutazione delle singole misure, in questo capitolo si tratta la valutazione dei punti sottostanti.

- **Risorse:** alla SNPC sono state complessivamente assegnate risorse finanziarie e di personale in misura adeguata?
- **Contenuti della SNPC:** gli obiettivi della strategia che sono stati fissati erano quelli giusti? Sono ancora validi? Il portafoglio delle misure è completo?
- **Strutture organizzative:** l'attuazione decentralizzata della SNPC si è dimostrata valida? Il CC SNPC e il SC SNPC fino a che punto hanno svolto bene il loro ruolo?
- **Comunicazione:** c'è stata sufficiente comunicazione, sia interna che esterna?

Per valutare questi aspetti consideriamo le risposte fornite dai responsabili dell'attuazione delle misure che abbiamo intervistato e dalle altre parti interessate. A tutte le persone che sono state intervistate è stata data anche la possibilità di esprimere un proprio parere su queste questioni, che riguardano trasversalmente tutte le misure. Non tutti hanno potuto o voluto esprimersi in merito a tali questioni, ma riunendo le risposte con l'analisi dei documenti si evince un quadro tutto sommato chiaro, che permette di formulare un giudizio sugli aspetti sopra elencati.

5.1. Pianificazione delle risorse (input)

La pianificazione delle risorse è stata in gran parte adeguata

Per l'attuazione delle misure è stato previsto nel complesso un numero di posti appena sufficiente. Poiché nella maggior parte delle UO coinvolte già si trattano temi analoghi, è stato possibile sfruttare il know-how disponibile. Questo ha permesso di attuare le misure con poche risorse di personale. In taluni casi è stato difficile per le UO occupare i posti, in quanto quelli che venivano offerti erano solo contratti di lavoro a tempo determinato. La SNPC non dispone di un proprio budget e ciò ha limitato il margine decisionale del CC SNPC.

- **Pianificazione delle risorse da destinare all'attuazione delle misure:** dei 30 nuovi posti complessivamente approvati per la SNPC, 28 sono stati creati direttamente nelle UO responsabili dell'attuazione delle misure. Il capitolo 3 illustra già le risorse impiegate per ogni singola misura. In una prospettiva globale possiamo dire che la stima delle risorse necessarie è stata realistica. Per la maggioranza delle misure le risorse messe a disposizione erano sufficienti, anche se calcolate in maniera piuttosto risicata. Sono state invece sottostimate le risorse da destinare all'attuazione della misura 3. Il posto presso SCOCI, relativo alla misura 6, non è stato occupato (o lo è stato solo per un breve periodo).

  Tra i partner intervistati, più di uno ha evidenziato che trovare la persona da assumere per un posto a tempo determinato può essere difficile. Per chi cerca un lavoro i posti a tempo determinato risultano meno interessanti e di conseguenza hanno un effetto tendenzialmente negativo sul numero e sulla qualità dei candidati.

- **Pianificazione delle risorse da destinare ai compiti sovraordinati:** per quanto riguarda i compiti di coordinamento, controlling e reporting – compiti non strettamente legati a singole misure – sono stati creati due posti del SC SNPC presso l'ODIC. Anche a questo proposito va detto che i due posti assegnati al SC SNPC per i compiti da svolgere si sono dimostrati appena sufficienti.

La SNPC non ha un proprio budget. I compiti sovraordinati (conferenza SNPC, verifica dell'efficacia) sono finanziati dall'ODIC. Questa mancanza fa sì che il CC SNPC abbia un margine di manovra limitato per avviare progetti propri o definire le priorità per il finanziamento di un supporto esterno nell'ambito di misure selezionate.

5.2. Valutazione dei contenuti della SNPC

I contenuti della SNPC si sono dimostrati validi

Gli obiettivi strategici della SNPC si sono dimostrati validi e sono tuttora consoni. Le misure dedotte dagli obiettivi coprono adeguatamente il vasto campo delle attività necessarie per lottare contro i cyber-rischi, anche se il portafoglio delle misure avrebbe potuto essere condensato di più.

Il piano di attuazione delle misure ne definisce gli obiettivi, ma non definisce i parametri per decretare il successo o meno delle misure. Questo perché per molte misure occorreva prima acquisire conoscenze e predisporre strutture, senza le quali appariva poco sensato definire esattamente obiettivi vincolanti. La creazione del controlling strategico ha permesso di avere uno strumento atto a verificare i progressi fatti nell'attuazione delle misure. Questo modo di procedere si è dimostrato tutto sommato corretto.

Per quanto riguarda i singoli aspetti dell'organizzazione contenutistica della SNPC, si può affermare quanto segue.

- **Validità degli obiettivi sovraordinati:** la maggior parte dei partner intervistati ritiene che gli obiettivi sovraordinati della SNPC (l'individuazione precoce dei cyber-rischi e delle cyber-minacce, l'aumento della resistenza delle infrastrutture critiche agli attacchi e la riduzione dei cyber-rischi) siano tuttora validi. Questi obiettivi, intesi come indicazioni strategiche generali, si sono dimostrati efficaci.
- **Condizioni generali e interfacce:** nella SNPC sono citate le principali strategie e i principali progetti della Confederazione correlati alla SNPC. Poiché si tratta di un tema trasversale le interfacce assumono grande importanza. Nel caso di un eventuale proseguimento della SNPC occorrerà tenere conto degli sviluppi di queste strategie e di questi progetti.
- **Completezza del portafoglio di misure:** anche il portafoglio delle misure della SNPC si è dimostrato sostanzialmente valido. Le misure formulate hanno coperto bene gli aspetti principali. I responsabili dell'attuazione delle misure sono però consapevoli del fatto che il lavoro fatto finora è stato soprattutto un lavoro di costruzione. Le strutture create devono servire ad affrontare le fasi successive. Tutte le parti coinvolte insistono sul fatto di garantire la continuità dei lavori finora realizzati.

  Per quanto concerne il portafoglio nella sua totalità è emerso che talune misure sono strettamente collegate sul piano dei contenuti. In taluni casi sarebbe stato possibile accorpare più misure già in sede di piano di attuazione (p. es. la M7 e la M8 avrebbero potuto essere riunite in un'unica misura). Concentrare il portafoglio limitandolo a un numero più ristretto di misure avrebbe favorito maggiore chiarezza e in futuro sarebbe opportuno ricordarselo.

  Le principali tematiche future identificate dai partner intervistati, attualmente non coperte dalla SNPC, sono le seguenti:

– significato e conseguenze per la Svizzera della direttiva (UE) 2016/1148 del 6 luglio 2016 recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione;
– questione dell'introduzione di un obbligo di segnalazione di cyber-eventi rilevanti ai fini della sicurezza per i gestori di infrastrutture critiche (questa questione acquista rilevanza anche sulla scia della direttiva UE summenzionata);
– partecipazione della Svizzera a iniziative di creazione di competenze per i Paesi in sviluppo.

- **Concretizzazione degli obiettivi delle misure nel piano di attuazione:** gli obiettivi delle singole misure formulati all'interno della SNPC sono concretizzati nel piano di attuazione della SNPC. Per tutte le misure sono stati definiti degli obiettivi, rinunciando però a determinare i parametri di misurazione del loro successo. La pianificazione degli obiettivi intermedi e la definizione dei risultati da conseguire è stata fatta direttamente dai responsabili dell'attuazione delle misure in collaborazione con il SC SNPC. Dal punto di vista del controlling e nell'ottica della dimostrazione dell'efficacia sarebbe stato auspicabile che tali criteri fossero stati stabiliti già nel piano di attuazione. Inoltre alcuni dei responsabili dell'attuazione delle misure intervistati avrebbero voluto avere indicazioni di questo genere.

  Sul fronte opposto, molti dei responsabili dell'attuazione delle misure hanno segnalato la necessità di modificare la pianificazione degli obiettivi intermedi in corso di attuazione a seguito dell'acquisizione di nuove conoscenze o del verificarsi di particolari eventi. L'attuazione di molte delle misure prevedeva l'acquisizione di una serie di conoscenze e l'allestimento di una serie di strutture e difficilmente si sarebbero potuti definire dei criteri di valutazione corretti già prima di iniziare i lavori. Diversi intervistati hanno sottolineato come il successo dell'attuazione delle misure sia imprescindibile da una certa flessibilità e che andrebbero formulati obiettivi generali piuttosto che indicazioni vincolanti.

  C'è dunque diversità di opinioni tra chi chiede criteri prestabiliti per raggiungere e misurare gli obiettivi e chi auspica flessibilità. Il piano di attuazione ha lasciato un sufficiente margine di manovra ai responsabili dell'attuazione delle misure, non prevedendo obiettivi immediatamente misurabili. A compensare questa assenza ha provveduto il controlling strategico voluto dal SC SNPC. Si è riusciti così a trovare una giusta via di mezzo che, pur stabilendo delle direttive, lasciasse però ai responsabili un sufficiente margine di manovra.

5.3. Strutture organizzative della SNPC

✔ **La scelta della struttura organizzativa della SNPC è stata in gran parte parte corretta**

L'attuazione decentralizzata della SNPC, con una ripartizione della responsabilità agli uffici di volta in volta competenti per ciascuna misura, si è dimostrata una scelta assolutamente adeguata. È il modo corretto di gestire un tema trasversale come quello dei cyber-rischi. Il presupposto affinché questa soluzione sia efficace è la presenza di organi di coordinamento ben funzionanti. In tal senso sia il CC SNPC che il SC SNPC si sono dimostrati validi. Occorrerebbe leggermente correggere la composizione del CC SNPC, nel quale dovrebbero sedere rappresentanti presso importanti interfacce. Per quanto riguarda il SC SNPC, la scelta di aderire a MELANI è controproducente: il SC SNPC infatti dovrebbe essere indipendente dai responsabili dell'attuazione delle misure (di cui fa parte MELANI) in modo da mantenere una posizione neutrale quando si deve mediare tra diversi interessi e da poter effettuare un efficace controlling strategico.

Sulla base delle interviste condotte e dell'analisi dei documenti, sulla struttura organizzativa della SNPC si possono formulare i seguenti giudizi:

- **Struttura organizzativa decentralizzata:** generalmente la struttura organizzativa decentralizzata della SNPC viene indicata come il principale elemento del suo successo. Essa riflette il carattere multi-settoriale dei cyber-rischi e ben si addice al sistema federale della Svizzera. Una delle difficoltà legate all'attuazione decentralizzata è il fatto di coinvolgere tutti gli attori rilevanti. Non sempre si è riusciti a coinvolgere nei lavori tutti i regolatori nella misura necessaria e in futuro bisognerebbe intensificare questi sforzi. Un'altra difficoltà è data dalla necessità di fornire all'esterno un'immagine di sé unitaria e chiaramente identificabile. Questo risulta più complicato se vi sono più attori che partecipano all'attuazione. L'analisi sull'eventuale riuscita di questo aspetto è descritta al capitolo 5.4 Comunicazione interna ed esterna.
- **Ruolo e composizione del CC SNPC:** il CC SNPC ha svolto la sua funzione di organo di sorveglianza approvando il controlling strategico semestrale. La decisione di adottare una misura straordinaria per la misura 3 ha dimostrato che il CC SNPC è pronto anche a intervenire nell'attuazione della SNPC quando ravvede la necessità di apportare correzioni.

  La rappresentanza diretta di tutte le UO interessate si è dimostrata valida, come merita di essere accolto favorevolmente il fatto che economiesuisse vi sia rappresentata in qualità di osservatrice. Per contro, in seno al CC SNPC non sono rappresentati né l'esercito né l'UFPP, il che che ha reso più difficile il coordinamento tra la CYD dell'esercito, la Strategia nazionale per la protezione delle infrastrutture critiche e la SNPC.

  Il CC SNPC opera sotto la direzione del delegato dell'ODIC. In linea di massima che la direzione sia affidata all'ODIC è giudicato opportuno, ma non obbligatorio. L'ODIC come organo direttivo è adatto a gestire una strategia e già da molto tempo si occupa delle questioni inerenti i cyber-rischi attraverso MELANI e ODIC-SEC. Affidare la direzione all'ODIC non è obbligatorio perché un tema trasversale come la SNPC in linea di principio può essere affidato alla gestione di diverse organizzazioni. Alcuni attori ritengono che affidare la direzione all'ODIC possa creare problemi, perché così facendo sorgerebbero potenziali conflitti di obiettivi con altri compiti principali dell'ODIC.
- **Ruolo del SC SNPC:** il SC SNPC è direttamente coinvolto nell'attuazione di diverse misure, svolge i lavori amministrativi per conto del CC SNPC, organizza l'annuale conferenza SNPC, redige i rapporti annuali sulla SNPC ed esegue il controlling strategico. Le parti coinvolte giudicano questi compiti molto importanti. A fronte di un'attuazione decentralizzata è fondamentale avere un organo di coordinamento.

  Alcuni dei partner intervistati hanno criticato il fatto che il SC SNPC abbia la propria sede organizzativa presso MELANI. Considerato che il SC SNPC esegue il controlling strategico per conto del CC SNPC, non dovrebbe essere sottoposto a un'unità che contemporaneamente è chiamato a controllare. In caso di proseguimento della SNPC sarebbe opportuno rendere il SC SNPC più indipendente spostandone la sede altrove.

5.4. Comunicazione interna ed esterna

La comunicazione è stata considerata soltanto in parte

Affinché una strategia che prevede un'attuazione decentralizzata abbia successo è fondamentale che la comunicazione tra i partner coinvolti funzioni in modo ottimale e che anche all'esterno si comunichi esattamente come e da chi viene implementata questa strategia. La comunicazione interna è stata buona e alle persone coinvolte sono sempre state predisposte le necessarie informazioni.

Per contro la comunicazione verso l'esterno non è stata efficace. Si sa poco su quali obiettivi persegua la SNPC, come venga concretamente attuata e quale sia il grado di attuazione. Di conseguenza non si conosce cosa la Confederazione stia facendo nell'ambito dei cyber-rischi e dove ponga i limiti della sua competenza.

Nel quadro della verifica dell'efficacia della strategia è stato chiesto alle parti coinvolte come giudichino la comunicazione interna ed esterna riguardo alla SNPC. Sono state raccolte le opinioni indicate di seguito.

- **Comunicazione interna:** gli intervistati si sono dichiarati soddisfatti del livello di comunicazione interna. Molti dei responsabili dell'attuazione delle misure intrattengono uno scambio regolare di informazioni con il SC SNPC e con le altre part coinvolte. In tutte le riunioni del CC SNPC i presenti vengono informati sullo stato di attuazione della strategia. È opinione generale che la SNPC abbia nettamente migliorato la comunicazione tra gli attori il cui ruolo li porta a occuparsi di cyber-rischi, se non addirittura l'abbia in taluni casi instaurata. A favorire la comunicazione c'è il fatto che molti dei responsabili dell'attuazione delle misure partecipano attivamente anche all'attuazione di altre misure e questo consente loro di instaurare un clima di ottima comprensione reciproca.

- **Comunicazione esterna:** se la comunicazione interna è apprezzata, per la comunicazione esterna la situazione richiede ulteriori interventi. Proprio in ragione della struttura decentralizzata, per chi guarda le cose da fuori spesso non è chiaro chi nel concreto sia responsabile dell'attuazione della strategia in generale o di una specifica misura. Gli strumenti di comunicazione disponibili per raggiungere un pubblico più ampio sono il rapporto annuale e la conferenza SNPC che si tiene una volta all'anno. Inoltre il SC SNPC e i responsabili dell'attuazione delle misure intervengono regolarmente in pubblico nel corso di varie manifestazioni per presentare la SNPC o singole misure. È stato però riscontrato che questi canali di comunicazione non sono sufficienti. Feedback provenienti dal mondo dell'economia e dalla popolazione come anche la fruizione nei media dei principali cyber-eventi hanno messo in evidenza che talvolta le aspettative che si hanno nei confronti della SNPC sono sbagliate. Ci si è preoccupati troppo poco di spiegare chiaramente che la responsabilità per la sicurezza delle imprese non spetta alla SNPC, bensì alle imprese stesse come di consueto. È dunque necessario rafforzare il profilo della SNPC verso l'esterno e comunicarlo in maniera più chiara.

6. Conclusione

Con la decisione riguardante l'attuazione della SNPC il Consiglio federale ha fatto capire di essere intenzionato ad affrontare i cyber-rischi con misure in grado di coprire diversi settori. Le 16 misure previste nel piano di attuazione indicano quali UO devono mobilitarsi e cosa devono fare da qui a fine 2017 per poter conseguire gli obiettivi strategici della SNPC (l'individuazione precoce di minacce e rischi, l'aumento della resistenza delle infrastrutture critiche e la riduzione dei cyber-rischi). Quando ha preso la sua decisione, il Consiglio federale era consapevole della complessità e della rapidità di evoluzione della tematica inerente i cyber-rischi. Per questo motivo ha disposto che trascorsi 5 anni dall'adozione della strategia si effettuasse un'analisi dell'efficacia, per evincere se le misure abbiano potuto essere attuate così come previsto e se siano idonee al raggiungimento degli obiettivi prefissati. Il presente rapporto rappresenta il completamento di tale compito e ora è dunque possibile trarre le conclusioni circa l'efficacia della SNPC.

Per prima cosa possiamo dire che l'attuazione delle misure è andata bene. La verifica dell'efficacia ha mostrato che le strutture organizzative e i processi previsti nel piano di attuazione sono in gran parte implementati e che diversi prodotti (rapporti e documenti programmatici) sono stati forniti nel termine convenuto. Questo risultato è stato possibile grazie al grande impegno degli uffici responsabili e con un impiego di risorse aggiuntive modesto.

L'output fornito ha anche già determinato un outcome ragguardevole. Le strutture, i processi e i prodotti creati hanno portato a un comprovato incremento delle capacità, un ampliamento delle conoscenze e un miglioramento del coordinamento nei differenti settori. Non per tutte le misure l'outcome è misurabile allo stesso modo e per tre delle 16 misure si è constatato che non tutti gli obiettivi sono stati raggiunti come auspicato. Nel complesso però si può affermare che i lavori hanno dato i risultati attesi e le capacità di gestire i cyber-rischi sono oggi nettamente migliori di quanto non lo fossero prima che venisse adottata la SNPC.

L'elemento più difficile da misurare è l'effetto diretto (impact) dei lavori svolti sugli obiettivi strategici. Nel contesto complesso e dinamico dei cyber-rischi difficilmente si possono dimostrare i nessi causali tra le misure adottate e il loro effetto sugli obiettivi della SNPC. Inoltre, la verifica dell'efficacia della strategia è stata fatta troppo presto per consentire una tale misurazione. Di norma, prima che le misure adottate sortiscano un effetto deve trascorrere un certo lasso di tempo. Pertanto solo per 3 misure è stato possibile rilevare un impatto su almeno uno dei tre obiettivi strategici. Ciò non significa che per le restanti misure non ci si possa attendere un impatto. I modelli di efficacia sviluppati nel quadro della verifica mostrano quale sia l'effetto concreto da attendersi sulla base dei risultati finora ottenuti.

La verifica dell'efficacia della strategia, però, non si è limitata soltanto a fornire una valutazione delle singole misure. Si è anche cercato di capire se si sia tenuto sufficientemente conto delle interfacce della SNPC con i lavori dei Cantoni e dell'esercito. Se per quanto riguarda i Cantoni la risposta al quesito è affermativa, in merito all'interfaccia con l'esercito restano ancora aperte importanti questioni. Fin dove può arrivare la competenza civile della SNPC e dove deve avvenire il passaggio alla gestione da parte dell'esercito in caso di conflitto non è ancora stato completamente chiarito. Resta altresì da stabilire in che modo l'esercito possa e debba fornire un supporto sussidiario alle autorità civili in relazione ai cyber-rischi.

Si sono poi analizzate questioni non strettamente legate alla singola misura: per la SNPC sono stati definiti degli obiettivi corretti? Sono state assegnate sufficienti risorse? La struttura organizzativa decentralizzata si è dimostrata valida? La comunicazione ha

funzionato? In linea di massima su questi aspetti si possono trarre conclusioni positive. I contenuti si sono dimostrati fondamentalmente validi, le risorse erano appena sufficienti e la struttura organizzativa decentralizzata è stata accolta con favore. L'unica critica riguarda la comunicazione esterna che, secondo il parere di diversi partner intervistati, deve essere migliorata.

Infine possiamo dire che la SNPC merita di essere considerata un successo sia sul piano delle misure che su quello delle interfacce e degli aspetti trasversali. Al contempo si deve però anche sottolineare che con le misure attuate è stato compiuto solo un primo passo. Un primo obiettivo è stato raggiunto Tuttavia è ancora troppo presto e sarebbe peraltro anche inadeguato al tema dichiararsi soddisfatti dei risultati ottenuti. Considerata la rapidissima evoluzione dei cyber-rischi, stare fermi significa regredire. Un'altra conclusione a cui siamo giunti durante la verifica dell'efficacia della strategia è che il lavoro finora svolto deve necessariamente continuare. Solo proseguendo in questo sforzo si riuscirà a proteggere la Svizzera contro i cyber-rischi nel miglior modo possibile.

A. Interviste e questionari

A.1. Elenco delle interviste svolte

Alle interviste è stato attribuito un indice (I 1-I 14) per aprire il link all'interno del documento.

N.	Data	Misure	Responsabili applicazione misure	Ora e luogo
I 1	26 febbraio 2016	M1, M7, M8	Blaise Roulet (delegato per compiti speciali presso la SEFRI) Manuel Suter (coordinatore SNPC ODIC)	14.00-16.00 AWK, Laupenstrasse 4, Berna
I 2	4 marzo 2016	M4, M14	Philipp Kronig Marc Henauer (responsabile MELANI-OIC nel SIC) Mauro Vignati (responsabile Cyber SIC nel SIC) Pascal Lamia (responsabile MELANI presso l'ODIC)	10.00-12.00 P20, Berna
I 3	15 marzo 2016	M2, M12	Ruedi Rytz (responsabile Segreterie Logistica e TIC presso l'UFAE) Daniel Caduff (collaboratore scientifico presso l'UFAE) Dario Walder (collaboratore scientifico presso l'UFAE)	10.00-12.00 AWK, Laupenstrasse 4, Berna
I 4	15 marzo 2016	M10	Michele Coduri (responsabile della DPS-DFAE) Laura Crespo (collaboratrice scientifica presso la DPS-DFAE)	14.00-16.00 DPS-DFAE, Bernastrasse, Berna
I 5	22 marzo 2016	M6	Adrian Lobsiger (sostituto del direttore del fedpol) Tobias Bolliger (capo del commissariato a.i. presso SCOCI-DFGP)	10.00-12.00 AWK, Laupenstrasse 4, Berna
I 6	5 aprile 2016	M9, M11	René Dönni Kuoni (vicedirettore e capo della divisione Servizi di telecomunicazione e posta presso l'UFCOM) Nicolas Rollier (collaboratore scientifico presso l'UFCOM) Matthias Ziehl (ingegnere delle telecomunicazioni presso l'UFCOM)	M9, M11 10.00-12.00 AWK, Laupenstrasse 4, Berna
I 7	5 aprile 2016	M3	Marcel Frauenknecht (responsabile ODIC SEC presso l'ODIC) Rolf Oppliger (ODIC)	14.00-16.00 AWK, Laupenstrasse 4, Berna
I 8	12 aprile 2016	M2, M12	Stefan Brem (capo Analisi dei rischi e coordinamento della ricerca presso l'UFPP) Angelika Bischof (collaboratrice scientifica presso l'UFPP) Giorgio Ravioli (collaboratore scientifico presso l'UFPP)	14.00-16.00 AWK, Laupenstrasse 4, Berna

N.	Data	Misure	Responsabili applicazione misure	Ora e luogo
I 9	15 aprile 2016	M15, RSS	André Duvillard (delegato della RSS) Melanie Friedli (collaboratrice scientifica presso la RSS) Nicolas Mueller (responsabile della formazione per la gestione delle crisi della Confederazione presso la CaF)	10.00-11.30 AWK, Laupenstrasse 4, Berna
I 10	25 aprile 2016	M5	Pascal Lamia (responsabile MELANI presso l'ODIC) Reto Inversini (analista GovCERT)	10.00-12.00 AWK, Laupenstrasse 4, Berna
I 11	3 maggio 2016	Interfaccia esercito, M4, M14	BV_CYD SIM Gérald Vernez BV_BAC CEO (CNO) Riccardo Sibillia	10.00-12.00 P20
I 12	3 maggio 2016	M13	Stefanie Frey (coordinatrice SNPC presso l'ODIC) Ronja Tschümperlin (analista MELANI-OIC presso il SIC) Manuel Suter (coordinatore SNPC presso l'ODIC)	14.00-16.00 P20
I 13	24 maggio 2016	M16	Stefanie Frey, SC SNPC	Questionario compilato per iscritto
I 14	3 giugno 2016	M2, M12	UFE Marc Kenzelmann, vicedirettore e capo della divisione Vigilanza e sicurezza presso l'UFE Hans-Peter Binder, capo Gestione dei rischi e vigilanza sul trasporto in condotta presso l'UFE Christian Holzner, specialista nella gestione dei rischi presso l'UFE	10.00-12.00 AWK, Laupenstrasse 4, Berna

A.2. Elenco dei questionari inviati

In alcuni sottosettori dell'infrastruttura critica è stato realizzato un sondaggio mediante un questionario sulle misure M2 e M12. Anche questi sondaggi sono muniti di un indice (F 1-F 6) per aprire il link all'interno del documento.

N.	Settore	Responsabili dell'attuazione delle misure dei sottosettori contattati
F 1	Approvvigionamento di gas naturale	• Andre Martin, Gasverbund Mittelland, andre.martin@gvm-ag.ch • Jens Harenberg, Swissgas, harenberg@swissgas.ch
F 2	Traffico aereo	• Peter Frey, aeroporto di Zurigo, peter.frei@zurich-airport.com • Reto Gasser, reto.gasser@2assistu.ch
F 3	Salute	Sottosettore Laboratori • Samuel Roulin, Ufficio federale della sanità pubblica, samuel.roulin@bag.admin.ch • Martin Risch, presidente dell'Unione Svizzera di Medicina di Laboratorio e sostituto del presidente del consiglio di amministrazione del centro di medicina di laboratorio Dr. Risch martin.risch@risch.ch Sottosettore Cure mediche e ospedaliere • Philipp Stoll, rappresentante H+, philipp.stoll@ukbb.ch
F 4	Banche	• Yves Obrist, FINMA, Yves.Obrist@finma.ch • Michael Brügger, FINMAl Michael.ruegger@finma.ch • Thomas Rhomberg, SIX Group Services SA, Thomas.Rhomberg@six-group.com
F 5	Media	• Andreas Schneider, Società svizzera di radiotelevisione, andreas.schneider@srgssr.ch • René Wehrlin, UFCOM, rene.wehrlin@bakom.admin.ch
F 6	Approvvigionatori di energia elettrica	• Reto Bondolfi, EWZ, reto.bondolfi@ewz.ch • Daniel Schelbert, Elektrizitätswerk des Bezirks Schwyz, d.schelbert@ebs-strom.ch • Beat Schüpbach, Swissgrid, beat.schuepbach@swissgrid.ch (nonostante i molteplici solleciti non ha risposto)

B. Riferimenti

N.B.: laddove il titolo è in lingua tedesca non è presente una traduzione del documento in italiano.

Titolo		Autore/editore	Data
[1]	Strategia nazionale per la protezione della Svizzera contro i cyber-rischi SNPC	DDPS	19.06.2012
[2]	Piano di attuazione	DFF, ODIC	13.05.2013
[3]	Detailkonzept zur Wirksamkeitsprüfung NCS	ECOPLAN	28.07.2015
[4]	Ausschreibung «Offerten-Anfrage - Wirksamkeitsüberprüfung Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken»	DFF, ODIC	16.11.2015
[5]	Offerte für Beratungs- und Ingenieurleistungen Wirksamkeitsüberprüfung NCS	AWK	22.10.2015
[6]	Roadmap SNPC	ODIC	13.07.2015
[7]	Programm Tagung Cyber-Risiken Schweiz 2015	ODIC	02.11.2015
[8]	Mandat Steuerungsausschuss NCS und Koordinationsstelle NCS	ODIC	15.05.2013
[9]	Strategisches Controlling des Steuerungsausschusses NCS zum Umsetzungsstand per 01.01.2015	SC SNPC	27.05.2015
[10]	Protokoll der 1. Sitzung des Steuerungsausschusses NCS	SC SNPC	30.10.2013
[11]	Protokoll der 2. Sitzung des Steuerungsausschusses NCS	SC SNPC	11.02.2014
[12]	Protokoll der 3. Sitzung des Steuerungsausschusses NCS	SC SNPC	19.08.2014
[13]	Protokoll der 4. Sitzung des Steuerungsausschusses NCS	SC SNPC	10.02.2015
[14]	Protokoll der 5. Sitzung des Steuerungsausschusses NCS	SC SNPC	20.08.2015
[15]	Protokoll der 6. Sitzung des Steuerungsausschusses NCS	SC SNPC	25.02.2016
Ricerca (M1), panoramica della formazione per la creazione di competenze (M7) e formazione per la creazione di competenze (M8)			
[16]	Strategia nazionale per la protezione della Svizzera contro i cyber-rischi SNPC, misura 1: Identificazione dei cyber-rischi attraverso la ricerca, obiettivo intermedio 1.1: Organisationsstruktur und Prozessbeschreibung	SC SNPC	30.07.2015
[17]	Protokoll CoPIRFCyber	DFF	11.09.2015
[18]	Protokoll CoPIRFCyber	DFF	18.12.2015
[19]	Protokoll CoPIRFCyber	DFF	22.05.2015
[20]	Provisorisches Programm	Swiss Cyber Risk Research Conference 2016	24.11.2015
[21]	Expertengruppe «Forschung und Bildung zu Cyber-Risiken»	DFF	Novembre 2015

Titolo		Autore/editore	Data
[22]	Thematische Untergruppen: Projekt «Forschung und Bildung zu Cyber-Risiken»	DFF	
[23]	Research Capabilities in Switzerland	Bernhard Hämmerli e Solange Ghernaoutie	
[24]	Strategia nazionale per la protezione della Svizzera contro i cyber-rischi SNPC, misura 7: Panoramica sulle offerte di formazione, obiettivo intermedio 7.1: Übersicht Kompetenzbildungs-angebote für den Umgang mit Cyber-Risiken	DFF	26.06.2014
[25]	Strategia nazionale per la protezione della Svizzera contro i cyber-rischi SNPC, misura 7: Panoramica sulle offerte di formazione, obiettivo intermedio 7.2: Kurzbericht Identifizierung qualitativ hochstehender Kompetenzbildungsangebote durch Expertenempfehlungen	DFF	30.06.2014
[26]	Kompetenzbildungsangebote im Umgang mit Cyber-Risiken (misura 7 SNPC)	iimt	16.03.2015
[27]	Strategia nazionale per la protezione della Svizzera contro i cyber-rischi SNPC, rapporto conclusivo per la misura 8: Incremento dell'impiego delle offerte di formazione in materia di creazione di competenze ed eliminazione delle lacune riscontrate nell'ambito delle offerte	DFF	25.02.2016
[28]	Strategia nazionale per la protezione della Svizzera contro i cyber-rischi SNPC, misura 8: Incremento dell'impiego delle offerte di formazione in materia di creazione di competenze ed eliminazione delle lacune riscontrate nell'ambito delle offerte, obiettivo intermedio 8.1: Organisationsstruktur (Mandat und Mitgliedschaft der steuernden Einheit)	DFF	30.07.2015
[29]	Strategia nazionale per la protezione della Svizzera contro i cyber-rischi SNPC, misura 8: Incremento dell'impiego delle offerte di formazione in materia di creazione di competenze ed eliminazione delle lacune riscontrate nell'ambito delle offerte, obiettivo intermedio 8.2: Konzeptentwurf	DFF	30.07.2015
[30]	Cybersecurity Competence Building Trends	DiploFoundation	Novembre 2015
[31]	Strategia nazionale per la protezione della Svizzera contro i cyber-rischi SNPC, misura 8: Incremento dell'impiego delle offerte di formazione in materia di creazione di competenze ed eliminazione delle lacune riscontrate nell'ambito delle offerte, obiettivo intermedio 8.4: Umsetzungskonzept	DFF	02.02.2016
[32]	ICT Security Expert, Ein neues Berufsbild	ODIC	20.05.2016
[33]	Tabella delle risorse per la SNPC	ODIC	10.02.2016
Analisi settori (M2, M12)			
[34]	Risiko- und Verwundbarkeitsanalyse des Teilsektors Luftverkehr	DEFR	27.11.2015

Titolo		Autore/editore	Data
[35]	Risiko- und Verwundbarkeitsanalyse des Teilsektors Medien	UFPP	03.12.2015
[36]	Risiko- und Verwundbarkeitsanalyse des Teilsektors Labors	UFPP	05.02.2016
[37]	Risiko- und Verwundbarkeitsanalyse des Teilsektors Zivilschutz	UFPP	16.02.2016
[38]	Risiko- und Verwundbarkeitsanalyse des Teilsektors Erdgasversorgung	DEFR	26.09.2014
[39]	Risiko- und Verwundbarkeitsanalyse des Teilsektors Strassenverkehr	DEFR	12.02.2015
[40]	Risiko- und Verwundbarkeitsanalyse des Teilsektors Stromversorgung	DEFR	27.11.2015
[41]	Massnahmen zur Stärkung der IKT-Resilienz der Erdgasversorgung	DEFR	23.02.2016
[42]	Methode: Risiko- und Verwundbarkeitsanalyse kritischer Teilsektoren	UFPP	26.05.2015
[43]	Risiko- und Verwundbarkeitsanalyse des Teilsektors ärztliche Betreuung und Spitäler	UFPP	18.12.2015
[44]	Risiko- und Verwundbarkeitsanalyse des Teilsektors Banken	UFPP	07.03.2016
[45]	Risiko- und Verwundbarkeitsanalyse des kritischen Teilsektors Blaulichtorganisationen	UFPP	20.05.2016
[46]	Risiko- und Verwundbarkeitsanalyse des kritischen Teilsektors Parlament, Regierung, Justiz und Verwaltung	UFPP	20.05.2016
[47]	Checklist: Überprüfung der Vorarbeiten zur Verwundbarkeitsanalyse SKI / NCS	UFPP	
[48]	Memorandum del colloquio UFAE-UFPP sull'attuazione della strategia SNPC/PIC	UFPP	24.03.2014
[49]	E-mail di Daniel Schelbert	Elektrizitätswerk des Bezirks Schwyz AG	21.07.2015
[50]	E-mail di Hansjörg Holenstein	AES	19.03.2015
[51]	Collaborazione MELANI-UFAE/allineamento informazioni sulla SNPC	Processo di collaborazione MELANI-UFAE	
[52]	Befundsliste: Ufficio federale dell'aviazione civile	DEFR	20.09.2015
[53]	Review Kommentare Stromversorgung	Review Kommentare Stromversorgung	???
[54]	Erstellung und Abnahme von Verwundbarkeitsanalysen	UFAE	11.09.2014
[55]	Massnahmen zur Steigerung der Resilienz im Luftverkehr	UFAE	12.01.2016
[56]	Kommentiertes Inhaltsverzeichnis Risiko- und Verwundbarkeitsanalyse in kritischen Teilsektoren	UFPP	
[57]	Reporting intermedio MS 2.1: Analisi dei rischi e della vulnerabilità della SNPC	UFPP	
[58]	Umsetzungsplanung M2 NCS / M15 SKI-Strategie	UFPP/UFAE	18.03.2014

Titolo		Autore/editore	Data
[59]	Kommentiertes Inhaltsverzeichnis Massnahmen zur Verbesserung der Resilienz kritischer Teilsektoren	UFPP	
[60]	Reporting intermedio MS 12.1: Massnahmen zur Verbesserung der Resilienz NCS	UFPP/UFAE	
[61]	Memorandum del colloquio UFAE-UFPP sull'attuazione della strategia SNPC/PIC	UFPP	24.03.2014
[62]	E-mail, altri indirizzi: Strategia per la protezione della Svizzera contro i cyber-rischi	Hansjörg Holenstein, AES	19.03.2015
[63]	Review-Kommentare Stromversorgung		15.03.2016
[64]	Prozessdarstellung zur Erstellung und Freigabe von Verwundbarkeitsanalysen NCS	UFAE	11.09.2014
Analisi della vulnerabilità TIC della Confederazione (M3)			
[65]	Antrag für den STA NCS (25.02.2016): Sondermassnahme zur Massnahme 3	DFF	25.02.2016
[66]	Verwundbarkeitsanalyse für die Prozesse- und IKT-Systemkomponenten		
[67]	Strategia nazionale per la protezione della Svizzera contro i cyber-rischi SNPC, misura 3: Analisi della vulnerabilità delle infrastrutture TIC dell'Amministrazione federale mediante un piano di verifica, Basisdokument	DFF	11.11.2015
[68]	Strategia nazionale per la protezione della Svizzera contro i cyber-rischi SNPC, misura 3: Analisi della vulnerabilità delle infrastrutture TIC dell'Amministrazione federale mediante un piano di verifica, obiettivo intermedio 3.3: Prüfkonzept	DFF	11.11.2015
[69]	Strategia nazionale per la protezione della Svizzera contro i cyber-rischi SNPC, misura 3: Analisi della vulnerabilità delle infrastrutture TIC dell'Amministrazione federale mediante un piano di verifica, obiettivo intermedio 3.2: il piano è contenuto nel progetto e viene costantemente sviluppato	DFF	04.02.2015
[70]	Strategia nazionale per la protezione della Svizzera contro i cyber-rischi SNPC, misura 3: Analisi della vulnerabilità delle infrastrutture TIC dell'Amministrazione federale mediante un piano di verifica, obiettivo intermedio 3.1: Grobkonzept (documento programmatico per la preparazione di un piano di verifica)	DFF	02.09.2014
Rappresentazione della situazione (M4) e identificazione degli autori (M14)			
[71]	Bedrohungslage im Cyberraum	MELANI	

Titolo		Autore/editore	Data
[72]	Strategia nazionale per la protezione della Svizzera contro i cyber-rischi SNPC, misure 4 e 14: rappresentazione della situazione e identificazione degli autori, obiettivi intermedi 4.6 e 14.3: le conoscenze specifiche e le capacità nell'ambito del cyberspazio vengono sviluppate presso il SIC, con BAC e SIM quali fornitori di prestazioni	DFF	
[73]	Strategia nazionale per la protezione della Svizzera contro i cyber-rischi SNPC, misura 4: Piano per il rafforzamento di MELANI come piattaforma per lo scambio di informazioni	DFF	20.02.2014
[74]	Attuazione della cyber-strategia nazionale (SNPC) presso il SIC, Bericht zu den Meilensteinen (4.2, 5.1, 14.1 della Umsetzungs-Roadmap)	DDPS	
[75]	Strategia nazionale per la protezione della Svizzera contro i cyber-rischi SNPC, misura 4: Elaborazione della rappresentazione e dell'evoluzione della situazione, obiettivo intermedio 4.3: l'adeguamento del Service Level Agreement (SLA) assieme al BAC-CEO è stato fatto	DFF	
[76]	Strategia nazionale per la protezione della Svizzera contro i cyber-rischi SNPC, misura 4: Elaborazione della rappresentazione e dell'evoluzione della situazione, obiettivo intermedio 4.4: Radar de la situation.	DFF	
[77]	Passive DNS Plattform	MELANI	22.12.2014
[78]	Strategia nazionale per la protezione della Svizzera contro i cyber-rischi SNPC, misure 4 e 14: Rappresentazione della situazione e identificazione degli autori, obiettivi intermedi 4.6 e 14.3: le conoscenze specifiche e le capacità nell'ambito del cyberspazio vengono sviluppate presso il SIC, con il BAC e il SIM come fornitori di prestazioni	DFF	
[79]	Strategia nazionale per la protezione della Svizzera contro i cyber-rischi SNPC, misura 14: Misure attive e identificazione degli autori, obiettivo intermedio 14.2: l'adeguamento del Service Level Agreement (SLA) assieme al BAC-CEO è stato fatto	DFF	
Analisi degli eventi (M5)			
[80]	Strategia nazionale per la protezione della Svizzera contro i cyber-rischi SNPC, misura 5: Analisi ed elaborazione di eventi, obiettivo intermedio 5.2: Organisationsstruktur GovCERT	DFF	29.04.2014
[81]	Strategia nazionale per la protezione della Svizzera contro i cyber-rischi(SNPC), misura 5: Analisi ed elaborazione di eventi, obiettivo intermedio 5.3: Erhöhung der Durchhaltefähigkeit im GovCERT	DFF	30.06.2014

Titolo		Autore/editore	Data
[82]	Strategia nazionale per la protezione della Svizzera contro i cyber-rischi SNPC, misura 5: Analisi ed elaborazione di eventi, obiettivo intermedio 5.4: la Malware Information Sharing Plattform (MISP) è approntata	DFF	16.06.2014
[83]	Passive DNS Platform	MELANI	18.06.2015
Panoramica dei casi penali (M6)			
[84]	Cyberkriminalitäts-Phänomene: Definitionen, Modus operandi und Massnahmen	DFGP	28.05.2015
[85]	Stato di attuazione della misura 6 SNPC: Übersicht Straffälle und Koordination interkantonaler Fallkomplexe	DFGP	20.08.2015
[86]	Rapporto annuale 2014: Servizio di coordinazione per la lotta contro la criminalità su Internet SCOCI	DFGP	26.03.2015
[87]	Documento programmatico per la misura 6 SNPC: Nationale Fallübersicht und Koordination interkantonaler Fallkomplexe	DFGP	Marzo 2016
[88]	Tabella delle strutture reato prioritario/settore del reato		
[89]	Stato di attuazione della misura 6 SNPC: Übersicht Straffälle und Koordination interkantonaler Fallkomplexe	DFGP	20.08.2015
Internet governance (M9) e standardizzazione internazionale (M11)			
[90]	Strategia nazionale per la protezione della Svizzera contro i cyber-rischi SNPC, misura 9: Internet governance, obiettivo intermedio 9.1: Übersicht zu prioritären Veranstaltungen, Initiativen und internationalen Gremien mit Bezug zur Internet Governance	UFCOM	30.05.2014
[91]	Strategia nazionale per la protezione della Svizzera contro i cyber-rischi SNPC: misura 9 «Internet governance», obiettivo intermedio 9.2: la panoramica sui processi di Internet governance e la partecipazione della svizzera sono approntate	UFCOM	30.05.2014
[92]	Obiettivo intermedio 9.3 della SNPC: Prioritäten der Schweiz in der Internet Governance und die Einbindung relevanter Akteure	UFCOM	20.10.2014
[93]	Workshop SNPC-M11	UFCOM	15.02.2016
[94]	Strategia nazionale per la protezione della Svizzera contro i cyber-rischi SNPC: misura 11: Iniziative internazionali e processi di standardizzazione nel settore della sicurezza: Übersicht über die Gremien im Bereich Sicherheit, Sicherung und Standardisierung	UFCOM	10.12.2014

Titolo		Autore/editore	Data
[95]	Strategia nazionale per la protezione della Svizzera contro i cyber-rischi SNPC: misura 11: Iniziative internazionali e processi di standardizzazione nel settore della sicurezza: Übersicht über beteiligte Akteure aus der Schweiz und deren Tätigkeiten	UFCOM	11.12.2015
[96]	Strategia nazionale per la protezione della Svizzera contro i cyber-rischi SNPC: misura 11: Iniziative internazionali e processi di standardizzazione nel settore della sicurezza: Übersicht über die Gremien im Bereich Sicherheit, Sicherung und Standardisierung	UFCOM	11.12.2015
[97]	Strategia nazionale per la protezione della Svizzera contro i cyber-rischi SNPC: misura 11: Iniziative internazionali e processi di standardizzazione nel settore della sicurezza: Übersicht über die Gremien im Bereich Sicherheit, Sicherung und Standardisierung	UFCOM	10.12.2014
Cooperazione internazionale (M10)			
[98]	Jahresübersicht der Aktivitäten im Cyber-Bereich		2014
[99]	Jahresübersicht der Aktivitäten im Cyber-Bereich		2015
[100]	Fragenkataloge WiÜ NCS – Cooperazione internazionale in materia di sicurezza cibernetica (misura 10)	Philipp Grabher e Markus Meier, AWK	08.03.2016
[101]	Promemoria per il segretario di Stato: Cyber-Kriminalität: Aussenpolitische Positionierung und Handlungsfelder für die Schweiz	DFAE	10.02.2015
[102]	Promemoria per il segretario di Stato: Cyber-Sicherheit: Schweizer Handlungsfelder zur Förderung von staatlichen Verhaltensnormen	DFAE	12.08.2015
[103]	Konzept zur Umsetzung der nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken im EDA		20.12.2013
[104]	Übersicht der in 2014 geleisteten Aktivitäten im Bereich Cyber-Aussenpolitik	DFAE	09.04.2015
[105]	Stato di attuazione della misura 6 SNPC: Übersicht Straffälle und Koordination interkantonaler Fallkomplexe	DFGP	20.08.2015
[106]	Aussenpolitische Aufgaben im Cyber-Bereich – Eine Übersicht der in 2015 geleisteten Aktivitäten	DFAE	04.01.2016
[107]	A Geneva Declaration for Cyberspace	Stein Schjolberg, Norvegia	Gennaio 2016
[108]	Mandat Fachgruppe Cyber-International (FG-CI)	DFAE	21.03.2014
[109]	Promemoria per il segretario di Stato: Cyber-Kriminalität: Aussenpolitische Positionierung und Handlungsfelder für die Schweiz	DFAE	10.02.2015
[110]	Promemoria per il segretario di Stato: Cyber-Sicherheit: Schweizer Handlungsfelder zur Förderung von staatlichen Verhaltensnormen	DFAE	12.08.2015

Titolo	Autore/editore	Data
[111] Promemoria per il segretario di Stato: Internet Governance: Aussenpolitische Grundlagen und Handlungsfelder für das EDA	DFAE	04.03.2015
[112] Konstituierende Sitzung der Fachgruppe Cyber-International (FG-CI)	DFAE	25.10.2013
[113] Protokoll Fachgruppe Cyber-International (FG-CI)	DFAE	21.03.2014
[114] Protokoll Cyber-International (FG-CI)	DFAE	18.12.2014
[115] Protokoll Fachgruppe Cyber-International (FG-CI)	DFAE	30.06.2015
[116] Protokoll: Fachgruppe Cyber-International (FG-CI)	DFAE	25.09.2015
Gestione delle crisi (M13, M15)		
[117] Konzept für das nationale Krisenmanagement bei Krisen mit Cyberausprägung auf der Grundlage der Massnahme 15 NCS		16.04.2016
[118] Auswertung Evaluation MELANI	Manuel Suter, SC SNPC	07.01.2016
[119] Fragebogen Evaluation MELANI	Manuel Suter, SC SNPC	
[120] Resultate Evaluation MELANI	SC SNPC	Marzo 2016
[121] Bericht der ersten Cyber Koordinationssitzung	Dario Walder, RSS	25.03.2013
[122] Serie di diapositive sul 3° Cyber-Landsgemeinde		23.04.2015
[123] Seminario strategico dell'11.06.2015, Kurzbericht		11.06.2015
[124] Attuazione misura 15 SNPC: Konzept für das Krisenmanagement bei Cyberkrisen	Stéphane Derron	26.09.2013
[125] Attuazione misura 15 SNPC: Konzept für das Krisenmanagement bei Cyberkrisen (Stufe Bund)	Stéphane Derron	17.02.2014
[126] Programma del 4° Cyber-Landsgemeinde		06.04.2016
Basi legali (M16)		
[127] Strategia nazionale per la protezione della Svizzera contro i cyber-rischi SNPC: misura 16: Necessità di modificare le basi legali, obiettivo intermedio 16.1: Übersicht zum vordringlichen Gesetzgebungs- und Revisionsbedarfs im Cyber-Bereich	Stefanie Frey, SC SNPC	30.06.2014
Interfacce RSS		
[128] Informationsblatt zur Fachgruppe und den Arbeitsgruppen Cyber des SVS	RSS	25.02.2016
[129] SVS: NCS und Schnittstellen zu den Kantonen	RSS	20.05.2016
[130] Bearbeitung der von MELANI ausgegebenen Meldungen	RSS	22.10.2015

C. Raccolta di tutti i questionari delle interviste

Tutti i questionari compilati con i partner intervistati sono raccolti in un allegato separato che è classificato come CONFIDENZIALE. Può essere visionato presso il SC SNPC.