Rapporto annuale 2016

sullo stato di attuazione della Strategia nazionale per la protezione della Svizzera contro i cyber-rischi (SNPC)

Comitato direttivo SNPC

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD
Informatiksteuerungsorgan des Bundes ISB
Melde- und Analysestelle Informationssicherung MELANI

Pubblicazione: Maggio 2017

Redazione: Servizio di coordinamento SNPC

Dipartimento federale delle finanze DFF

Organo direzione informatica della Confederazione (ODIC)
Centrale d'annuncio e d'analisi per la sicurezza dell'informazione

Schwarztorstrasse 59
CH-3003 Berna

Tel. +41 (0)58 462 45 38
E-mail: info@isb.admin.ch

Rapporto annuale SNPC: www.isb.admin.ch

Indice

Premessa

Anche nel corso del 2016 si è confermata la crescente importanza e complessità della digitalizzazione e dell'automatizzazione in tutti gli ambiti della vita. Questa tendenza è risultata particolarmente evidente all'ultima edizione del CeBIT, di cui la Svizzera è stata il Paese partner. La fiera, che si poneva all'insegna della progressiva digitalizzazione e automatizzazione di nuovi settori, ha fornito dimostrazioni emblematiche in tal senso coi progressi nello sviluppo verso la mobilità autonoma o sull'esempio di robot che si sostituiscono all'uomo nell'espletamento di numerose mansioni. Le opportunità offerte dalla digitalizzazione assumono grande importanza anche per la Svizzera. Purtroppo, però, comportano anche dei rischi, come hanno mostrato in modo eloquente i recentissimi cyber-attacchi. Attività di spionaggio e sabotaggio, nuove forme di malware finora sconosciute e ricatti con attacchi DDoS sono all'ordine del giorno. Pertanto, se vogliamo essere pronti ad affrontare la crescente minaccia dei cyber-attacchi, dobbiamo tenere alta la guardia e accrescere ulteriormente la cyber-sicurezza.

La domanda principale che dobbiamo porci appare dunque scontata: la Svizzera è sulla strada giusta e le odierne misure di protezione sono sufficienti per neutralizzare i cyber-rischi in modo duraturo? Con l'approvazione della «Strategia nazionale per la protezione della Svizzera contro i cyber-rischi (SNPC)» e il suo piano di attuazione ci siamo mossi nella direzione giusta e abbiamo già ottenuto parecchi risultati. In concreto, entro la fine del 2016 sono state concluse 15 delle 16 misure della SNPC in programma. Il successo nella loro attuazione è stato sottoposto nel 2016 a una verifica dell'efficacia, la quale ha illustrato gli ambiti in cui gli obiettivi sono stati centrati e quelli che richiedono ancora degli interventi. I risultati di questa verifica sono sintetizzati brevemente nel presente rapporto.

Senza anticipare i risultati della verifica dell'efficacia, si può affermare che l'attuazione della SNPC ha consentito di compiere considerevoli progressi in numerosi settori. Grazie alla SNPC abbiamo posto la prima pietra di una collaborazione improntata alla fiducia tra la Confederazione, i Cantoni, l'economia e la società per proteggere meglio la Svizzera contro i cyber-attacchi. Anche sul piano internazionale, nell'ambito della politica estera e di sicurezza, la Svizzera ha continuato a impegnarsi per un cyber-spazio aperto, libero e sicuro. Nel 2016, il nostro Paese è stato scelto per far parte del gruppo di esperti dell'ONU sulla cyber-sicurezza[1] per un periodo di un anno.

I risultati degli ultimi anni e gli esiti della verifica dell'efficacia hanno evidenziato come tanto sia stato fatto, ma ancora molto rimanga da fare. Anche nel 2017 intraprenderemo pertanto tutti i passi necessari affinché la Svizzera possa continuare a utilizzare Internet come spazio sicuro, aperto e libero per l'economia, le autorità e la popolazione. Pensiamo in particolare all'ulteriore sviluppo della SNPC. L'attuazione dell'attuale SNPC si concluderà entro la fine di quest'anno, ma noi siamo già al lavoro per definire l'ulteriore modo di procedere in stretta collaborazione con tutti i soggetti interessati.

In questo senso saremo lieti di rafforzare, insieme a voi, la protezione della Svizzera contro i cyber-rischi in modo da poter sfruttare le opportunità della digitalizzazione senza correre rischi eccessivi.

Peter Fischer
Delegato per la direzione informatica della Confederazione (ODIC)

[1] UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.

1 Sintesi

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 suo piano di attuazione. La SNPC, articolata in 16 misure, è incentrata sull'identificazione precoce dei cyber-rischi, sul rafforzamento della capacità di resistenza delle infrastrutture critiche e sulla riduzione delle cyber-minacce, in particolare lo spionaggio, il sabotaggio e la cyber-criminalità.

L'attuazione della SNPC è organizzata in modo decentralizzato. Per ciascuna delle 16 misure, la responsabilità è stata affidata a un Ufficio federale. Questi lavori vengono organizzati dal servizio di coordinamento (SC SNPC), aggregato alla Centrale d'annuncio e d'analisi per la sicurezza dell'informazione (MELANI) in seno all'Organo direzione informatica della Confederazione (ODIC). La responsabilità generale spetta al comitato direttivo (CD SNPC), incaricato di seguire i lavori di attuazione mediante un controlling strategico.

Le 16 misure interessano quattro settori: prevenzione, reazione, continuità e processi di sostegno (collaborazione internazionale, ricerca e formazione, basi legali). Negli anni scorsi sono stati raggiunti importanti obiettivi in tutti i settori, anche grazie a una stretta collaborazione e a una proficua comunicazione con tutti gli attori coinvolti. Ciò ha consentito di concludere, entro la fine del 2016, 15 delle 16 misure della SNPC e di rispettare la tabella di marcia indicata nel piano di attuazione. Dalla verifica dell'efficacia eseguita nel 2016 è inoltre emerso che la SNPC ha prodotto un considerevole effetto e che l'approccio decentralizzato e basato sui rischi ha dato buoni risultati.

Nell'ambito della **prevenzione**, l'Ufficio federale della protezione della popolazione (UFPP) e l'Ufficio federale per l'approvvigionamento economico del Paese (UFAE) hanno condotto analisi dei rischi e della vulnerabilità nei sottosettori critici identificati nella «Strategia per la protezione delle infrastrutture critiche (PIC)». I relativi rapporti sono ora disponibili.

La rappresentazione delle minacce globali in atto è stata allestita a cura del Servizio delle attività informative della Confederazione (SIC). Questa riproduzione interattiva, il cosiddetto radar della situazione di minaccia, visualizza le diverse cyber-minacce per le infrastrutture svizzere indicandone inoltre la rilevanza. A partire dal 2017, il radar della situazione verrà messo a disposizione dei membri della cerchia chiusa di clienti di MELANI. Una panoramica delle principali cyber-minacce nel 2016 è contenuta nel Rapporto semestrale MELANI e nel Rapporto annuale fedpol (Ufficio federale di polizia).

Nel settore della **reazione**, nel 2016 sono stati ulteriormente potenziati i centri di competenze specialistiche per l'analisi dei software nocivi presso l'ODIC e il Dipartimento federale della difesa, della protezione della popolazione e dello sport (DDPS), ad es. GovCERT-ODIC, CI-SIRT-UFIT, milCERT-DDPS, nonché sviluppati numerosi altri prodotti che accrescono la capacità di individuazione e di reazione. Inoltre, si è provveduto a implementare importanti processi interni ed esterni volti a migliorare la comunicazione e a rafforzare la collaborazione internazionale.

Nella divisione specializzata Cyber del Servizio delle attività informative della Confederazione (SIC) si sono potute acquisire conoscenze e competenze specialistiche che consentono di analizzare gli obiettivi, i metodi e gli attori di un attacco e di identificare in tal modo i possibili autori. La legge sulle attività informative (LAIn) accolta dal popolo introduce inoltre la base legale che autorizza il SIC a intraprendere contromisure anche offensive in caso di cyber-attacchi gravi a infrastrutture critiche, agevolando l'acquisizione di informazioni da parte del Servizio delle attività informative. Al momento, tuttavia, per una gestione più sistematica e duratura dei cyber-attacchi presso il SIC mancano soprattutto ulteriori analisti tecnici e operativi così come specialisti di lingue.

Nell'ambito della **continuità**, l'UFPP e l'UFAE insieme con i gestori delle infrastrutture critiche e le autorità specializzate, di vigilanza e di regolamentazione competenti elaborano misure volte a migliorare la resilienza TIC nei sottosettori critici. Queste attività si basano sui risultati delle analisi dei rischi e della vulnerabilità e servono a ridurre i punti deboli e i rischi

identificati. Al riguardo occorre rilevare come per molti settori divenga sempre più importante l'introduzione di linee guida e standard minimi e si debba tenere conto della necessità di coordinare le misure con le direttive esistenti.

Nei **processi di sostegno** l'accento è posto sulla ricerca e sulla formazione nonché sulla collaborazione internazionale. La Segreteria di Stato per la formazione, la ricerca e l'innovazione (SEFRI) ha costituito insieme al SC SNPC organi importanti che, in collaborazione con l'economia e l'Amministrazione, hanno allestito una panoramica delle offerte di formazione in materia di creazione di competenze e formulato proposte per impiegare tali offerte ed eliminare le lacune riscontrate. In collaborazione con l'associazione ICT-Formazione professionale Svizzera e grazie al sostegno di numerose imprese è stato possibile istituire a tempo di record un nuovo diploma federale di «Esperto in sicurezza delle TIC».

Contestualmente, nell'ambito di un rapporto di esperti si è provveduto a identificare i principali temi di ricerca sui cyber-rischi in Svizzera. Inoltre, in seno all'Amministrazione, il coordinamento dei servizi specialistici correlati alla ricerca (cyber-rischi) è stato affidato a un nuovo comitato che coinvolge uffici e dipartimenti vari. La rete dei ricercatori ha potuto essere potenziata in occasione della «Swiss Cyber Risk Research Conference».

La collaborazione internazionale nell'ambito della pace e della sicurezza internazionale è stata ulteriormente rafforzata e ampliata a livello bilaterale e multilaterale sotto la direzione della Divisione politica di sicurezza (DPS) del Dipartimento federale degli affari esteri (DFAE). La responsabilità per il settore Internet governance competeva all'Ufficio federale delle comunicazioni (UFCOM). A livello bilaterale sono stati instaurati nuovi contatti e intensificati quelli esistenti. Sul piano multilaterale si è provveduto a sviluppare ulteriormente i lavori relativi alle misure di rafforzamento della fiducia dell'OSCE; nel 2016, inoltre, la Svizzera è stata scelta per far parte per un anno dello «UN Group of Governmental Experts (UN GGE)» sulla cyber-sicurezza.

Principali cyber-minacce nel 2016

Il 2016 è stato caratterizzato principalmente da cyber-minacce analoghe a quelle del 2015.[2] Una differenza sostanziale è rappresentata tuttavia dall'intensità e dalla frequenza dei cyber-attacchi, nel senso che durante l'anno in rassegna si è potuta osservare una crescente specializzazione. Si è inoltre notato un aumento del numero di atti criminali derivanti da operazioni di spionaggio. Come evidenzia il Rapporto semestrale MELANI 2016/2, il cyber-spionaggio è un pericolo da prendere sul serio e le imprese devono essere consapevoli che si tratta di un rischio reale e non ipotetico. Una conferma in tal senso giunge dai numerosi casi di cui è a conoscenza MELANI. Un'altra tendenza preoccupante consiste negli attacchi complessi, i cosiddetti advanced persistent threat (APT), che sono sempre più frequenti anche tra i cyber-criminali.

Qui di seguito sono riportati in sintesi i maggiori pericoli rilevati per il 2016[3]:

- **spionaggio** (attacco a un'azienda produttrice di armamenti);
- **furto di dati** (dati di accesso a Twitter sul mercato nero, furto di password);
- **DDoS e ricatti** (Cryptolocker, Locky, Armada Collective, KeRanger, CTB Locker);
- **social engineering e phishing** (CEO Fraud);
- **crimeware** (trojan di e-banking come Gozi, Conficker, Dyre);
- **attacchi a sistemi di controllo industriali** (attacco ai sistemi di controllo in centrali elettriche ucraine).

[2] Rapporto semestrale MELANI 2015 (gennaio-giugno): www.melani.admin.ch

[3] Per i dettagli relativi a queste minacce si rimanda al Rapporto semestrale MELANI 2016 (gennaio-giugno): www.melani.admin.ch

2 Stato dei lavori di attuazione della SNPC 2016

La SNPC è una strategia integrale, che con le sue 16 misure (M1-M16) persegue un approccio globale per proteggere la Svizzera dalle cyber-minacce. Le misure si suddividono in quattro settori in base al loro sviluppo temporale e alle loro interdipendenze:

- prevenzione (M2, M3, M4);
- reazione (M5, M6, M14);
- continuità (M12, M13, M15);
- processi di sostegno (M1, M7, M8, M9, M10, M11, M16).

In questo capitolo il quadro generale dell'attuazione è spiegato sulla base di una roadmap. Nei capitoli seguenti un breve rapporto del rispettivo Ufficio responsabile informa sullo stato attuale dell'attuazione delle singole misure nei quattro settori.

Roadmap SNPC

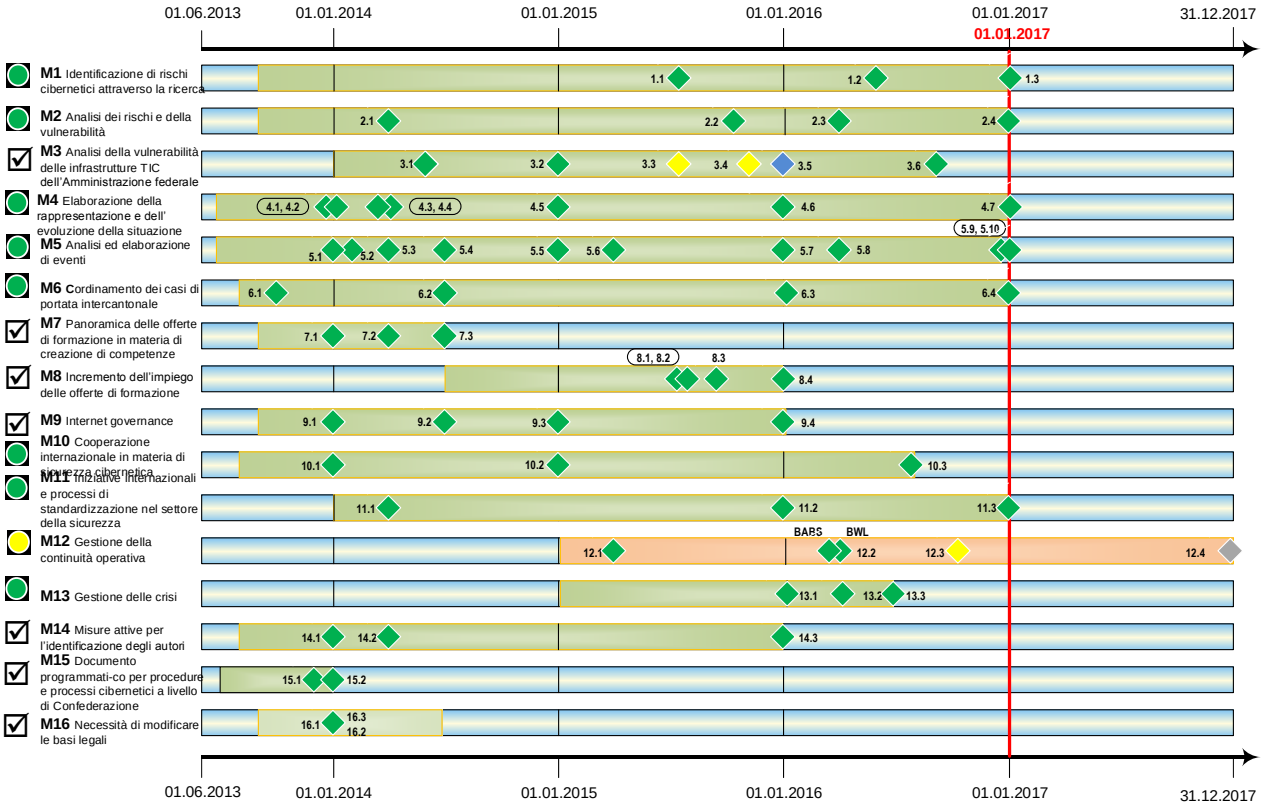

Figura 1: Roadmap SNPC

Legenda: stato di avanzamento delle tappe principali

- Tappa principale compromessa
- Tappa principale ritardata
- Tappa principale attuata secondo il piano
- Misura straordinaria

2.1 Prevenzione

La prevenzione riguarda le seguenti misure: analisi dei rischi e della vulnerabilità (M2), analisi della vulnerabilità delle infrastrutture TIC dell'Amministrazione federale (M3) e rappresentazione della situazione (M4).

2.1.1 Misura 2: Analisi dei rischi e della vulnerabilità

Responsabilità: DEFR-UFAE, DDPS-UFPP, autorità specializzate, di vigilanza e di regolamentazione; DFF-MELANI

L'obiettivo della misura è quello di individuare le vulnerabilità delle infrastrutture critiche TIC per la Svizzera. I cyber-rischi si presentano quando queste vulnerabilità sono minacciate (ad es. attacchi informatici).

L'UFAE e l'UFPP si dividono i lavori nei 28 sottosettori complessivi della Svizzera e coordinano il loro modo di procedere. Nei singoli sottosettori le analisi dei rischi e della vulnerabilità si sono svolte in larga misura secondo i piani. In questo contesto sono stati consultati numerosi esperti delle aziende e delle associazioni di categoria, così come delle autorità specializzate, di vigilanza e di regolamentazione competenti a livello federale e cantonale. Le analisi poggiano pertanto su un ampio consenso e nel contempo confermano il grande interesse dei servizi coinvolti.

Stato attuale
Questa misura è stata ampiamente conclusa nel 2016; seguiranno ancora attività di finalizzazione. In questo contesto sono state eseguite analisi della vulnerabilità in 28 sottosettori critici. Le analisi fungono da base per l'elaborazione di misure volte a rafforzare la capacità di resistenza TIC (cfr. capitolo 3.3.1 Gestione della continuità operativa).

2.1.2 Misura 3: Analisi della vulnerabilità delle infrastrutture TIC dell'Amministrazione federale sulla base di un piano di verifica

Responsabilità: DFF-ODIC; DFF-MELANI e UFIT, DDPS-BAC

Secondo la SNPC gli Uffici federali devono verificare le vulnerabilità delle proprie infrastrutture TIC considerando i fornitori di prestazioni TIC come pure i fornitori di sistemi. L'ODIC è stato incaricato di predisporre un piano per verificare periodicamente le vulnerabilità sistemiche, organizzative e tecniche delle infrastrutture TIC dell'Amministrazione federale.

Stato attuale
Questa misura è stata conclusa nel 2016.

In adempimento al proprio mandato, l'ODIC ha allestito entro la fine del 2015 un piano di verifica per le infrastrutture TIC dell'Amministrazione federale (denominato di seguito «piano di verifica»). Quest'ultimo è improntato alle best practice e agli standard basati sul rischio affermati nella gestione della sicurezza TIC (ad es. ISF IRAM2) e riflette in tal senso la dottrina attuale. L'implementazione del piano di verifica comporterebbe però un ingente carico di lavoro; per questa ragione, il 25 febbraio 2016 il comitato direttivo SNPC (CD SNPC) su richiesta dell'UFAE, del DFAE e del SIC ha incaricato l'ODIC di elaborare ai sensi di una misura straordinaria relativa alla M3 una proposta alternativa al piano di verifica che definisse l'ulteriore modo di procedere nel settore delle analisi della vulnerabilità TIC nell'Amministrazione federale. Sebbene il servizio a tempo determinato per la M3 fosse già stato sospeso alla fine del 2015, l'ODIC in seno a questa misura straordinaria ha saputo mettere a punto un nuovo approccio e lo ha sottoposto al CD SNPC il 31 maggio 2016. Il CD SNPC si è espresso a favore della proposta, che rinuncia sostanzialmente a un approccio basato sul rischio e prevede al suo posto un'analisi della vulnerabilità.

2.1.3 Misura 4: Elaborazione della rappresentazione e dell'evoluzione della situazione

Responsabilità: **DFF-MELANI, DDPS-SIC, DFGP-SCOCI;** DDPS-BAC e SIM, DFF-UFIT

Per fronteggiare i cyber-attacchi occorre una rappresentazione della situazione che informi degli sviluppi in atto nel settore e descriva i rischi e i danni potenziali degli attacchi per i rispettivi settori critici oltre che la loro rilevanza per la Svizzera.

Tutte le informazioni rilevanti evinte dalle analisi tecniche e attinte dal Servizio delle attività informative e dalla polizia devono confluire nella rappresentazione della situazione affinché questa sia per quanto possibile completa. A tal fine occorre definire i processi presso i singoli attori e tra di essi e assegnare le responsabilità. Fra gli attori figurano il Computer Emergency Response Team di MELANI all'interno dell'ODIC (GovCERT), l'Operation Information Center di MELANI nel SIC (OIC MELANI), il settore Cyber nel SIC e il Servizio informazioni militare (SIM). L'obiettivo della SNPC è quello di allestire un quadro della situazione in stretta collaborazione con tutti gli attori rilevanti.

Stato attuale
Questa misura è stata conclusa nel 2016.

Si è provveduto ad allestire la rappresentazione delle minacce globali in atto. A partire dal 2017, questa riproduzione interattiva (radar della situazione di minaccia) verrà messa a disposizione dei membri della cerchia chiusa di clienti di MELANI. Una versione pubblica dovrà seguire in un secondo tempo.

È stata anche redatta una perizia esterna che giudica i processi avviati di MELANI ai fini di un miglioramento autonomo.

2.2 Reazione

Per poter reagire il più velocemente possibile in caso di eventi sono necessarie un'analisi coordinata dell'evento e la sua elaborazione. La SNPC prevede un rafforzamento delle capacità e un potenziamento della capacità di reazione di tutte le organizzazioni e degli attori interessati. Ciò garantisce una rapida analisi degli eventi, un sollecito intervento delle autorità di perseguimento penale e la possibilità di identificare tempestivamente gli autori. Nel settore della reazione sono previste le seguenti misure: analisi ed elaborazione di eventi (M5), panoramica dei casi penali e coordinamento dei casi di portata intercantonale (M6) nonché misure attive per l'identificazione degli autori (M14).

2.2.1 Misura 5: Analisi ed elaborazione di eventi

Responsabilità: DFF-MELANI, DDPS-SIC; DDPS-BAC e SIM, DFF-UFIT

La capacità di essere pronti ad affrontare cyber-eventi e di reagire ad essi è una condizione essenziale per la riduzione dei cyber-rischi. Secondo il piano di attuazione della SNPC, le attività di analisi ed elaborazione di eventi devono essere ulteriormente sviluppate. I diversi Computer Emergency Response Team (CERT) come GovCERT, CISIRT-UFIT e milCERT-DDPS dovranno ampliare le competenze nell'ambito dell'analisi di malware affinché, in caso di evento, sia possibile analizzare e trattare i dati nonché adottare contromisure di natura tecnica. Per adempiere a questo mandato, occorre in primo luogo ampliare le capacità tecniche e le conoscenze specialistiche e procedere in secondo luogo a un'analisi e a una valutazione esaustive delle minacce. È altresì necessario migliorare la capacità di resistenza, aumentare la capacità di reazione di tutti i CERT e creare una rete di questi ultimi.

Stato attuale
Questa misura è stata conclusa nel 2016.

Nell'insieme si è provveduto ad ampliare la capacità di individuazione e di reazione presso i centri di competenze specialistiche (GovCERT, UFIT-CISIRT, mil-CERT).

Inoltre, la LAIn, accolta dal popolo svizzero nel 2016, prevede espressamente che le infrastrutture critiche vengano protette contro i cyber-attacchi dal Servizio delle attività informative e introduce la base legale che autorizza il SIC a intraprendere contromisure anche offensive in caso di cyber-attacchi gravi a infrastrutture critiche. Nella LAIn, ai fini dell'acquisizione di informazioni da parte del Servizio delle attività informative, è contemplata anche la penetrazione in sistemi informatici e reti.

Nel 2016 è stato assegnato il posto di lavoro creato nell'ambito della SNPC per fare chiarezza nel settore cyber. Qui di seguito sono elencate le mansioni svolte:

- reclutamento e gestione delle fonti (ingaggio di esperti esterni)
- acquisizione di informazioni (senza misure sottoposte ad autorizzazione ai sensi della LAIn)
- analisi strategiche
- analisi tecniche
- identificazione degli autori da parte del Servizio delle attività informative (attribuzione)
- cooperazione internazionale

La creazione di una rete di fonti e l'ulteriore interconnessione internazionale con i servizi dei partner hanno sempre consentito al SIC di scoprire i cyber-attacchi in una fase precoce. Oggi, tuttavia, il SIC, con i mezzi e le capacità a disposizione, può elaborare soltanto una piccola parte delle informazioni acquisite nel settore. I cyber-attacchi, inoltre, si protraggono spesso per anni impegnando a lungo i pochi specialisti in forza. Nel contempo aumenta il rischio che eventuali nuovi attacchi non possano essere individuati tempestivamente. Per questo motivo, un elemento centrale è rappresentato da una gestione più sistematica e duratura dei cyber-attacchi. Attualmente, però, per adempiere a questo mandato al SIC mancano soprattutto ulteriori analisti tecnici e operativi così come specialisti di lingue.

2.2.2 Misura 6: Documento programmatico per una panoramica dei casi penali e il coordinamento dei casi di portata intercantonale

Responsabilità: DFGP-SCOCI; DFF-MELANI

Per minimizzare i cyber-rischi in modo duraturo occorre un efficiente perseguimento penale nazionale e internazionale della criminalità informatica. A tale scopo, nella misura 6 della SNPC è stato sancito che il Servizio di coordinazione per la lotta contro la criminalità su Internet (SCOCI), aggregato all'Ufficio federale di polizia (fedpol) presso il Dipartimento federale di giustizia e polizia (DFGP), presenti, entro la fine del 2016, un documento programmatico «Panoramica dei casi penali e coordinamento dei casi di portata intercantonale» elaborato in collaborazione con i Cantoni.

Stato attuale
Questa misura è stata conclusa nel 2016.

Il coordinamento delle indagini nel settore della cyber-criminalità previsto nella misura 6 della SNPC e la rappresentazione della situazione generale in Svizzera sono già oggetto dell'accordo amministrativo tra il DFGP e la Conferenza dei direttori cantonali di giustizia e polizia (CDCGP) in merito ai mandati di base del SCOCI diretto da fedpol. Questi mandati di base del SCOCI, finanziato su base congiunta dalla Confederazione e dai Cantoni, hanno tuttavia potuto essere attuati fino ad ora solo in parte. Il documento programmatico relativo alla misura 6 della SNPC, frutto della collaborazione tra le autorità di perseguimento penale della Confederazione e dei Cantoni, propone misure per il rilevamento, il coordinamento e la divulgazione unitaria delle informazioni necessarie a elaborare la rappresentazione completa

della situazione sulla cyber-criminalità. Per l'auspicato coordinamento intercantonale dei casi in tutti i cyber-reati, il documento descrive prime misure di polizia volte a designare le autorità responsabili di perseguire localmente e materialmente gli autori che agiscono spesso dall'estero e attraverso cyber-infrastrutture straniere. Secondo la sessione autunnale del 18 novembre 2016, la CDCGP sostiene il documento programmatico.

La rappresentazione della situazione generale in Svizzera e il coordinamento intercantonale dei casi, tuttavia, sono solo due aspetti parziali della sfida alla cyber-criminalità. Per questa ragione, la Conferenza dei comandanti delle polizie cantonali della Svizzera (CCPCS) lavora all'elaborazione del dispositivo nazionale sulla cyber-criminalità e sull'informatica forense nell'ambito del quale dovranno essere affrontate nell'insieme tutte le questioni organizzative e infrastrutturali. A questi lavori partecipa anche fedpol. La questione concernente l'attuazione del documento programmatico relativo alla misura 6 dovrà essere dunque chiarita dalla CCPCS nell'ambito del suddetto dispositivo.

2.2.3 Misura 14: Misure attive per l'identificazione degli autori

Responsabilità: DDPS-SIC; DFF-MELANI, DFGP-SCOCI, DDPS-SIM

La SNPC intende potenziare le capacità del Servizio delle attività informative della Confederazione (SIC) per identificare gli autori (analisi degli attori e del contesto e sviluppo di strumenti tecnici). Anche qui è necessaria una stretta collaborazione dei rilevanti attori (MELANI, SIC, SCOCI, Cyber SIC e, a titolo sussidiario, l'esercito).

Stato attuale
Questa misura è stata conclusa nel 2016.

Alle considerazioni di cui al punto 3.2.1 si deve aggiungere che, anche nel 2016, il SIC ha saputo ricondurre cyber-attacchi contro la Svizzera a determinati attori statali o sostenuti da Stati. Queste scoperte sono confluite in brevi analisi, rapporti e note informative all'attenzione delle autorità competenti. L'attribuzione è un processo del Servizio delle attività informative che consente di identificare gli autori con una probabilità stimata e non prevede come obiettivo primario il perseguimento penale bensì la salvaguardia della capacità di agire nell'ambito della politica. I risultati sono pertanto indirizzati principalmente agli organi decisionali politici.

2.3 Gestione della continuità operativa e delle crisi

La gestione di una crisi presuppone procedure e processi di condotta chiaramente definiti per l'evento. La gestione della continuità operativa garantisce che i processi operativi siano disponibili anche durante una crisi. La continuità comprende le seguenti misure: gestione della continuità volta a migliorare la resilienza dei sottosettori critici (M12), coordinamento delle attività con gli attori interessati e supporto attraverso perizie specializzate (M13) nonché documento programmatico per procedure e processi di condotta che include anche i cyber-aspetti (M15).

2.3.1 Misura 12: Gestione della continuità operativa: miglioramento della resilienza dei sottosettori critici

Responsabilità: DEFR-UFAE, DDPS-UFPP, autorità specializzate, di vigilanza e di regolamentazione; DFF-MELANI

Sulla base dei risultati dell'analisi dei rischi e della vulnerabilità l'UFAE in qualità di responsabile e l'UFPP definiscono le misure necessarie a garantire la continuità operativa insieme con le imprese rilevanti e i responsabili servizi specialistici. Per ciascuno dei 28 sottosettori viene elaborato un rapporto sulle misure fondato sull'analisi dei rischi e della vulnerabilità.

Stato attuale
L'UFPP e l'UFAE, insieme con i gestori delle infrastrutture critiche e le autorità specializzate, di vigilanza e di regolamentazione competenti, elaborano misure volte a migliorare la resilienza TIC nei sottosettori critici. Queste attività si basano sui risultati delle analisi dei rischi e della vulnerabilità e servono a ridurre i punti deboli e i rischi identificati.

I rapporti sulle misure volte a migliorare la resilienza TIC di tutti i sottosettori critici definiti nella «Strategia per la protezione delle infrastrutture critiche (PIC)» saranno disponibili alla fine del 2017. Diverse misure sono già state attuate o si trovano in fase di implementazione. In tal modo potrà essere rafforzata la capacità di resistenza a perturbazioni e attacchi TIC dei sottosettori critici per l'approvvigionamento di beni e prestazioni di servizi importanti al nostro Paese.

2.3.2 Misura 13: Coordinamento delle attività con gli attori direttamente interessati e supporto con perizie specializzate

Responsabilità: DEFR-UFAE, DFF-MELANI, DDPS-UFPP; DFAE-DP, DFGP-SCOCI

In caso di crisi, MELANI fornisce agli attori interessati un supporto sussidiario mettendo a disposizione le proprie conoscenze e competenze. Lo scambio facoltativo di informazioni tra gestori di infrastrutture critiche, fornitori di prestazioni TIC e fornitori di sistemi viene assicurato al fine di rafforzare la continuità e la capacità di resistenza sulla base dell'autoaiuto. A questo scopo non sono stati soltanto garantiti, ma anche ulteriormente sviluppati i servizi attualmente disponibili.

Il DFAE viene informato nei casi in cui si presentano possibili implicazioni di politica estera ed è coinvolto nell'elaborazione della pianificazione preventiva.

Stato attuale
Questa misura è stata conclusa nel 2016.

La consultazione condotta nel novembre 2015 fra i membri della cerchia chiusa di clienti è stata oggetto di analisi nel 2016 e i risultati più importanti sono stati fissati in un rapporto. Il sondaggio evidenzia come il modello della collaborazione tra settore pubblico e privato di MELANI continui a funzionare bene. MELANI ha saputo far fronte anche alla forte crescita registrata negli ultimi anni dalla cerchia chiusa di clienti. Le sfide si pongono nel consolidamento di quei settori che ancora non si sono affermati pienamente.

Basandosi sui risultati di questo sondaggio, MELANI ha allestito un piano per il rafforzamento del proprio ruolo quale piattaforma di scambio di informazioni. Questo piano chiarisce il mandato di base e gli obiettivi di MELANI e illustra misure su come MELANI intenda svilupparsi ulteriormente a livello operativo e strategico. Il piano è integrato da una perizia sui provvedimenti proposti.

2.3.3 Misura 15: Documento programmatico per procedure e processi di condotta cibernetici

Responsabilità: CaF

La misura 15 intende integrare la gestione generale delle crisi con gli aspetti cibernetici.

Stato attuale
Questa misura è stata conclusa nel 2014.

La misura 15 è stata conclusa a livello di Confederazione con un documento programmatico per procedure e processi di condotta in situazioni di crisi che include anche i cyber-aspetti. Nel contempo è stata ulteriormente sviluppata la collaborazione con i Cantoni e i gestori di infrastrutture critiche nell'ambito dell'attuazione della SNPC da parte della Rete integrata Svizzera per la sicurezza nel gruppo di lavoro 3 Gestione delle crisi. Le attività di questo

gruppo di lavoro dovranno pertanto essere documentate anche nel rapporto annuale sull'attuazione della SNPC. I relativi dettagli sono riassunti al capitolo 3.6.

Nel novembre 2016 si è svolta l'esercitazione «Populа», che ha simulato un cyber-attacco al sistema previdenziale svizzero. Organizzata sotto la responsabilità della RSS in collaborazione con la Confederazione, i Cantoni e le infrastrutture critiche, aveva l'obiettivo di mettere alla prova la prontezza e la gestione delle crisi a livello federale e cantonale.

2.4 Processi di sostegno

Le cooperazioni internazionali, lo sviluppo di competenze attraverso la formazione e la ricerca ed eventualmente l'adeguamento delle basi legali costituiscono i fondamenti e i processi necessari ad affrontare la cyber-problematica. A tale scopo sono stati creati i seguenti pacchetti di misure:

- ricerca e formazione delle competenze (M1, M7, M8);
- cooperazioni internazionali (M9, M10, M11);
- basi legali (M16).

2.4.1 Misura 1: Identificazione di cyber-rischi attraverso la ricerca

Responsabilità: SEFRI; SC SNPC

Con l'aiuto della ricerca dovranno essere evidenziati i cyber-rischi rilevanti per il futuro, nonché i cambiamenti intervenuti nel panorama delle minacce, affinché le decisioni politiche ed economiche possano essere prese in modo tempestivo e mirato. A tal fine dovrà essere opportunamente utilizzata e rafforzata la ricerca (la ricerca di base e quella applicata) nell'ambito della protezione contro i cyber-rischi. La responsabilità per l'attuazione spetta alla SEFRI in collaborazione con il servizio di coordinamento SNPC (SC SNPC).

Stato attuale
Questa misura è stata conclusa nel 2016.

Nell'ambito dei lavori volti a identificare i temi di ricerca centrali si sono potuti compiere importanti progressi. Il comitato direttivo interdipartimentale «Ricerca e formazione nel settore dei cyber-rischi» (CoPIRFCyber) ha istituito un gruppo di esperti, composto da 15 specialisti delle scuole universitarie svizzere, e lo ha incaricato di identificare i principali temi di ricerca. Il gruppo di esperti ben assortito si è occupato a fondo delle diverse discipline, prospettive e sfide nel panorama della ricerca identificando nove campi in cui dare maggiore spazio alla ricerca in futuro. Inoltre, considerata la forte vocazione interdisciplinare della tematica, ha raccomandato come priorità della ricerca tre argomenti chiave di particolare rilevanza che coinvolgono materie e discipline diverse. Il rapporto 2016 consolidato dal gruppo di esperti verrà pubblicato presumibilmente nel 2° trimestre 2017.

L'11 gennaio 2017, il Consiglio federale, sulla scorta dei lavori di base svolti nel 2016 dalla SEFRI e dalla SECO, ha approvato il rapporto «Condizioni quadro dell'economia digitale» e incaricato nel contempo il Dipartimento federale dell'economia, della formazione e della ricerca (DEFR) di valutare a fondo le sfide che ne derivano nei settori della formazione e della ricerca. Secondo l'incarico si devono sostanzialmente valutare gli effetti sistemici della digitalizzazione sul settore della formazione e identificare le eventuali lacune a livello di scuole universitarie nella gestione della trasformazione digitale, coinvolgendo in tutto ciò i servizi federali competenti come pure i Cantoni e la Conferenza svizzera delle scuole universitarie. I lavori per la redazione del rapporto di valutazione (sezione Ricerca) riprenderanno, sviluppandoli ulteriormente se necessario, i risultati del rapporto di esperti sulla ricerca nel settore dei cyber-rischi (v. sopra).

La «Swiss Cyber Risk Research Conference», tenutasi il 20 maggio 2016 presso il Politec-

nico federale di Losanna, ha segnato un passo importante verso l'interconnessione e la sensibilizzazione dei ricercatori nel settore dei cyber-rischi. Oltre 300 partecipanti hanno seguito gli interventi di specialisti nazionali e internazionali. La conferenza ha lanciato un segnale importante a favore di un rafforzamento della ricerca sui cyber-rischi in Svizzera riunendo per la prima volta i ricercatori di tutte le discipline rilevanti.

2.4.2 Misura 7: Panoramica delle offerte di formazione

Responsabilità: SC SNPC; DATEC-UFCOM, DFAE-DP, DFI-UFAS

Per aumentare la resilienza della Svizzera nel settore cibernetico, è necessario creare e potenziare competenze specifiche in modo mirato. Secondo la SNPC occorre allestire una panoramica che fornisca informazioni sulle attuali offerte di formazione, in modo da individuare e colmare eventuali lacune nell'offerta. L'attuazione di questa misura è sintonizzata sull'attuazione della «Strategia del Consiglio federale per una società dell'informazione in Svizzera» e con il DFAE.

Stato attuale
Questa misura è stata conclusa nel 2015.

2.4.3 Misura 8: Incremento dell'impiego delle offerte di formazione in materia di creazione di competenze ed eliminazione delle lacune riscontrate nell'ambito delle offerte

Responsabilità: SC SNPC; SEFRI; DFAE-DP

La misura 8 intende, da un lato, accrescere le attuali offerte in materia di creazione di competenze concernenti la gestione dei cyber-rischi e, dall'altro, colmare le lacune riscontrate nell'ambito dell'offerta. La promozione della formazione avviene in stretto coordinamento con la promozione della formazione nel settore dei cyber-rischi e si basa sui risultati della misura 7.

Stato attuale
Questa misura è stata conclusa nel 2016.

La misura 8 ha potuto essere conclusa nel 2016 come previsto. Il comitato direttivo interdipartimentale «Ricerca e formazione nel settore dei cyber-rischi» ha approvato un documento programmatico che illustra le modalità per promuovere la formazione nel settore dei cyber-rischi.

Il risultato più importante della misura è rappresentato dall'istituzione di un nuovo diploma federale di «Esperto in sicurezza delle TIC» a opera dell'associazione ICT-Formazione professionale Svizzera. Grazie al sostegno della SNPC, l'associazione è riuscita a creare un'ampia base di sponsor provenienti dall'economia privata e a sviluppare insieme a questi partner il profilo di qualificazione per il diploma. I lavori sono stati conclusi, tant'è che i primi esami potranno già avere luogo nell'autunno 2018.

2.4.4 Misura 9: Internet governance

Responsabilità: DATEC-UFCOM; DFAE-DP, DDPS-POLSIC, DFF-MELANI, autorità specializzate

Con la misura 9 della SNPC la Svizzera (l'economia, la società, le autorità) deve impegnarsi attivamente e nel modo più coordinato possibile per una Internet governance, che sia conciliabile con gli ideali svizzeri di libertà e (auto)responsabilità, approvvigionamento di base, pari opportunità, diritti umani e stato di diritto. L'Ufficio federale delle comunicazioni (UFCOM), in qualità di Ufficio responsabile, prende parte attivamente ai pertinenti lavori internazionali e

regionali, ad esempio nel quadro della ICANN (Internet Cooperation for Assigned Names and Numbers), del VMSI, della Commissione dell'ONU per la scienza e la tecnologia al servizio dello sviluppo (CSTD), dell'IGF (UN Internet Governance Forum) e del Consiglio d'Europa.

Stato attuale
Questa misura è stata conclusa nel 2016.

Come ultima tappa, durante l'anno in rassegna è stata condotta un'analisi dell'efficacia della misura in cui si giunge alla conclusione che, con l'attuazione della misura 9, l'impegno della Svizzera nel settore della Internet governance può considerarsi conforme agli obiettivi sostanziali, oltre che risultare nell'insieme più coordinato. Tutto ciò grazie all'ulteriore istituzionalizzazione e strutturazione della collaborazione nell'ambito dell'Amministrazione federale e con i vari gruppi d'interesse, ma anche in virtù di un maggiore sfruttamento delle sinergie. La collaborazione dovrà essere ampliata ulteriormente anche in futuro affinché la Svizzera possa rendersi protagonista attiva e coordinata delle sempre nuove sfide nel settore della Internet governance.

2.4.5 Misura 10: Cooperazione internazionale in materia di sicurezza cibernetica

Responsabilità: DFAE-DP; DDPS-POLSIC, DFF-MELANI, DATEC-UFCOM

La misura 10 comprende la salvaguardia degli interessi a livello della politica di sicurezza nel settore cibernetico nei confronti dell'estero. Avvalendosi di iniziative e delle sue relazioni internazionali, la Svizzera si impegna affinché lo spazio cibernetico non sia utilizzato in modo abusivo con finalità criminali, di spionaggio, terroristiche e politiche.

Stato attuale
Questa misura è stata conclusa nel 2016.

Nel 2016, la Svizzera, nell'ambito della politica estera e di sicurezza, ha continuato a impegnarsi per un cyber-spazio aperto, libero e sicuro che possa contare su regole di utilizzo chiare. Gli sforzi del nostro Paese si sono concentrati in particolare sull'attività all'interno dello «UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE)», l'unico organo dell'ONU che si occupa dell'elaborazione di norme globali per la condotta degli Stati, dell'applicabilità del diritto internazionale, della creazione di fiducia e dello sviluppo di capacità nel cyber-spazio. Per la prima volta, la Svizzera è stata scelta per farvi parte per il periodo 2016–2017. Le sue priorità sono il consolidamento e la concretizzazione dei lavori programmatici già svolti dal Gruppo così come il coinvolgimento nel processo dei non membri dello UN GGE e degli attori non statali.

La Svizzera ha continuato a partecipare attivamente anche al processo dell'OSCE inteso a creare fiducia nel settore cibernetico. Questo processo punta, attraverso misure mirate, ad accrescere la fiducia fra Stati in virtù della trasparenza, della cooperazione e della stabilità. La fiducia fra Stati deve contribuire a ridurre il rischio di errori di valutazione ed equivoci. In questo contesto, la Svizzera ha promosso l'attuazione delle misure già decise e, in parallelo, sostenuto lo sviluppo di ulteriori provvedimenti intesi a creare fiducia. Considerata la natura globale dei cyber-rischi, la Svizzera si è altresì impegnata a favore dell'universalizzazione del processo dell'OSCE.

La Svizzera si è inoltre adoperata per creare capacità specifiche correlate alla cibernetica. Ha infatti sostenuto progetti del «Global Forum on Cyber Expertise (GFCE)» (ad es. l'iniziativa Meridian finalizzata alla protezione delle infrastrutture informatiche critiche) e, nell'ottica di un ulteriore sviluppo delle proprie capacità, ha proseguito la collaborazione con il «Cooperative Cyber Defence Centre of Excellence (CCDCoE)» di Tallin (Estonia).

Anche quest'anno la Svizzera ha partecipato attivamente al dialogo tra gli Stati europei e la

Cina volto a comprendere meglio la rispettiva percezione delle minacce e a identificare le questioni da approfondire nel reciproco interesse.

Infine, la Svizzera ha condotto con Paesi selezionati consultazioni bilaterali specifiche alla cyber-problematica.

2.4.6 Misura 11: Iniziative internazionali e processi di standardizzazione nel settore della sicurezza

Responsabilità: DATEC-UFCOM; SC SNPC, autorità specializzate, DFAE-DP, DFF-ME-LANI

L'obiettivo della misura 11 consiste nel coordinamento e nella cooperazione degli esperti in cyber-sicurezza in Svizzera per ottimizzare l'impegno internazionale in seno agli organismi di normazione e altre opportune iniziative.

Stato attuale
Questa misura è stata conclusa nel 2016.

Nel 2016, nel quadro della misura 11, è stato organizzato un workshop con gli attori coinvolti finalizzato allo scambio di informazioni e condotto un sondaggio per l'analisi dell'efficacia. I risultati del sondaggio verranno analizzati verso la fine del 2016 e all'inizio di dicembre seguirà il trattamento dei feedback degli attori. Per la fine dell'anno, con la consegna del rapporto sull'analisi dell'efficacia al SC SNPC, tutte le tappe e gli oggetti della fornitura indicati saranno presumibilmente raggiunti secondo il piano.

La misura si considera conclusa ai sensi della pianificazione del progetto della SNPC. Le attività e i risultati definiti verranno proseguiti nel corso del 2017.

2.4.7 Misura 16: Necessità di modificare le basi legali

Responsabilità: SC SNPC

La misura 16 prevede di verificare se il diritto applicabile contiene le basi necessarie alla protezione contro i cyber-rischi, eventualmente apportando le necessarie modifiche. Le unità amministrative devono individuare le rilevanti basi giuridiche per il loro ambito di attività e valutare la necessità di revisione e di integrazione.

Stato attuale
Questa misura è stata conclusa nel 2014.

I primi chiarimenti sulle basi legali sono stati effettuati nel 2014. Sulla scorta dei recenti sviluppi non si ravvisa la necessità generalizzata di una regolamentazione. Tale necessità è oggetto di continue valutazioni.

2.5 Attività di attuazione nell'esercito

L'esercito rientra tra le infrastrutture critiche del Paese per le quali il cyber-spazio e le minacce in questo ambito sono diventati una sfida di capitale importanza. Con il rapidissimo sviluppo e la crescente importanza del cyber-spazio si presentano nuove opzioni operative in ambito militare da considerare. Tra i principali compiti immediati dell'esercito si annovera tuttavia la protezione dei suoi sistemi e delle sue infrastrutture TIC in ogni situazione, per garantire la loro capacità d'intervento e la libertà d'azione.

L'esercito dispone di notevoli competenze e capacità, di cui se necessario i responsabili Uffici federali possono avvalersi in via sussidiaria, a condizione che non occorrano contemporaneamente all'esercito stesso.

A questo scopo l'esercito sviluppa costantemente le proprie conoscenze e competenze. I suoi compiti nel settore sussidiario e i suoi compiti in caso di guerra o di conflitto vengono al momento precisati. Nel settore del personale non è stato possibile reperire le risorse pianificate nel 2015; questo ritardo dovrebbe essere colmato nel 2016.

Stato attuale

Nel 2016, l'esercito ha proseguito l'attuazione del proprio concetto di cyber-difesa e apportato svariate migliorie a livello organizzativo. Il costante aumento delle cyber-minacce e dei cyber-eventi, il sì del popolo alla LAIn, l'approvazione della legge militare (LM, RS *510.10*) da parte del Parlamento e le conseguenze dell'attacco degli hacker ai danni della RUAG sono alcuni degli eventi principali per cui è stato interpellato e tenuto impegnato l'esercito nel settore della cyber-difesa.

Nell'ambito del DDPS è stato disposto l'allestimento di un Piano d'azione per la cyber-difesa DDPS (PACD). Il piano in linea con gli obiettivi del 2016 si conforma alla Strategia nazionale per la protezione della Svizzera contro i cyber-rischi (SNPC), risponde concretamente alle sue aspettative e non ne ostacola lo sviluppo.

Il piano persegue tre obiettivi:

- rafforzare il DDPS, in particolare l'esercito, al fine di gestire le crescenti cyber-minacce nella quotidianità così come nelle situazioni di crisi e di conflitto;
- sostenere concretamente, nel settore cyber, l'attuazione della LAIn e delle disposizioni della LM che a partire dal 2018 consentiranno all'esercito, in determinate circostanze, di difendersi attivamente contro i cyber-attacchi;
- creare condizioni favorevoli che (ai sensi della LAIn) consentano al DDPS di sostenere i gestori di infrastrutture critiche colpiti da attacchi degli hacker.

Il solo fatto di aver elaborato questo piano d'azione ha portato a un'ottimizzazione dei mezzi esistenti; inoltre, tutto ciò è stato propedeutico all'introduzione di una governance nel DDPS. L'implementazione vera e propria del piano d'azione, tuttavia, richiederà una significativa ridistribuzione delle risorse all'interno del DDPS. Il risultato finale auspicato dovrebbe essere raggiunto nel 2020.

Il grado di maturità e la prontezza dell'esercito, tuttavia, migliorano anche attraverso l'istruzione e la sensibilizzazione del personale di milizia e di professione. L'esercito ha così preso parte a diverse esercitazioni nel corso del 2016, segnatamente all'esercitazione internazionale LOCKED SHIELD 16 e all'esercitazione della Rete integrata Svizzera per la sicurezza (RSS), che aveva come tema un cyber-attacco al sistema previdenziale svizzero con ripercussioni sui numeri AVS. Il servizio Cyber Defence dell'esercito ha organizzato l'esercitazione CYBER PAKT 16, nell'ambito della quale sono stati simulati vari scenari di notevole intensità e complessità. In questo modo si sono potute verificare le procedure sviluppate in seno al PACD, migliorare la comprensione delle nuove basi legali e regolamentare i principi di sussidiarietà dell'esercito. Oltre a queste esercitazioni, nel 2016 si sono tenute anche numerose iniziative di sensibilizzazione che hanno coinvolto il personale del DDPS e la truppa (ad es. con l'impiego di sicurezza dell'esercito al Forum economico mondiale), ma anche la popolazione nell'ambito di manifestazioni pubbliche dell'esercito a Meiringen e Thun.

2.6 Attività di attuazione nei Cantoni

La Rete integrata Svizzera per la sicurezza (RSS) è l'interfaccia della SNPC con i Cantoni. Il Gruppo specializzato Cyber (GS-C) dell'RSS garantisce il coordinamento tra Confederazione e Cantoni nell'attuazione della SNPC in collaborazione con i Cantoni, i Comuni e i servizi federali interessati. Il servizio di coordinamento SNPC è membro del GS-C e a livello di Confederazione funge da ponte con i lavori di progetto che coinvolgono i Cantoni. Per l'attuazione cantonale della SNPC sono stati istituiti quattro gruppi di lavoro, diretti dal Gruppo specializzato Cyber.

Stato attuale

L'indagine sullo status quo cantonale dei cyber-rischi ha costituito la base per la messa a punto di uno strumento ausiliario che consente di individuare i processi rilevanti a livello cantonale. L'idoneità di questo strumento, che segna un importante passo avanti verso una migliore gestione dei rischi nel settore cyber, è attualmente oggetto di test da parte di tre Cantoni prima che venga reso generalmente disponibile in ambito cantonale.

Le descrizioni dei processi per trattare i cyber-eventi, allestite dal gruppo di lavoro «Incident Management», sono state in parte adattate o migliorate.

Con l'ausilio di «POPULA», l'esercitazione quadro di stato maggiore della durata di due giorni tenutasi nel novembre 2016, si doveva verificare il documento programmatico per procedure e processi cibernetici a livello di Confederazione in situazioni di crisi e con l'estensione ai Cantoni e alle infrastrutture critiche. L'esercitazione ha visto la partecipazione di Confederazione, Cantoni, infrastrutture critiche e terzi interessati dallo scenario «Cyber-attacco al sistema previdenziale». In particolare erano presenti una cinquantina di rappresentanti di varie organizzazioni che nel quotidiano non hanno generalmente contatti fra loro (o solo in rare occasioni). L'esercitazione è stata introdotta da una dimostrazione dal vivo a cura della RUAG (gruppo industriale che annovera diverse divisioni, di cui una dedicata agli armamenti) che ha effettuato la simulazione tecnica di un cyber-attacco. L'obiettivo dell'esercitazione era quello di verificare le interfacce tra le varie organizzazioni interessate dallo scenario. I partecipanti hanno così dovuto cercare i propri partner, condividere le informazioni e dare disposizioni per l'aggravamento del caso (escalation). L'esercitazione ha fornito elementi importanti per il documento programmatico e la gestione nazionale delle crisi in situazioni con aspetti cibernetici. Tuttavia, per via della modalità con cui si è sviluppata, non è stato possibile verificare tutte le parti del documento programmatico.

Nell'ambito del gruppo di lavoro sulla cyber-criminalità è stata presa la decisione di distribuire ad ampio spettro presso le autorità di perseguimento penale le schede informative allestite dal SCOCI con la collaborazione dei Cantoni. Queste ultime contengono la descrizione dei fenomeni principali nel settore della cyber-criminalità e, in tal modo, potranno essere utilizzate dalle autorità competenti nell'espletamento del loro lavoro quotidiano.

3 Comitato direttivo e controlling strategico

Il Consiglio federale ha incaricato il comitato direttivo SNPC (CD SNPC) di seguire l'attuazione con un controlling strategico allo scopo di verificare a intervalli semestrali lo stato di avanzamento in termini di obiettivi e di tempistica delle misure della «Strategia nazionale per la protezione della Svizzera contro i cyber-rischi (SNPC)». Secondo la decisione del Consiglio federale del 15 maggio 2013 relativa al piano di attuazione della SNPC, l'affare dovrà essere sottoposto al Consiglio federale tramite la Conferenza dei segretari generali (CSG). Il controlling al 31.12.2016 evidenzia come 15 delle 16 misure della SNPC siano già state concluse e l'ultima misura in corso nell'ambito della gestione della continuità operativa potrà essere realizzata come previsto entro la fine del 2017.

Nel corso dell'anno in rassegna, il comitato direttivo SNPC si è occupato assiduamente dell'ulteriore sviluppo della SNPC a partire dal 2018. In particolare ha discusso l'ulteriore modo di procedere con una cerchia allargata di partecipanti in occasione di una riunione straordinaria il 30 giugno 2016, della settima seduta ordinaria del CD SNPC il 17 agosto 2016 e di un workshop il 26 ottobre 2016. Alla luce dei risultati della verifica dell'efficacia, il CD SNPC e la cerchia allargata di partecipanti si sono trovati concordi nell'affermare che la SNPC ha prodotto un considerevole effetto, che l'approccio decentralizzato e basato sui rischi è corretto e che la SNPC deve essere proseguita.

4 Verifica dell'efficacia

Nella decisione relativa al piano di attuazione della SNPC, il Consiglio federale ha conferito all'ODIC l'incarico di presentare una verifica dell'efficacia della SNPC nel mese di aprile del 2017. Per adempiere al mandato entro il termine, la verifica è avvenuta già nel corso del 2016. Tra marzo e luglio, un'azienda esterna ha condotto un totale di 14 interviste e 15 consultazioni scritte e analizzato complessivamente 130 documenti che erano stati redatti nell'ambito della SNPC.

La SNPC è stata valutata a tre livelli: il successo nell'attuazione delle 16 misure, gli aspetti trasversali alle misure (pianificazione delle risorse, contenuti, struttura organizzativa e comunicazione) e le interfacce con le attività dei Cantoni e dell'esercito. La verifica ha prodotto i risultati seguenti.

- **Misure:** l'attuazione delle 16 misure della SNPC ha avuto complessivamente successo e gli obiettivi indicati sono stati in gran parte raggiunti. Ciò, come dimostrato, ha portato a un rafforzamento delle capacità, alla creazione di conoscenze specialistiche e al miglioramento del coordinamento. Dimostrare un effetto causale immediato delle misure sugli obiettivi strategici risulta difficoltoso per via della fase precoce in cui è avvenuta la verifica. Con l'ausilio di modelli d'efficacia, tuttavia, si possono delineare in modo plausibile gli effetti previsti. Per quattro misure non sono stati centrati tutti gli obiettivi fissati. In questi casi viene certificata la necessità di ulteriori interventi.
- **Contenuti, risorse, struttura organizzativa e comunicazione:** al livello superiore, la verifica dell'efficacia attesta come gli obiettivi strategici formulati dal Consiglio federale nel 2012 abbiano dato sostanzialmente buoni risultati. Le risorse per l'attuazione delle misure sono state, seppur di stretta misura, sufficienti e la struttura organizzativa decentralizzata ha funzionato bene nel complesso. Qualche carenza viene segnalata per la comunicazione verso l'esterno a livello nazionale. Insufficiente è infatti la percezione della SNPC nell'opinione pubblica e non si sa abbastanza delle iniziative intraprese dalla Confederazione nel settore dei cyber-rischi e dei limiti che essa ravvisa nella propria competenza.
- **Interfacce con le attività dei Cantoni e dell'esercito:** le attività della SNPC vengono coordinate con quelle dei Cantoni attraverso la Rete integrata Svizzera per la sicurezza (RSS). La verifica ha dimostrato come la collaborazione funzioni bene e a livello cantonale sia subentrata una certa sensibilizzazione. Viceversa, rimangono ancora aperte questioni importanti all'interfaccia con le attività dell'esercito. La delimitazione tra i compiti civili della SNPC e le competenze dell'esercito in situazioni di crisi non è stata chiarita in modo esaustivo e devono essere altresì precisate le aspettative e le possibilità dell'esercito in relazione al sostegno sussidiario.

I risultati della verifica dell'efficacia evidenziano come la scelta dell'orientamento strategico si sia rivelata corretta e l'attuazione decentralizzata ma strettamente coordinata della SNPC funzioni bene nel complesso. In tutti i settori è riuscita l'implementazione di strutture e processi efficienti come pure la creazione delle conoscenze specialistiche necessarie, cosicché oggi la Svizzera appare più preparata ad affrontare i cyber-rischi rispetto al 2012. Al tempo stesso emerge chiaramente come con la SNPC siano state poste solo le basi e occorra pertanto procedere all'ulteriore sviluppo della protezione contro i cyber-rischi.

5 Attività

In questo capitolo vengono presentate alcune importanti attività e manifestazioni svoltesi a livello nazionale e internazionale nel 2016.

5.1 Livello nazionale

Il 6 aprile 2016 si è tenuta la quarta «Cyber-Landsgemeinde». Anche quest'anno, circa 100 cyber-responsabili della Confederazione e dei Cantoni nonché alcuni partner della Rete integrata Svizzera per la sicurezza (RSS) hanno preso parte a questa manifestazione di networking. Come negli anni passati, l'evento era dedicato allo stato di avanzamento dei progetti realizzati a livello cantonale e nel quadro della SNPC nonché alla verifica della sua efficacia.

Dal 7 all'8 aprile 2016 si è svolta a Ginevra la «Cyber 9/12 Student Challenge». Come lo scorso anno, l'Atlantic Council e il Geneva Centre for Security Policy (GCSP) hanno ospitato la manifestazione. Anche in questa edizione, 28 squadre provenienti da 13 Paesi europei e dalla Svizzera, dal Medio Oriente e dagli Stati Uniti si sono incontrate per prepararsi ad affrontare un grande cyber-attacco e a elaborare raccomandazioni operative adeguate. Questa volta, il concorso è stato vinto da un team britannico. Il sostegno da parte della Confederazione è giunto attraverso la partecipazione del SC SNPC e di ulteriori rappresentanti in qualità di giurati.

Il 20 maggio 2016 si è tenuta a Losanna presso il Politecnico federale di Losanna (EPFL) la prima «Swiss Cyber Risk Research Conference», organizzata dalla Segreteria di Stato per la formazione, la ricerca e l'innovazione (SEFRI). La conferenza aveva lo scopo di dare slancio alla ricerca sul tema dei cyber-rischi e di rafforzare la rete di ricercatori in Svizzera.

Il 18 settembre 2016 si è svolta a Lucerna la terza edizione della «European Cyber Security Challenge». Nell'ambito di questa competizione internazionale allievi e studenti provenienti da Austria, Germania, Romania, Gran Bretagna, Spagna e Svizzera si sono cimentati nell'identificazione, nello sfruttamento e nell'eliminazione delle vulnerabilità dei sistemi d'informazione e di comunicazione (sistemi TIC). La manifestazione è stata organizzata dall'associazione Swiss Cyber Storm, dal Dipartimento federale degli affari esteri (DFAE) e dal Dipartimento federale delle finanze (DFF). Vincitrice di quest'anno è stata la Spagna.

Il 26 ottobre si è tenuta la terza conferenza SNPC, ma in un formato diverso rispetto agli anni precedenti. Il programma del mattino prevedeva un workshop interno per individuare l'ulteriore modo di procedere a partire dal 1° gennaio 2018. Lo scopo era quello di stabilire con i responsabili delle varie misure della SNPC gli interventi necessari in vista di una possibile strategia successiva. Nel pomeriggio è poi seguita la parte ufficiale della conferenza SNPC con l'obiettivo di offrire ai rappresentanti dell'economia e della politica una panoramica dettagliata sullo stato di attuazione aggiornato delle misure della SNPC e di presentare i primi risultati della verifica dell'efficacia.

Dal 23 al 24 novembre 2016 si è svolta l'esercitazione di gestione delle crisi «Popula» che ha simulato un cyber-attacco al sistema previdenziale svizzero. Organizzata sotto la responsabilità della RSS in collaborazione con la Confederazione, i Cantoni e le infrastrutture critiche, aveva l'obiettivo di mettere alla prova la prontezza e la gestione delle crisi a livello federale e cantonale.

5.2 Livello internazionale

Dal 14 al 18 marzo 2016 si è tenuto a Hannover il «CeBIT», la fiera annuale dedicata all'informatica di cui la Svizzera è stata il Paese partner. Questa edizione era incentrata sui temi seguenti: processi in azienda e interconnettività nella vita quotidiana, Internet delle cose e industria 4.0.

Il 10-11 maggio e il 14-15 novembre 2016, la Svizzera ha preso nuovamente parte al «Sino-European Cyber Dialogue», un dialogo multilaterale tra Stati europei e Cina finalizzato a comprendere meglio la rispettiva percezione delle minacce e a identificare le questioni da approfondire nel reciproco interesse. Il contributo apportato dal nostro Paese alla quinta e alla sesta edizione della manifestazione si è rivelato decisivo.

Dall'8 al 10 giugno 2016 si è svolto a Bruxelles il «Dialogo europeo sulla governance di Internet (EuroDIG)». La manifestazione prende esempio dall'Internet Governance Forum delle Nazioni Unite ed è all'avanguardia in quanto a formati di discussione innovativi e quando si tratta di coinvolgere i vari gruppi d'interesse nel dibattito sui temi correlati a Internet. L'Ufficio federale delle comunicazioni (UFCOM) fa parte dei membri fondatori dell'EuroDIG e, anche quest'anno, la Svizzera ha saputo fare attivamente la propria parte nelle discussioni sul campo.

Dal 29 agosto al 2 settembre e dal 28 novembre al 2 dicembre 2016 si è riunito, rispettivamente a New York e a Ginevra, lo «UN Group of Governmental Experts» sulla cyber-sicurezza. La Svizzera, che nel 2016 è entrata a far parte di questo gruppo per un anno, sviluppa raccomandazioni per l'utilizzo del cyber-spazio in relazione a cinque aree tematiche: situazione di minaccia, norme per la condotta degli Stati, diritto internazionale, creazione della fiducia e sviluppo delle capacità.

Il 18 settembre 2016, alla vigilia dell'Assemblea generale delle Nazioni Unite, si è riunita a New York per il suo incontro annuale la «Broadband Commission for Sustainable Development (BBCOM)», co-presieduta da ITU e UNESCO. La BBCOM e i suoi gruppi di lavoro si impegnano in particolar modo per estendere l'accesso alla banda larga.

Dal 28 al 30 settembre 2016 si è tenuta a Nuova Delhi la conferenza indiana «CyFy», dove la Svizzera era rappresentata in qualità di Stato partner. Si tratta della maggiore conferenza asiatica in materia di cyber-sicurezza e Internet governance alla quale prendono parte, oltre ai governi, anche esponenti dell'economia privata e della ricerca.

Il 30 settembre 2016 si è concluso il ruolo di vigilanza degli Stati Uniti sulla «Internet Corporation for Assigned Names and Numbers (ICANN)», l'ente di gestione degli indirizzi Internet. Da allora, la gestione degli indirizzi Internet a livello mondiale è affidata alla comunità globale ove sono rappresentati tutti i gruppi d'interesse. Questo passaggio ha segnato un passo importante verso l'obiettivo perseguito dalla Svizzera di una gestione internazionale del sistema di nomi di dominio (DNS).

Il 4 novembre 2016 si è svolto a Vienna l'«OSCE Cyber Showcase Event», presieduto dalla Germania. L'evento era incentrato sul tema dell'attribuzione, ossia l'identificazione degli autori. Gli Stati partecipanti si sono trovati d'accordo sul fatto che l'attribuzione dei cyber-eventi rappresenti una sfida e debbano essere pertanto messe a punto soluzioni comuni. L'OSCE ha saputo offrire un contesto adeguato per discussioni approfondite su questo tema.

Dal 3 al 9 novembre 2016 si è tenuto a Hyderabad (India) il convegno dell'«ICANN57». Dopo Marrakech (5-10 marzo) e Helsinki (27-30 giugno) si è trattato del terzo incontro dell'ICANN durante l'anno in rassegna. Dopo il trasferimento del ruolo di vigilanza degli Stati Uniti alla comunità globale, occorrerà implementare i dettagli e portare avanti le riforme nell'ambito dell'ICANN. La Svizzera è stata eletta per acclamazione per altri due anni alla presidenza del Comitato consultivo governativo dell'ICANN.

Dal 16 al 18 novembre 2016, il governo cinese ha organizzato a Wuzhen, piccola città nei pressi di Shanghai, la terza «World Internet Conference (WIC)». La WIC è la risposta cinese all'«Internet Governance Forum (IGF)» e funge innanzitutto da portavoce del Partito comunista. Con queste iniziative e gli investimenti connessi, la Cina vuole avallare la propria ambizione di rivestire un ruolo sempre più rilevante nell'ambito delle discussioni sulla Internet governance. Il presidente Xi Jinping ha conferito grande priorità a questo tema nell'agenda politica del Paese e la Cina non baderà dunque a spese pur di essere all'altezza della situazione.

Dal 6 al 9 dicembre 2016 si è svolto a Guadalajara (Messico) il primo Internet Governance Forum (IGF) delle Nazioni Unite dopo la proroga del mandato da parte degli Stati membri dell'ONU avvenuta nel dicembre 2015. L'IGF è uno dei maggiori appuntamenti annuali nel settore della Internet governance e offre a tutti i gruppi d'interesse una piattaforma di discussione per scambiare opinioni sul tema di Internet. In Messico, la Svizzera ha annunciato di volersi candidare a ospitare l'IGF 2017 presso la sede dell'ONU a Ginevra.

Nell'agosto 2016, la Commissione europea ha approvato la direttiva comunitaria per la sicurezza delle reti e dell'informazione (direttiva NIS), la quale ha carattere vincolante per gli Stati membri dell'UE. Il nostro Paese dovrà monitorare gli ulteriori sviluppi della direttiva, poiché l'obbligo di notifica potrebbe avere ripercussioni anche per la Svizzera e le imprese elvetiche che operano nell'UE. Il servizio di coordinamento SNPC è membro del gruppo di esperti Cyber dell'ENISA e partecipa regolarmente alle sue attività e conferenze.

6 Considerazioni finali

L'attuazione della SNPC volge ormai al termine. Delle 16 misure in programma, alla fine del 2016 ne sono state concluse 15 e una misura verrà realizzata come previsto entro la fine del 2017. Sono altresì disponibili i primi risultati della verifica dell'efficacia che evidenziano come con la SNPC si sia prodotto un considerevole effetto, gli obiettivi strategici del Consiglio federale abbiano dato buoni risultati e la Svizzera appaia più preparata ad affrontare i cyber-rischi rispetto al 2012. Attraverso la SNPC sono stati estesi e sviluppati ulteriormente i processi e le strutture esistenti, definendone anche di nuovi, allo scopo di rafforzare la collaborazione, la cooperazione e la comunicazione tra i principali attori coinvolgendone altri in futuro se ve ne sarà l'esigenza.

L'aumento del numero di cyber-attacchi registrato nel 2016 ha sottolineato ancora una volta la necessità di tenere sempre alta la guardia e di approfondire ulteriormente la fruttuosa cooperazione instaurata con i partner nazionali e internazionali. Per accrescere la resilienza della Svizzera, anche in futuro occorrerà intensificare la preziosa collaborazione con i gestori di infrastrutture critiche, l'economia e i Cantoni e rafforzare ancora assiduamente lo scambio di informazioni con le organizzazioni di polizia e i pubblici ministeri nonché i fornitori di prestazioni TIC, i fornitori di sistemi, le autorità specializzate e gli organi di regolamentazione.

L'attività della Svizzera è stata ancora una volta rilevante anche sul piano internazionale. La Svizzera si è impegnata per la creazione di una normativa volta a disciplinare l'utilizzo e i confini del cyber-spazio con l'ausilio di strumenti politici e giuridici e a promuovere la propria visione di un cyber-spazio aperto, libero e sicuro.

Il futuro porterà nuove sfide. Nel corso degli ultimi anni, le minacce si sono sensibilmente acuite e hanno presentato un comportamento molto mutevole. Anche nel 2016 è apparso evidente come le minacce di oggi non corrispondono a quelle di domani. Per questo la Svizzera deve prepararsi al meglio per affrontare le cyber-minacce del futuro. I responsabili delle misure e gli attori a livello federale e cantonale sono concordi nell'affermare che i risultati della SNPC debbano essere garantiti anche oltre l'orizzonte temporale del 2017. Il comitato direttivo SNPC elaborerà pertanto un'analisi approfondita sull'ulteriore sviluppo della strategia da sottoporre al Consiglio federale.

7 Allegati

7.1 Documenti di base sulla SNPC

«Strategia nazionale per la protezione della Svizzera contro i cyber-rischi (SNPC)»:
https://www.isb.admin.ch/isb/it/home/themen/cyber_risiken_ncs/ncs_strategie.html

«Piano di attuazione della Strategia nazionale per la protezione della Svizzera contro i cyber-rischi (PA SNPC)»:
https://www.isb.admin.ch/isb/it/home/themen/cyber_risiken_ncs/umsetzungsplan.html

«Rapporto annuale SNPC 2013» (disponibile in tedesco e in francese):
http://www.isb.admin.ch/themen/01709/01891/index.html?lang=de

«Rapporto annuale SNPC 2014»:
https://www.isb.admin.ch/isb/it/home/themen/cyber_risiken_ncs/jahresberichte_ncs.html

7.2 Riepilogo degli interventi parlamentari concernenti i cyber-rischi

Intervento Ip. = interpellanza; Mo. = mozione; Po. = postulato; I = interrogazione	Depositato il:	Stato al 31.12.2015:
08.3050 Po. Schmid-Federer «Protezione dal bullismo elettronico»	11.03.2008	Liquidato
08.3100 Mo. Burkhalter «Strategia nazionale per combattere la criminalità su Internet»; con deliberazioni del Consiglio degli Stati del 2.06.2008 (BU CS 2.06.2008), rapporto della CPS-CN dell'11.11.2008 nonché deliberazioni del Consiglio nazionale del 3.06.2009 (BU CN 3.06.2009)	18.03.2008	Liquidato
08.3101 Po. Frick «Proteggere meglio la Svizzera dalla criminalità informatica»	18.03.2008	Liquidato
08.3924 Ip. Graber «Misure contro la guerra elettronica»	18.12.2008	Liquidato
09.3114 Ip. Schlüer «Sicurezza in Internet»	17.03.2009	Liquidato
09.3266 Mo. Büchler «Sicurezza della piazza economica Svizzera»	20.03.2009	Liquidato
09.3628 Po. Fehr HJ «Rapporto "Internet in Svizzera"»	12.06.2009	Liquidato
09.3630 Ip. Fehr HJ «Domande su Internet»	12.06.2009	Liquidato
09.3642 Mo. Fehr HJ «Osservatorio di Internet»	12.06.2009	Liquidato
10.3136 Po. Recordon «Valutazione della minaccia in materia di cyberguerra»	16.03.2010	Liquidato
10.3541 Mo. Büchler «Protezione contro gli attacchi cibernetici»	18.06.2010	Liquidato
10.3625 Mo. CPS-CN «Misure contro gli attacchi informatici»; con deliberazioni del Consiglio nazionale del 2.12.2010 (BU CN 2.12.2010), rapporto della CPS-CS dell'11.1.2011 nonché	29.06.2010	Liquidato

deliberazioni del Consiglio degli Stati del 15.3.2011 (BU CS 15.03.2011)		
10.3872 Ip. Recordon «Rischio di un black out di ampie dimensioni della rete elettrica svizzera»	01.10.2010	Liquidato
10.3910 Po. Gruppo liberale radicale «Centro di condotta e di coordinamento nell'ambito delle cyberminacce»	02.12.2010	Liquidato
10.4020 Mo. Glanzmann «MELANI per tutti»	16.12.2010	Liquidato
10.4028 Ip. Malama «Rischio di attacco di virus nelle centrali nucleari svizzere»	16.12.2010	Liquidato
10.4038 Po. Büchler «Capitolo sulla guerra cibernetica nel rapporto sulla politica di sicurezza»	16.12.2010	Liquidato
10.4102 Po. Darbellay «Concetto per la protezione delle infrastrutture digitali della Svizzera»	17.12.2010	Liquidato
11.3906 Po. Schmid-Federer «Legge quadro sulle TIC»	29.09.2011	Liquidato
12.3417 Mo. Hodgers «Mercati delle telecomunicazioni aperti. Strategie per la sicurezza digitale nazionale»	30.05.2012	Liquidato
12.4161 Mo. Schmid-Federer «Strategia nazionale contro il bullismo e il mobbing elettronici»	13.12.2012	Liquidato
13.3228 Ip. Recordon «Sistema federale di intercettazioni telefoniche e lacune generali della Confederazione in materia di informatica e telecomunicazioni»	22.03.2013	Liquidato
13.3229 Ip. Recordon «Portata della minaccia e misure di lotta contro la guerra e la criminalità cibernetiche»	22.03.2013	Liquidato
13.5224 Dom. Reimann «Zur Präsenz von US-Geheimdiensten und ihren Cyber-Schnüffelaktivitäten in der Schweiz»	10.06.2013	Liquidato
13.3558 Ip. Eichenberger «Spionaggio informatico. Valutazione e strategia»	20.06.2013	Liquidato
13.3677 Ip. Gruppo socialista «Atti di spionaggio della NSA e di altri servizi informazioni anche in Svizzera?»	11.09.2013	Liquidato
13.5325 Dom. Sommaruga «Verwendet der Nachrichtendienst des Bundes illegal von der NSA beschaffte Daten?»	11.09.2013	Liquidato
13.3692 Ip. Hurter «Mercato delle telecomunicazioni. Sono ancora attuali la legislazione e le misure di regolamentazione in vigore?»	12.09.2013	Non ancora trattato nel plenum
13.3696 Mo. Müller-Altermatt «Protezione dei dati anziché scudo protettivo per coloro che non pagano le imposte»	12.09.2013	Non ancora trattato nel plenum
13.3707 Po. Gruppo BD «Strategia globale per il ciberspazio al passo con i tempi»	17.09.2013	Non ancora trattato nel plenum
13.3773 Ip. Gruppo liberale radicale «Legge sulle comunicazioni al passo con i tempi. Una strategia globale per il ciberspazio»	24.09.2013	Non ancora trattato nel plenum
13.3841 Mo. Rechsteiner «Commissione di esperti per il futuro del trattamento e della sicurezza dei dati»	26.09.2013	Adottato
13.3927 Ip. Reimann «Protezione dei bunker svizzeri per l'archiviazione dei dati»	27.09.2013	Non ancora trattato nel plenum

13.4009 Mo. CPS-CN «Attuazione della Strategia nazionale per la protezione della Svizzera contro i cyber-rischi» («Il Consiglio federale è incaricato di accelerare l'attuazione della Strategia nazionale per la protezione della Svizzera contro i cyber-rischi e di attuare le 16 misure concrete entro la fine del 2016.»)	05.11.2013	Liquidato
13.4077 Ip. Clottu «Spionaggio di dati e sicurezza su Internet»	05.12.2013	Liquidato
13.4086 Mo. Glättli «Programma nazionale di ricerca "Protezione idonea dei dati nella società dell'informazione"»	05.12.2013	Liquidato
13.4308 Po. Graf-Litscher «Migliorare la sicurezza e l'indipendenza del settore informatico svizzero»	13.12.2013	Non ancora trattato nel plenum
14.3654 Ip. Derder «Sicurezza digitale. Abbiamo preso la direzione sbagliata?»	20.06.2014	Non ancora trattato nel plenum
14.5569 Dom. Leutenegger «NSA. Ein Jahr Schnüffelstaat»	26.11.2014	Liquidato
14.4138 Ip. Noser «Prassi in materia di acquisti pubblici nel settore delle infrastrutture TIC critiche dell'Amministrazione federale»	10.12.2014	Non ancora trattato nel plenum
14.1105 I Buttet «Mezzi a favore della „cyber defense" nel quadro della politica di sicurezza della Svizzera»	10.12.2014	Depositato
14.4299 Ip. Derder «Vigilanza trasversale sulla rivoluzione digitale. È necessario istituire una segreteria di Stato della società digitale?»	12.12.2014	Non ancora trattato nel plenum
15.3359 Po. Derder «Per un esercito innovativo»	20.03.2015	Non ancora trattato nel plenum
15.3375 Ip. Recordon «Sottrazione di codici SIM da parte della NSA e del GCHQ presso la società Gemalto»	20.03.2015	Liquidato
15.5299 Dom. Leutenegger «Schutz vor NSA-Spionage»	09.06.2015	Liquidato
15.3656 Ip. Munz «Pericolo per la centrale nucleare di Mühleberg a causa della manutenzione a distanza del sistema informatico. Discutibile sorveglianza da parte dell'IFSN»	18.06.2015	Non ancora trattato nel plenum
15.1059 Berberat «Aiuto finanziario urgente della Confederazione in seguito all'attacco informatico contro TV5 Monde»	10.09.2015	Liquidato
15.4073 Ip. Derder «L'esercito è realmente in grado di proteggere il cyberspazio svizzero?»	25.09.2015	Non ancora trattato nel plenum
16.3186 Mo. Eichenberger «Cyber-rischi. Scambio di informazioni tecniche»	17.03.2016	Liquidato
16.3348 Po. Béglé «Creazione di un consiglio per la cyber defence. Una priorità per la nostra sovranità e la nostra sicurezza»	27.04.2016	Non ancora trattato nel plenum
16.3353 Ip. Salzmann «Scopo della Rete integrata Svizzera per la sicurezza»	30.05.2016	Non ancora trattato nel plenum

16.3356 Ip. Nordmann «Ridistribuire finalmente le risorse finanziarie e di personale a favore della lotta per la cybersicurezza»	31.05.2016	Non ancora trattato nel plenum
16.3363 Ip. Glättli «Cyberattacchi contro RUAG e DDPS. È necessario trarre le dovute conclusioni!»	31.05.2016	Liquidato
16.3364 Ip. Glanzmann-Hunkeler «Accertamenti concernenti il cyberattacco contro la RUAG»	31.05.2016	Liquidato
16.1020 I urgente Gruppo BD «Sistema di controllo e centro di competenza come futuri strumenti nella lotta contro i cyberrischi»	02.06.2016	Liquidato
16.1021 I urgente Gruppo dei Verdi	02.06.2016	Liquidato
16.1022 I urgente Gruppo PPD «Accertamenti concernenti il cyberattacco contro la RUAG»	02.06.2016	Liquidato
16.1024 I Knecht «Interpol, rischi cibernetici e cybercriminalità»	07.06.2016	Liquidato
16.3413 Ip. Heim «Criminalità informatica e rischi per gli impianti nucleari»	09.06.2016	Liquidato
16.3528 Mo. Glanzmann-Hunkeler «Competenza per la cyberdifesa»	16.06.2016	Non ancora trattato nel plenum
16.3561 Ip. Dittli «Dichiarazione della NATO. Gli attacchi da parte di hacker possono provocare un “casus foederis”»	17.06.2016	Liquidato
16.061 «La politica di sicurezza della Svizzera» Rapporto	24.08.2016	Non ancora trattato nel plenum
16.3706 Po. Vonlanthen «Economia digitale e mercato del lavoro»	27.09.2016	Adottato
16.4073 Po. Golay «Cyber-rischi. Per una protezione globale, indipendente ed efficace»	15.12.2016	Non ancora trattato nel plenum
16.4115 Ip. Quadranti «Identità elettronica»	16.12.2016	Non ancora trattato nel plenum

7.3 Elenco delle abbreviazioni

DPS	Divisione politica di sicurezza
BAC	Base d’aiuto alla condotta
CaF	Cancelleria federale
CCPCS	Conferenza dei comandanti delle polizie cantonali della Svizzera
CD SNPC	Comitato direttivo della strategia nazionale per la protezione della Svizzera contro i cyber-rischi
CDCGP	Conferenza dei direttori cantonali di giustizia e polizia
CERT	Computer Emergency Response Team
CSG	Conferenza dei segretari generali
CSTD	Commission on Science and Technology for Development
Cyber SIC	Settore Cyber del Servizio delle attività informative della Confederazione
DATEC	Dipartimento federale dell’ambiente, dei trasporti, dell’energia e delle comunicazioni
DDPS	Dipartimento federale della difesa, della protezione della popolazione e dello sport
DDPS-POLSIC	Dipartimento federale della difesa, della protezione della popolazione e dello sport - Politica di sicurezza
DEFR	Dipartimento federale dell’economia, della formazione e della ricerca

DFAE	Dipartimento federale degli affari esteri
DFF	Dipartimento federale delle finanze
DFGP	Dipartimento federale di giustizia e polizia
DFI	Dipartimento federale dell'interno
ENISA	European Network and Information Security Agency
fedpol	Ufficio federale di polizia
GCHQ	Government Communications Headquarters
GovCERT	Swiss Governmental Computer Emergency Response Team
GS-C	Gruppo specializzato Cyber
ICANN	Internet Cooperation for Assigned Names and Numbers
ICT	Information and Communication Technology
IGF	Internet Governance Forum
LAIn	Legge federale sulle attività informative
MELANI	Centrale d'annuncio e d'analisi per la sicurezza dell'informazione
NATO	Organizzazione del Trattato dell'Atlantico del Nord
NSA	National Security Agency
ODIC	Organo direzione informatica della Confederazione
OIC MELANI	Operation Information Center della Centrale d'annuncio e d'analisi per la sicurezza dell'informazione
ONU	Organizzazione delle Nazioni Unite
OSCE	Organizzazione per la sicurezza e la cooperazione in Europa
PA SNPC	Piano di attuazione della strategia nazionale per la protezione della Svizzera contro i cyber-rischi
RSS	Rete integrata Svizzera per la sicurezza
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
SG-DDPS	Segreteria generale del Dipartimento federale della difesa, della protezione della popolazione e dello sport
SIC	Servizio delle attività informative della Confederazione
SIM	Servizio informazioni militare
SNPC	Strategia nazionale per la protezione della Svizzera contro i cyber-rischi
Strategia PIC	Strategia per la protezione delle infrastrutture critiche
TIC	Tecnologie dell'informazione e della comunicazione
UFAE	Ufficio federale per l'approvvigionamento economico del Paese
UFAS	Ufficio federale delle assicurazioni sociali
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
VMSI	Vertice mondiale sulla società dell'informazione (World Summit on the Information Society)