Strategia nazionale per la protezione della Svizzera contro i rischi informatici

del 27 giugno 2012

Riassunto

Le infrastrutture di informazione e di comunicazione hanno profondamente modificato l'economia, lo Stato e la società. L'utilizzazione del cyberspazio (per es. Internet e reti mobili) comporta molteplici vantaggi e opportunità. Tuttavia l'interconnessione digitale implica anche la possibilità di perturbare il funzionamento delle infrastrutture di informazione e di comunicazione e di abusare di tali infrastrutture a fini criminali, spionistici, egemonici o terroristici. Perturbazioni, manipolazioni e attacchi mirati eseguiti tramite le reti elettroniche sono rischi con i quali convive una società dell'informazione. È quindi ipotizzabile che in futuro gli attacchi informatici si moltiplichino.

Dato che la protezione delle infrastrutture di informazione e di comunicazione contro i rischi informatici è nell'interesse nazionale della Svizzera, il Consiglio federale ha dato l'incarico di elaborare una strategia nazionale per la protezione della Svizzera contro i rischi informatici. Il Governo federale persegue i seguenti obiettivi strategici:

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

La presente strategia tiene anche conto di diversi interventi parlamentari che esortano a rafforzare le misure contro gli attacchi informatici.

Le condizioni quadro e le premesse essenziali per ridurre i rischi informatici sono un modo di agire autoresponsabile, la collaborazione nazionale tra economia e autorità nonché la cooperazione con l'estero. Un permanente scambio reciproco di informazioni deve garantire trasparenza e fiducia. Lo Stato deve intervenire solo quando sono in gioco interessi pubblici o nei casi in cui agisce in funzione del principio di sussidiarietà.

La gestione dei rischi informatici deve essere intesa come componente di un processo aziendale, produttivo e amministrativo integrale, nel quale devono essere coinvolti tutti gli attori, dal livello amministrativo e tecnico sino al livello direttivo. Una gestione efficace dei rischi informatici parte dal principio che nei compiti e nelle responsabilità attuali delle autorità, dell'economia e della popolazione sono compresi numerosi aspetti inerenti al cyberspazio. Alla base della strategia nazionale vi è la considerazione che ogni unità organizzativa del livello politico, economico e sociale è responsabile dell'individuazione di tali aspetti e dell'integrazione – e pertanto, nei limiti del possibile, della riduzione – dei conseguenti rischi nei rispettivi processi. Le strutture decentrate dell'Amministrazione e dell'economia devono essere rafforzate per questi compiti; le risorse e i processi già esistenti devono essere impiegati di conseguenza.

La costante integrazione di informazioni tecniche e non tecniche è indispensabile per analizzare e valutare globalmente i rischi informatici nonché per poter diffondere le conoscenze risultanti dalle ricerche.

Un caso effettivo di crisi è caratterizzato da un attacco riuscito con gravi conseguenze e necessita una specifica gestione della crisi da parte degli attori coinvolti, autorità addette al perseguimento penale comprese.

Alla luce di queste considerazioni, la presente strategia propone una serie di misure concrete ripartite in sette campi d'azione:

Campo d'azione 1	***Misure***	
Individuazione dei rischi mediante la ricerca	*1*	*Ricerche in merito ai nuovi rischi in relazione con la problematica del cyberspazio*
Campo d'azione 2	***Misure***	
Analisi dei rischi e della vulnerabilità	*2*	*Verifica autonoma dei sistemi Analisi dei rischi per la minimizzazione dei rischi in collaborazione con le autorità, i fornitori di prestazioni TIC e i fornitori di sistemi*
	3	*Verifica – a livello di sistemi, di organizzazione e di caratteristiche tecniche – della vulnerabilità dell'infrastruttura TIC*
Campo d'azione 3	***Misure***	
Analisi della situazione di minaccia	*4*	*Elaborazione della rappresentazione e dell'evoluzione della situazione*
	5	*Elaborazione di eventi per l'ulteriore sviluppo di misure*
	6	*Panoramica dei casi e coordinamento dei casi di portata intercantonale*
Campo d'azione 4	***Misure***	
Creazione di competenze	*7*	*Allestimento di una panoramica delle offerte di formazione in materia di creazione di competenze e individuazione delle lacune*
	8	*Eliminazione delle lacune riscontrate nell'ambito delle offerte di formazione in materia di creazione di competenze e incremento dell'impiego di offerte di elevata qualità*

Campo d'azione 5	*Misure*	
Relazioni e iniziative internazionali	*9*	*Partecipazione attiva della Svizzera nel settore dell'Internet governance*
	10	*Cooperazione al livello della politica di sicurezza internazionale*
	11	*Coordinamento degli attori in occasione della partecipazione a iniziative e «best practices» nell'ambito dei processi di sicurezza e di protezione*
Campo d'azione 6	***Misure***	
Gestione della continuità operativa e gestione delle crisi	*12*	*Rafforzamento e miglioramento della resistenza (resilienza) nei confronti di perturbazioni e di eventi*
	13	*Coordinamento delle attività in primo luogo con gli attori direttamente interessati e appoggio dei processi decisionali mediante competenze specialistiche*
	14	*Misure attive per l'identificazione degli autori ed eventuale perturbazione della loro infrastruttura nel caso di una minaccia specifica*
	15	*Elaborazione di un concetto per procedure e processi di condotta volti alla soluzione tempestiva dei problemi*
Campo d'azione 7	***Misure***	
Basi legali	*16*	*Verifica delle basi legali vigenti in base alle misure e ai concetti d'attuazione e definizione delle priorità per quanto riguarda gli adeguamenti immediati*

Nell'ambito del loro mandato fondamentale, gli organi della Confederazione designati quali responsabili nella Strategia dovranno concretizzare le misure entro la fine del 2017. In tale processo di concretizzazione occorrerà coinvolgere i partner in seno alle autorità, all'economia e alla società. Nella fattispecie, un organo di coordinamento verificherà la concretizzazione delle misure e la necessità di ulteriori provvedimenti di minimizzazione dei rischi. Tale organo di coordinamento sarà integrato in un servizio della Confederazione.

Indice

Strategia

1 Introduzione

La rete digitale globale ha creato possibilità inaspettate, sia in senso positivo che in senso negativo. Stato, economia e società fanno largo uso delle infrastrutture di informazione e di comunicazione e dell'accesso al cyberspazio (Internet, reti e applicazioni mobili, e-business, Governo elettronico, programmi di gestione computerizzati). Ciò significa però anche che la vulnerabilità e la dipendenza nei confronti di perturbazioni, manipolazioni e attacchi è aumentata. Se, da un lato, le possibilità di un impiego positivo delle infrastrutture di informazione e di comunicazione sono pressoché illimitate, dall'altro, anche le possibilità di un loro abuso a fini criminali, spionistici, terroristici o militari oppure le possibilità di perturbazioni del funzionamento sono pressoché infinite. È ipotizzabile che la tendenza all'aumento del grado di interconnessione e della complessità delle infrastrutture di informazione e di comunicazione persista.

Il funzionamento della Svizzera quale sistema globale (Stato, economia, trasporti, approvvigionamento energetico, comunicazioni ecc.) dipende da un numero sempre maggiore di sistemi di informazione e di comunicazione interconnessi (calcolatori e reti). Questa infrastruttura è vulnerabile. Turbative capillari o durature o eventuali attacchi possono compromettere notevolmente le prestazioni tecniche, economiche e amministrative della Svizzera. Questi attacchi possono avere diversi autori e motivi: si può trattare di singoli individui, attivisti con obiettivi politici, organizzazioni criminali con intenzioni fraudolente o ricattatorie, spie statali o terroristi che vogliono perturbare o destabilizzare Stato e società. Gli attacchi alle infrastrutture di informazione e di comunicazione (TIC) sono particolarmente attrattivi non solo perché tali infrastrutture offrono molte possibilità di abuso, di manipolazione o di arrecare danni, ma anche perché richiedono pochi mezzi e permettono di mantenere l'anonimato.

La protezione[1] delle infrastrutture di informazione e di comunicazione contro simili turbative e attacchi è nell'interesse nazionale della Svizzera. Sebbene negli ultimi anni siano state adottate misure per ridurre i rischi[2] nel cyberspazio, è tuttavia emerso che queste misure non sono sufficienti per tutti i casi. Poiché bisogna attendersi un ulteriore aumento delle turbative e attacchi contro le infrastrutture di informazione e di comunicazione (e quindi, per il loro tramite, anche ad altre infrastrutture), il 10 dicembre 2010 il Consiglio federale ha incaricato il Dipartimento federale della difesa, della protezione della popolazione e dello sport (DDPS) di elaborare una strategia nazionale per la protezione della Svizzera contro i rischi informatici. Obiettivo della strategia è di indicare quali sono i rischi attuali, i mezzi di cui dispone la Svizzera per combatterli, dove risiedono le lacune e come queste ultime possono

1 Comprende tutte le misure per la protezione delle infrastrutture di informazione e di comunicazione contro intrusioni e perturbazioni non autorizzate delle loro funzioni, ma non la lotta contro la diffusione di contenuti illeciti, come ad esempio la pornografia infantile. Vengono considerati gli aspetti tecnici, ma non le questioni contenutistiche inerenti a disinformazione e propaganda.

2 I rischi sono definiti in funzione della portata del danno attesa e dalla probabilità di insorgenza delle minacce e dei pericoli. La strategia tiene conto di entrambi.

essere colmate efficacemente ed efficientemente. La presente strategia nazionale per la protezione della Svizzera contro i rischi informatici è il risultato di tali lavori[3].

I rischi informatici sono molteplici. Economia, società e Stato sono esposti a questi rischi. Una strategia efficace per la protezione contro i rischi informatici deve quindi poggiare su un approccio globale e integrare tutti gli attori statali e privati più importanti, gestori di infrastrutture critiche, utenti e produttori. La presente strategia per la protezione della Svizzera contro i rischi informatici si rivolge in primo luogo agli organi della Confederazione ed è stata elaborata in collaborazione con rappresentanti di tutti i dipartimenti, diversi gestori di infrastrutture critiche, i fornitori di prestazioni TIC e i fornitori di sistemi e l'economia. Descrive i ruoli dei diversi attori e l'impostazione della collaborazione necessaria per una migliore protezione contro i rischi informatici e costituisce pertanto la base dell'intensa collaborazione con i Cantoni nell'ambito della concretizzazione.

Molte prestazioni sono oggi offerte e utilizzate tramite canali elettronici. Ciò comporta una crescente presenza di tutti gli attori in Internet nonché un aumento della loro dipendenza dalle infrastrutture critiche[4]. L'economia è pertanto altamente vulnerabile rispetto ai rischi informatici, si pensi ad esempio agli attacchi a scopo di frode o di lucro o allo spionaggio economico. Il coinvolgimento dell'economia, segnatamente dei gestori di infrastrutture critiche, dei fornitori di prestazioni TIC e dei fornitori di sistemi, in una strategia per la protezione contro i rischi informatici è pertanto essenziale.

- Gli attacchi informatici contro infrastrutture critiche possono avere ripercussioni particolarmente gravi perché pregiudicano funzioni vitali o possono provocare reazioni a catena fatali. I gestori (spesso privati) di infrastrutture critiche rivestono pertanto un ruolo fondamentale in qualità di fornitori di prestazioni di importanza sovraordinata e rilevante sotto il profilo della sicurezza.
- Le autorità statali e le amministrazioni di ogni livello (Confederazione, Cantoni e Comuni) possono parimenti essere vittime di attacchi informatici tali da pregiudicare le loro funzioni legislative, esecutive e giudiziarie oppure danneggiarli nella loro qualità di gestori e utenti di infrastrutture critiche o di istituti di ricerca.
- I rischi informatici minacciano anche la popolazione con tutti i singoli utenti privati e professionali di sistemi di informazione e di comunicazione nonché di infrastrutture critiche. Una strategia efficace contro i rischi informatici deve pure tenere conto del comportamento individuale e dei relativi rischi.

3 La strategia tiene conto di diversi interventi parlamentari che chiedevano il rafforzamento delle misure contro i rischi informatici: 08.3100 – Mozione Burkhalter: Strategia nazionale per combattere la criminalità su Internet; 08.3101 – Postulato Frick: Proteggere meglio la Svizzera dalla criminalità informatica; 10.3136 – Postulato Recordon: Valutazione della minaccia in materia di cyberguerra; 10.3625 – Mozione CPS-CN: Misure contro gli attacchi informatici; 10.3910 – Postulato Gruppo liberale radicale: Centro di condotta e coordinamento nell'ambito delle cyberminacce; 10.4102 – Postulato Darbellay: Concetto per la protezione delle infrastrutture digitali della Svizzera.

4 Le infrastrutture critiche sono infrastrutture la cui perturbazione, interruzione o distruzione comporta serie ripercussioni sulla società, sull'economia e sullo Stato. Tra queste rientrano ad esempio impianti di controllo e commutazione dell'approvvigionamento energetico o delle telecomunicazioni. Le infrastrutture critiche saranno repertoriate in un inventario nel quadro della strategia nazionale per la protezione delle infrastrutture critiche (FF **2012** 6875).

In prima linea i singoli attori sono responsabili essi stessi del mantenimento e dell'ottimizzazione delle misure di protezione per minimizzare i rischi informatici. È nella natura delle cose: i rischi informatici rientrano in compiti, responsabilità e processi già disciplinati. È pertanto nell'interesse degli utenti elaborare e attuare soluzioni su misura specifiche ai settori o rami economici. Questo approccio corrisponde anche alla natura decentrata delle strutture economiche e statali della Svizzera. Lo Stato fornisce in via sussidiaria prestazioni per la protezione contro i rischi informatici, ad esempio mediante lo scambio di dati e informazioni dei servizi di intelligence. Laddove un'azione autoresponsabile e settoriale non è efficace, efficiente o praticabile, lo Stato deve fornire in via sussidiaria prestazioni supplementari per la protezione contro i rischi informatici e sostenere gli altri attori. La presente strategia intende indicare le attuali lacune nella gestione dei rischi informatici. Descrive le prestazioni che lo Stato e gli altri attori devono garantire per incrementare il livello di protezione in Svizzera.

Al riguardo occorre osservare che gli sforzi per garantire maggiore protezione possono collidere con altri interessi altrettanto legittimi. Occorre creare una base d'informazione per quanto possibile esaustiva, basata su conoscenze tecnico-operative e strategico-politiche, per poter adottare le relative decisioni fondandosi su informazioni affidabili: le considerazioni in materia di protezione possono contrapporsi a quelle economiche, ad esempio quando la realizzazione di ridondanze e sovraccapacità nelle infrastrutture sarebbe auspicabile per motivi di protezione, ma entra in conflitto con riflessioni di ordine economico. A ciò si aggiunge il fatto che la liberalizzazione economica ha modificato la situazione di partenza, in quanto un numero sempre maggiore di gestori di infrastrutture critiche (per es. energia, telecomunicazioni) sono stati privatizzati o parzialmente privatizzati e sottostanno quindi primariamente a una logica di mercato. Un secondo settore in cui potrebbero sorgere conflitti d'interesse è quello dei diritti della personalità: gli sforzi volti a migliorare i meccanismi di protezione del cyberspazio (per es. tramite il rafforzamento dei controlli o della sorveglianza) devono essere ponderati tenendo conto della protezione della sfera privata. È altresì compito della presente strategia eseguire una ponderazione degli interessi e indicare come si possano attuare provvedimenti in modo avveduto.

Se insorge un caso effettivo di crisi caratterizzato da un attacco riuscito o da un pregiudizio durevole con gravi conseguenze, si impone una particolare gestione della crisi. Gli sforzi sono in tal caso incentrati su una combinazione di azioni in seno alle strutture esistenti, da eseguire tenendo conto di misure di carattere nazionale e a guida politica nonché in considerazione delle disposizioni legali concernenti il perseguimento penale. Al riguardo va osservato che sono parte integrante della gestione di una crisi anche l'individuazione delle cause e il miglioramento della capacità di resistenza dell'infrastruttura interessata. A tal fine sono integrati nella pertinente procedura, sulla base di appositi accordi, anche i gestori di infrastrutture critiche nonché i fornitori determinanti di prestazioni TIC e i fornitori determinanti di sistemi.

La strategia per la protezione della Svizzera contro i rischi informatici presenta interfacce con altri progetti che a livello di Confederazione si occupano di questioni di sicurezza e sono affini sotto il profilo contenutistico. Nel quadro della concretizzazione questi lavori devono essere strettamente armonizzati tra loro. I progetti più importanti al riguardo sono:

Strategia del Consiglio federale per una società dell'informazione in Svizzera

Il 9 marzo 2012 il Consiglio federale ha adottato la sua strategia per una società dell'informazione in Svizzera. La Confederazione pone l'accento su «sicurezza e fiducia». Gli obiettivi perseguiti sono l'ampliamento delle competenze in materia di sicurezza, la protezione contro la criminalità in Internet e l'aumento della resilienza delle tecnologie dell'informazione e della comunicazione (TIC) nonché delle infrastrutture critiche. Il relativo concetto, già approvato nel 2010 dal Governo federale, prevede misure finalizzate alla sensibilizzazione della popolazione e delle piccole e medie imprese a un impiego delle TIC sicuro e conforme alla legge.

Strategia nazionale per la protezione delle infrastrutture critiche

L'Ufficio federale della protezione della popolazione (UFPP) è stato incaricato dal Consiglio federale di coordinare i lavori nell'ambito della protezione delle infrastrutture critiche (PIC). Fondandosi sulla strategia di base PIC adottata dal Consiglio federale il 18 maggio 2009[5], l'UFPP allestirà, tra l'altro, un elenco di infrastrutture critiche in Svizzera (inventario PIC), nell'ambito del quale saranno identificate anche le infrastrutture critiche TIC. Inoltre sarà elaborata una guida per il miglioramento della protezione globale (integrale) delle infrastrutture critiche. Attualmente la strategia di base PIC sta evolvendo verso una strategia nazionale PIC che sarà presentata al Consiglio federale unitamente alla presente strategia.

Legislazione sulla sicurezza dell'informazione in seno alla Confederazione

Nella sua decisione del 12 maggio 2010, il Consiglio federale ha incaricato il DDPS di elaborare basi legali formali per la protezione e la sicurezza dell'informazione, al fine di proteggere e garantire confidenzialità, disponibilità, integrità e autenticità di dati e informazioni. In primo luogo, questa nuova legislazione si prefigge di definire i principi della sicurezza dell'informazione per tutte le autorità federali e di disciplinare uniformemente le responsabilità. Saranno pertanto definite direttive per il trattamento di dati e informazioni degni di protezione. La procedura di consultazione è prevista per la fine del 2012.

Rapporto del Consiglio federale in adempimento del postulato Malama (Sicurezza interna: chiarire le competenze)

Il postulato Malama incaricava il Consiglio federale di verificare in un rapporto l'adeguatezza dell'ordinamento costituzionale delle competenze e l'effettiva ripartizione dei compiti tra Confederazione e Cantoni nel campo della sicurezza interna. Al riguardo, è stato verificato se l'attuale ripartizione delle competenze sia appropriata e conforme alle sfide odierne. Il Consiglio federale ha licenziato il rapporto in data 2 marzo 2012[6].

5 Il testo della strategia di base è consultabile al sito www.bevoelkerungsschutz.admin.ch/internet/bs/it/home.html > Temi > Protezione delle infrastrutture critiche > Strategia di base PIC

6 FF **2012** 3973

2 Rischi informatici

I rischi informatici sono reali e molteplici. Sebbene non siano disponibili dati precisi, ma solo valutazioni sommarie sulla loro portata, sulla frequenza di attacchi informatici o perturbazioni tecniche nonché sull'entità dei danni effettivi o dei danni potenziali, la tendenza degli ultimi anni è incontestabile e chiara: i casi in cui sono attaccati e danneggiati Stati, imprese e privati attraverso reti di dati continuano a crescere, sia quantitativamente, sia qualitativamente.

Questo deriva dall'incremento del grado di interconnessione delle infrastrutture di informazione e di comunicazione, dalle loro interdipendenze e dall'assenza di trasparenza dei processi di supporto. Con la complessità di questi sistemi aumenta anche il potenziale di errore nonché la sensibilità ai disturbi e parimenti le possibilità di attacchi. Verosimilmente, in futuro gli attacchi informatici saranno più professionali e pericolosi. Oltre ai casi noti, si sospetta un numero elevato di attacchi non segnalati o non scoperti. Il numero dei casi non divulgati è anche in relazione con la temuta perdita di reputazione delle imprese attaccate.

2.1 Metodi

Gli attacchi informatici sono rivolti contro computer, reti e dati. Mirano a danneggiare l'integrità dei dati o il funzionamento dell'infrastruttura nonché a limitarne o interromperne la disponibilità. Si tratta quindi, tra l'altro, di compromettere la confidenzialità o l'autenticità delle informazioni leggendo, cancellando o modificando dati senza autorizzazione, sovraccaricando i server, spiando i canali d'informazione oppure manipolando in maniera mirata i sistemi di sorveglianza o di gestione.

Gli strumenti cui ricorrono gli autori di attacchi informatici sono molteplici. Si può trattare di malware installati in modo mirato e all'insaputa dell'utente sul suo computer allo scopo di compromettere la confidenzialità, l'integrità e l'autenticità dei dati. Funzioni lacunose di sistemi operativi e applicazioni (per es. navigatori Internet o applicazioni specifiche) mal protetti e oggetto di manutenzione insufficiente servono agli aggressori per assumere il controllo dei computer in questione. Questi computer possono pertanto essere controllati a distanza, attraverso Internet, offrendo la possibilità di installare sui sistemi ulteriori malware. Questi ultimi sono a loro volta in grado di accedere ai dati salvati, trasmetterli agli aggressori, modificarli o cancellarli. I dati immessi dall'utente con la tastiera possono essere registrati e trasmessi all'aggressore. È inoltre possibile provocare l'accesso involontario a siti non protetti. In questo modo si possono sottrarre, tra l'altro, numeri di carte di credito, dati di accesso ai servizi di e-banking o altri dati confidenziali dell'utente. Gli aggressori sfruttano però anche le lacune organizzative dei concetti di sicurezza delle imprese per penetrare in sistemi protetti. Gli autori degli attacchi informatici riescono sovente a penetrare nei sistemi sfruttando processi di elaborazione dati e sistemi mal concepiti sotto il profilo della sicurezza o sistemi con una manutenzione lacunosa (per es. la password iniziale non viene cambiata).

Inoltre, gli aggressori utilizzano i computer manipolati inviando ai server richieste di massa coordinate e a tappeto. Questi attacchi, detti «Distributed Denial of Service», perturbano la disponibilità dei dati.

Per compromettere la confidenzialità dei dati, in molti casi vengono applicati metodi simili a quelli usati nello spionaggio (per es. sfruttamento delle debolezze umane,

furto o effrazione). Gli utenti di sistemi vengono sollecitati a fornire informazioni su misure di sicurezza. Inoltre, vengono rubati supporti di dati o modificate infrastrutture effettuando direttamente in loco manipolazioni della configurazione. Possono anche essere impiegati metodi analoghi a quelli utilizzati nell'ambito del sabotaggio per sferrare attacchi mirati contro impianti di controllo industriali[7] ricorrendo a malware appositamente sviluppati.

Nel cyberspazio gli aggressori godono di molti vantaggi, che evitano a loro stessi e ai loro attacchi di essere scoperti (tempestivamente) e di essere oggetto di un perseguimento penale (efficace): anonimato, distanza geografica, ostacoli giuridici, eliminazione di tracce tramite falsificazione di dati tecnici e aumento della complessità tecnica dei metodi di aggressione. Spesso, partendo dai metodi di attacco e dagli strumenti individuati non è possibile risalire inequivocabilmente agli aggressori e ai loro motivi. Tutti gli aggressori dispongono degli stessi metodi e strumenti, ma nel contempo agiscono per motivi diversi e per conto di altri mandanti.

Gli attacchi informatici più frequenti possono essere sferrati in modo relativamente semplice, in quanto spesso i mezzi necessari e le conoscenze tecniche possono essere acquisiti facilmente e a buon mercato. Nella maggior parte degli attacchi si tratta di atti di vandalismo non coordinati, di spionaggio o di azioni fraudolente in Internet che di regola provocano danni contenuti (per es. danni alla reputazione) che possono essere eliminati abbastanza facilmente. Anche se la protezione contro questi attacchi è importante, la presente strategia si focalizza in particolare sugli attacchi con potenziale di dannosità talmente elevato da compromettere direttamente o indirettamente la capacità operativa dell'economia, dello Stato e della società.

Anche con attacchi specifici contro obiettivi particolarmente protetti è possibile provocare grossi danni. Questi attacchi richiedono un impegno molto elevato.

Realisticamente, non è possibile raggiungere una protezione assoluta contro gli attacchi informatici, per cui occorre dare la priorità a una combinazione efficace di capacità reattive e preventive che, nel quadro di un approccio orientato alla minimizzazione dei rischi, hanno lo scopo di limitare i danni e di ripristinare la situazione iniziale.

2.2 Attori e motivi

Gli autori sono individui, gruppi o Stati e si differenziano notevolmente quanto a intenzioni, mezzi tecnici e risorse finanziarie.

Di regola gli *attori statali o finanziati dallo Stato* dispongono di risorse finanziarie, tecniche e di personale più importanti e sono meglio organizzati, per cui il loro potenziale di dannosità è relativamente elevato. Con i loro attacchi si prefiggono di spiare, ricattare, compromettere Stati, singole autorità, eserciti, l'economia o istituti di ricerca, o di agire in altro modo contro gli interessi nazionali o economici, per perseguire interessi egemonici ed economici. Anche le imprese, le istituzioni e le persone straniere stabilite in Svizzera sono minacciate.

7 A livello internazionale si parla di sistemi SCADA (Supervisory Control and Data Acquisition). Questi sistemi TIC servono alla sorveglianza e al controllo di processi tecnici.

Nel mese di ottobre del 2009 nel Dipartimento federale degli affari esteri (DFAE) è stato individuato un malware finalizzato ad attività di spionaggio. Questo malware, giunto nella rete attraverso la posta elettronica, è rimasto occultato per molto tempo. Qualche anno prima anche le imprese d'armamento RUAG e Mowag erano state attaccate in un modo simile. Nel mese di giugno del 2010 è stato scoperto un malware (Stuxnet) sviluppato presumibilmente per danneggiare un impianto iraniano di arricchimento dell'uranio introducendo un errore nei sistemi di controllo (SCADA). Vista la complessità tecnica dell'operazione si presuppone che solo un attore statale abbia potuto sferrare questo tipo di attacco.

Gli *attori della criminalità organizzata* sono ritenuti altrettanto pericolosi, in quanto di regola dispongono anch'essi di organizzazioni altamente professionali, ingenti risorse finanziarie e capacità specifiche. Nell'intento di arricchirsi, con i loro attacchi di massa organizzati e permanenti contro l'economia (per es. il settore finanziario) e i privati provocano enormi danni economici e mettono in discussione la credibilità dello Stato di diritto.

Per attaccare gli utenti dei servizi di online banking, da anni viene impiegato, tra gli altri, il cavallo di Troia[8] *ZeuS. Il malware viene introdotto nelle strutture informatiche di privati attraverso siti web falsificati o manipolati. In questo modo, gli aggressori possono piratare la connessione con i servizi di telebanking e prelevare denaro dai conti.*

Negli ultimi tempi assumono un'importanza sempre maggiore gli attacchi contro siti Internet del settore pubblico e privato sferrati dai cosiddetti *«hacktivisti»*. Questi attori non statali, isolati o organizzati in maniera poco rigida, ma che in determinate circostanze possono agire in massa, dispongono di buone capacità tecniche. Il potenziale di dannosità di attacchi di massa in provenienza da queste cerchie è da considerarsi da medio a elevato. Gli «hacktivisti» mirano a interrompere prestazioni di servizi, a provocare danni finanziari o di reputazione allo scopo di attirare l'attenzione del pubblico nei confronti delle loro rivendicazioni.

Nel dicembre del 2010 il gruppo di hacker «Anonymous» ha invitato ad attaccare PostFinance. L'attacco ha comportato l'interruzione dei servizi forniti su Internet per un intero giorno. All'origine di questa reazione vi era la chiusura del conto del fondatore di WikiLeaks, Julian Assange. Nel 2007 attivisti russi hanno attaccato massicciamente infrastrutture di informazione e di comunicazione estoni a causa della rimozione di un monumento militare sovietico a Tallin. Durante diversi giorni non è più stato possibile usufruire dell'offerta di Governo elettronico e dei servizi Internet di diverse ditte. Inoltre, i siti Internet di servizi governativi e imprese sono stati deturpati con propaganda pro-russa.

8 Software con funzioni malevoli (detti anche *malware* o *malicious software*).

I *terroristi* sfruttano il cyberspazio per diffondere la loro propaganda, radicalizzare simpatizzanti, reclutare e formare membri, procurarsi denaro nonché pianificare e comunicare azioni. Sinora in primo piano vi è l'utilizzazione dell'infrastruttura di informazione e di comunicazione, ma non gli attacchi contro quest'ultima: come in passato, i terroristi mirano soprattutto a perpetrare con metodi convenzionali pesanti attacchi fisici contro la vita e l'integrità personale nonché contro le infrastrutture. Gli attacchi informatici di matrice terroristica con conseguenti elevati danni fisici appaiono attualmente poco probabili. Non si può tuttavia escludere che in futuro i terroristi tentino di sferrare attacchi informatici contro infrastrutture critiche di un Paese. Anche se la Svizzera non rappresenta un obiettivo diretto, potrebbe essere interessata dalle ripercussioni transfrontaliere (per es. l'interruzione dell'approvvigionamento di elettricità o perturbazioni del mercato finanziario).

Sino ad oggi non vi è alcun esempio concreto di attentati terroristici per il tramite di attacchi informatici. Tuttavia, le pagine Internet di organizzazioni terroristiche o di gruppi simpatizzanti del terrorismo sono sotto costante sorveglianza allo scopo di individuare appelli alla violenza e indizi di attentati imminenti (per es. siti Internet jihadisti).

Del rimanente, anche eventi o incidenti imprevedibili come guasti ai sistemi causati da usura prematura, eccessiva sollecitazione, difetti di costruzione, manutenzione lacunosa o risultanti da catastrofi naturali possono provocare interruzioni o turbative dell'infrastruttura con gravi ripercussioni.

3 Strutture esistenti

Nel seguito vengono illustrate le strutture per la riduzione dei rischi informatici di cui dispone la Svizzera e i ruoli che spettano ai singoli attori.

3.1 Economia e gestori di infrastrutture critiche

Cerchie interessate[9]

La piazza economica svizzera è caratterizzata da un settore di prestazioni di servizi forte. Lungo tutta la catena di valore aggiunto, le relazioni e le attività commerciali si basano sulle infrastrutture di informazione e di comunicazione. I dati sono salvati ed elaborati in sistemi informatici interni ed esterni alle imprese. Le comunicazioni e il traffico dei pagamenti avvengono tramite servizi Internet (per es. posta elettronica, telefonia Internet, e-banking e negoziazioni in borsa). Sempre più spesso i contratti vengono conclusi elettronicamente (commercio elettronico, procedure di offerta ecc.). Questo illustra le dipendenze della nostra economia dal funzionamento delle

9 Il DDPS ha chiesto a rappresentanti dell'economia e a gestori di infrastrutture critiche (comprese organizzazioni mantello e associazioni) quali sono le misure che intendono adottare o hanno già adottato per la sicurezza informatica, dove risiedono le lacune e le difficoltà e quali fattori influiscono sulle loro misure di protezione (per es. considerazioni finanziarie). Nel complesso l'inchiesta ha fornito un quadro unitario.

TIC e da altre infrastrutture critiche che essa utilizza, come ad esempio l'approvvigionamento energetico. Pertanto, la protezione della piazza economica svizzera contro i rischi informatici riveste importanza nazionale.

Le infrastrutture critiche garantiscono la disponibilità di beni e prestazioni di servizi fondamentali. Perturbazioni o interruzioni di ampia portata di queste infrastrutture avrebbero gravi ripercussioni sul funzionamento dello Stato, dell'economia e della società. La protezione delle infrastrutture critiche – anche contro i rischi informatici – è pertanto essenziale. I gestori di infrastrutture critiche non devono considerare i rischi unicamente in base a principi puramente economici, ma devono anche compiere sforzi per minimizzarli. Pertanto, già oggi sottostanno in parte a norme speciali. Tuttavia, mancano di regola direttive concrete e vincolanti concernenti standard di protezione nel campo delle TIC impiegate. A dipendenza del grado di criticità e vulnerabilità di un'infrastruttura come pure della situazione di minaccia, le direttive per gli standard di sicurezza e per ulteriori misure volte alla riduzione dei rischi dovrebbero essere disciplinate in modo più esaustivo e preciso in collaborazione con gli organi amministrativi competenti.

Produttori e fornitori di prodotti e prestazioni di servizi TIC assumono una grande responsabilità per la sicurezza dei loro prodotti e quindi anche per la sicurezza informatica dei loro clienti.

Gli attori dell'economia agiscono in gran parte sotto propria responsabilità e liberamente. Per ottenere una panoramica della situazione, ai fini dell'elaborazione della strategia sono state selezionate alcune imprese, alle quali sono state poste domande sulle loro attuali valutazioni, misure e difficoltà nonché sulle previsioni in materia di sicurezza informatica.

Percezione del problema

I rischi informatici rappresentano senza dubbio un tema importante per le imprese. Ciononostante, le valutazioni dei rischi e le misure adottate si differenziano fortemente le une dalle altre, tra un settore economico e l'altro, ma anche all'interno dei settori o rami economici nonché in seno alle aziende. Non è pertanto possibile effettuare una classificazione settoriale semplice della percezione del problema.

Esistono imprese con un'*elevata percezione del problema.* Tra queste si annoverano per lo più grandi aziende che dispongono di risorse importanti in termini di capitale, personale, infrastruttura e conoscenze specifiche (per es. scienze forensi, gestione dei rischi e delle crisi, *Computer Emergency Response Team*). Nella maggior parte dei casi queste imprese sono attive a livello internazionale e vantano buone interconnessioni. Anche le imprese principalmente attive nel settore della sicurezza (per es. industria dell'armamento) hanno necessità elevate in materia di sicurezza e sono per lo più in grado di difendersi da sole dagli attacchi informatici non coordinati cui la Svizzera è esposta quotidianamente.

Anche i gestori di infrastrutture critiche fanno parte degli attori con un'elevata percezione del problema. Secondo l'inchiesta, essi auspicano che le direttive per gli standard di sicurezza vengano definite in modo più esaustivo e preciso d'intesa con le autorità di vigilanza, in funzione della criticità e vulnerabilità della singola infrastruttura.

Il gruppo più grande è costituito dalle piccole e medie imprese con una *media percezione del problema*. Esse utilizzano di regola infrastrutture e concetti di sicurezza

commerciali (per es. *firewall*, programmi antivirus). La loro capacità di migliorare le misure di protezione nel cyberspazio è limitata soprattutto dalle risorse finanziarie.

Un altro gruppo è costituito dalle imprese che presentano una *bassa percezione del problema*. Queste imprese non hanno le risorse per adottare misure di protezione riguardanti i rischi informatici o non ne vedono la necessità.

Misure

Solo una minoranza degli attori dell'economia intervistati sono in grado di difendersi da attacchi informatici di elevata intensità (in relazione a simultaneità, complessità, potenziale di dannosità e durata).

Numerose imprese conoscono standard di sicurezza (per es. ISO 2700x, NERC) e li applicano. Sono altresì disponibili provvedimenti di tipo tecnico e organizzativo (per es. esercizio di sistemi autonomi, impiego di incaricati della sicurezza). Inoltre, vengono adottate misure per migliorare la consapevolezza in materia di sicurezza dei collaboratori, anche se spesso, al riguardo, vengono trascurati i decisori. I provvedimenti contribuiscono a identificare i punti deboli all'interno dell'impresa e a migliorare costantemente e a lungo termine le misure di protezione. Tuttavia, la maggioranza delle piccole e medie imprese (PMI) non fa molto per la propria sicurezza. L'accettazione dei rischi è spesso dettata da considerazioni di ordine economico. I rischi informatici sono una parte integrante dei processi aziendali globali e non possono di conseguenza essere trattati isolatamente (individualmente) o unicamente a livello tecnico. A ciò si aggiunge che le informazioni destinate a fungere da basi decisionali spesso sono lacunose e comprendono soltanto marginalmente indicazioni specifiche al cyberspazio. Per conseguire un grado di sicurezza per quanto possibile ineccepibile e neutro sul piano della concorrenza, gli imprenditori e i gestori di infrastrutture critiche si attendono che direttive e norme siano elaborate e attuate in modo unitario nonché in collaborazione con tutti gli interessati e con tutti i responsabili.

L'ottimizzazione dello scambio di informazioni tra gli attori dell'economia, in particolare tra i gestori di infrastrutture critiche, i fornitori di prestazioni TIC, i fornitori di sistemi e le autorità, è determinante per trovare soluzioni ai problemi e minimizzare i danni. Tuttavia, si constata che sinora la collaborazione oltre i confini aziendali (anche nel caso delle autorità) non è stata molto intensa. A tutt'oggi, le più importanti associazioni economiche si sono occupate troppo poco del tema della sicurezza informatica e del loro ruolo al riguardo. Dall'inchiesta emerge la necessità di sviluppare ulteriormente e ampliare in particolare forme di collaborazione tra economia e autorità, soprattutto per lo scambio di informazioni sulla situazione e i provvedimenti in materia di gestione delle crisi[10]. Spesso tuttavia gli attacchi informatici vengono taciuti, precludendo ad altri potenziali interessati la possibilità di essere allertati per tempo. Le imprese e i gestori di infrastrutture critiche che hanno partecipato all'inchiesta chiedono forme di collaborazione principalmente facoltative. L'autoresponsabilità rimane un elemento centrale, mentre dalla collaborazione

10 Cfr. al riguardo lo studio «Evaluation und Weiterentwicklung der Melde- und Analysestelle Informationssicherung Schweiz (MELANI)», («Valutazione e ulteriore sviluppo della Centrale svizzera d'annuncio e d'analisi per la sicurezza dell'informazione [MELANI]», non tradotto in italiano) pubblicato nel 2010 dal Politecnico federale di Zurigo. Lo studio comprende una verifica dell'efficacia della centrale MELANI, un confronto a livello internazionale con altri modelli di protezione delle informazioni, le conseguenti possibilità per l'ulteriore sviluppo della Centrale e relative raccomandazioni.

devono risultare contributi per quanto concerne l'eliminazione congiunta di eventuali lacune e l'ottenimento di informazioni rilevanti per la situazione e utili per la rispettiva gestione dei rischi.

Negli ultimi anni sono stati compiuti dei progressi nella collaborazione tra gestori di infrastrutture critiche, fornitori di prestazioni TIC, fornitori di sistemi e Confederazione per la riduzione dei rischi informatici. Per quanto riguarda la pianificazione strategica a lungo termine, l'analisi dei rischi e la gestione della continuità operativa vi è una cooperazione in primo luogo con l'Ufficio federale per l'approvvigionamento economico del Paese (UFAE), i Cantoni e parti delle infrastrutture critiche nonché con i fornitori di prestazioni TIC e i fornitori di sistemi. Oltre a ciò, tra la Centrale d'annuncio e d'analisi per la sicurezza dell'informazione (MELANI) della Confederazione, i Cantoni e l'economia privata esiste una *public private partnership (PPP)* funzionante, nell'ambito della quale MELANI sostiene i gestori di infrastrutture critiche in Svizzera nel loro processo di sicurezza dell'informazione e incentiva lo scambio tra le imprese di informazioni in materia di rischi informatici. Siccome le risorse di personale disponibili permettono a MELANI di adempiere il mandato di base solo in misura limitata, è prioritario domandarsi in che misura la Centrale possa soddisfare le future maggiori esigenze dei gestori di infrastrutture e interrogarsi sulle conseguenti possibili ripercussioni a livello di risorse.

Stretti margini di guadagno e una forte concorrenza internazionale non permettono di stabilire requisiti in materia di sicurezza più rigorosi, valevoli unicamente per la Svizzera. I maggiori costi che ne risulterebbero procurerebbero uno svantaggio concorrenziale al nostro Paese. Ci si attende pertanto che le prescrizioni in materia di protezione e le soluzioni per l'attuazione vengano elaborate in un contesto internazionale. La cooperazione internazionale non deve tuttavia essere intensificata solo in relazione a norme e prescrizioni, bensì anche ai fini dell'individuazione dei rischi e di una gestione comune delle crisi. Al riguardo, oltre agli attori statali occorre integrare anche rappresentanti dell'economia (segnatamente i gestori di infrastrutture critiche, i fornitori di prestazioni TIC e i fornitori di sistemi) e della società.

La scarsità di specialisti come pure l'acquisizione e il mantenimento di conoscenze specializzate rappresentano una grande sfida. Le imprese e i gestori di infrastrutture critiche che hanno partecipato all'inchiesta auspicano l'incoraggiamento della ricerca e dello sviluppo in materia nonché il reclutamento e la formazione di specialisti.

3.2 Confederazione

Negli ultimi anni la Confederazione ha adottato diversi provvedimenti per rafforzare il dispositivo di protezione e i mezzi dell'Amministrazione contro gli attacchi informatici. A livello di Confederazione diversi servizi si occupano di compiti preventivi e reattivi nel settore della sicurezza informatica:

Ministero pubblico della Confederazione

Il Ministero pubblico della Confederazione è l'autorità della Confederazione preposta alle indagini e alla pubblica accusa ed è competente per il perseguimento di reati che sottostanno alla giurisdizione federale (la maggior parte dei reati è di competenza dei Cantoni) nonché per la cooperazione con l'estero.

Incaricato federale della protezione dei dati e della trasparenza

L'Incaricato federale della protezione dei dati e della trasparenza è un servizio di vigilanza e consulenza per gli organi federali e i privati. Nella sua funzione si occupa in particolare di spiegare la legge sulla protezione dei dati e le ordinanze d'esecuzione. Fornisce consulenza sia per questioni giuridiche, sia per gli aspetti tecnici della salvaguardia dei dati.

Stato maggiore speciale per la sicurezza dell'informazione

Lo Stato maggiore speciale per la sicurezza dell'informazione (SONIA) consta di decisori provenienti dagli ambienti dell'amministrazione e dell'economia (gestori di infrastrutture critiche) ed è diretto dal Delegato dell'Organo di direzione informatica della Confederazione. In caso di crisi a livello nazionale nell'ambito della sicurezza dell'informazione entra in azione su richiesta di MELANI. Attualmente, SONIA è operativo soltanto in misura limitata, in quanto dopo l'ultimo esercizio effettuato nel 2005 si è constatato che nella pratica la struttura, i processi e l'organizzazione non funzionano. In caso di crisi, i membri previsti per lo Stato maggiore sono generalmente già impegnati in processi sovraordinati di gestione delle crisi.

Centrale d'annuncio e d'analisi per la sicurezza dell'informazione

MELANI è un organo congiunto dell'Organo di direzione informatica della Confederazione (ODIC: gestione di MELANI e *Government Computer Emergency Response Team, GovCERT*[11]) e del Servizio delle attività informative della Confederazione (centro operazioni e informazioni). MELANI appoggia in via sussidiaria il processo di sicurezza dell'informazione delle infrastrutture critiche fornendo informazioni su incidenti e minacce. Raccoglie informazioni tecniche e non, le valuta e trasmette i dati rilevanti ai gestori di infrastrutture critiche. In tal modo, MELANI appoggia il processo di gestione dei rischi all'interno delle infrastrutture critiche, ad esempio offrendo valutazioni della situazione e analisi per l'individuazione precoce di attacchi o incidenti, valutandone le ripercussioni ed esaminando, in caso di bisogno, eventuali malware.

Attualmente MELANI coadiuva una cerchia chiusa di clienti, della quale fanno parte gestori scelti di infrastrutture critiche della Svizzera (un centinaio di membri, quali banche, aziende di telecomunicazione e di approvvigionamento energetico). Per il resto dell'economia e la popolazione MELANI offre il proprio appoggio sotto forma di liste di controllo, guide e programmi didattici. In caso di crisi MELANI è competente per allertare lo Stato maggiore speciale per la sicurezza dell'informazione (SONIA) e coadiuvarlo a livello direttivo per quanto riguarda il campo della sicurezza dell'informazione. Attualmente, il mandato di base di MELANI non può essere adempito interamente in ragione delle risorse di personale insufficienti.

11 I CERT sono organizzazioni competenti per le analisi tecniche degli incidenti. Raccolgono e analizzano informazioni tecniche nel quadro globale di una serie di incidenti. Assumono pure un ruolo di coordinamento. A livello di Confederazione, la corrispondente organizzazione è denominata GovCERT e assume inoltre un ruolo di coordinamento in caso di incidenti internazionali.

Dipartimento federale di giustizia e polizia

Ufficio federale di polizia

Polizia giudiziaria federale

La Polizia giudiziaria federale è un'autorità inquirente della Confederazione. Nella sua sfera di competenza assume compiti di polizia criminale e di polizia giudiziaria ai fini dell'individuazione, della lotta e del perseguimento di reati. Nella sua sfera di competenza garantisce inoltre la collaborazione tra i partner nazionali ed esteri e segue in particolare lo sviluppo tecnico nel settore della cibercriminalità. Garantisce inoltre il mantenimento e lo sviluppo delle conoscenze tecniche e forensi in questi ambiti. È responsabile nell'ambito della polizia giudiziaria soltanto per i casi di competenza federale. Quando non è ancora chiaro se la competenza spetti alla Confederazione o a un Cantone, è autorizzata ad avviare le indagini preliminari. La PGF assume pure il coordinamento di procedure sovracantonali.

Servizio di coordinazione per la lotta contro la criminalità su Internet

Il Servizio di coordinazione per la lotta contro la criminalità su Internet (SCOCI) è un servizio congiunto della Confederazione e dei Cantoni responsabile di individuare per tempo reati in Internet, evitare doppioni nel perseguimento penale e analizzare la criminalità su Internet[12]. SCOCI è aggregato all'Ufficio federale di polizia e funge da punto di contatto nazionale per le persone che intendono segnalare siti o contenuti sospetti su Internet. Dopo un primo esame e dopo aver effettuato una salvaguardia dei dati, SCOCI inoltra le segnalazioni alle autorità di perseguimento penale nazionali o estere competenti. SCOCI è a disposizione del pubblico, delle autorità e dei provider per questioni di natura criminalistica, giuridica e tecnica inerenti alla criminalità su Internet. Effettua anche ricerche attive in rete di contenuti criminali, ad esempio nei settori della pedofilia e della criminalità economica (truffe con carte di credito, phishing mediante e-mail ecc.). È competente per lo sviluppo delle tecniche d'indagine e – con il sostegno dei Cantoni e delle autorità federali operative in questo settore – per l'allestimento di una panoramica globale nazionale delle procedure e per l'osservazione dell'evoluzione del diritto in materia di criminalità su Internet. Funge inoltre da interlocutore per i servizi esteri con compiti analoghi. D'intesa con MELANI, SCOCI garantisce lo scambio di informazioni rilevanti in ambito informatico con le autorità di perseguimento penale e il Servizio delle attività informative della Confederazione.

Cooperazione internazionale di polizia

La Cooperazione internazionale di polizia è competente, tra l'altro, per i contatti con i partner nazionali e internazionali, curati in seno alla Centrale operativa dell'Ufficio federale di polizia. È inoltre responsabile per la collaborazione strategica e operativa con unità e organizzazioni di polizia internazionali (EUROPOL, INTERPOL, ONU, OSCE, Consiglio d'Europa).

12 Cfr. al riguardo l'accordo amministrativo del 19 dicembre 2001 concernente il coordinamento della lotta contro la criminalità su Internet e il regolamento di gestione del 30 marzo 2011 del Servizio di coordinazione per la lotta contro la criminalità su Internet (SCOCI).

Centrale operativa dell'Ufficio federale di polizia

La Centrale operativa dell'Ufficio federale di polizia è l'organo di contatto permanente per le autorità estere. Appoggia, tra l'altro, le inchieste giudiziarie penali nazionali e internazionali nei casi di cibercriminalità. La Centrale non può adottare autonomamente misure nei settori della consulenza giuridica, dell'assistenza giudiziaria, dell'assunzione di prove, della salvaguardia di dati o delle inchieste giudiziarie. Ha tuttavia l'incarico, in qualità di organo di contatto, di agevolare i contatti tra le competenti autorità estere e nazionali (in particolare SCOCI).

Cooperazione strategica

Il compito principale della divisione Cooperazione strategica è di provvedere allo sviluppo della collaborazione internazionale con le organizzazioni partner di polizia. D'intesa e in coordinamento con i servizi specialistici dell'Uffico federale di polizia, rappresenta l'Ufficio nel quadro di conferenze e commissioni bilaterali e multilaterali al fine, tra l'altro, di seguire gli sviluppi della lotta alla criminalità in Internet.

Dipartimento federale della difesa, della protezione della popolazione e dello sport

Servizio delle attività informative della Confederazione

Con i mezzi propri dei servizi di intelligence, il Servizio delle attività informative della Confederazione (SIC) raccoglie informazioni, che vengono analizzate, valutate e diffuse. In Svizzera l'interesse del SIC è focalizzato sul terrorismo, sull'estremismo violento, sulla proliferazione, sugli attacchi all'infrastruttura critica in materia di informazione e sullo spionaggio. Per quanto concerne l'estero, l'interesse del SIC si concentra su questioni attinenti alla politica di sicurezza, tra cui la proliferazione, il terrorismo e l'evoluzione delle forze armate, su tematiche quali la tecnologia degli armamenti e il commercio di armamenti nonché su analisi strategiche. Questi temi sono sempre più di attualità anche nel cyberspazio. Per poterli rilevare, il SIC segue quindi anche l'evoluzione della situazione dei rischi nel cyberspazio. In collaborazione con l'ODIC, il SIC gestisce la parte riguardante le attività informative della Centrale MELANI.

Ufficio federale della protezione della popolazione

La protezione della popolazione ha lo scopo di proteggere la popolazione e le sue basi vitali in caso di catastrofe, in situazioni d'emergenza e in caso di conflitto armato, contribuendo in maniera determinante a limitare e superare gli effetti di eventi dannosi. Catastrofi e situazioni d'emergenza possono risultare anche da gravi attacchi informatici o da altri generi di turbative delle tecnologie dell'informazione e delle comunicazioni (TIC). I pericoli sono di conseguenza oggetto anche dei lavori relativi al progetto «Rischi Svizzera», che fungono da base di pianificazione in seno alla protezione della popolazione. Nel quadro del programma per la protezione delle infrastrutture critiche (programma PIC), l'UFPP coordina per incarico del Consiglio federale i lavori di allestimento dell'Inventario PIC, nel quale sono rilevate non soltanto le infrastrutture critiche TIC, ma anche le applicazioni TIC rilevanti ai fini della sicurezza presenti nelle altre categorie di infrastrutture critiche. In qualità di centro di notifica e di analisi della situazione della Confederazione per gli eventi straordinari, la Centrale nazionale d'allarme (CENAL) in seno all'UFPP deve asso-

lutamente poter contare anche in situazioni di crisi sul corretto funzionamento dei sistemi informatici e delle reti di comunicazione nonché su un ininterrotto approvvigionamento energetico. In futuro la comunicazione di condotta tra gli organi della Confederazione e quelli dei Cantoni (POLYCONNECT/POLYDATA) si svolgerà tramite reti a prova di crisi e di blackout, protette mediante apposita cifratura. Pure il sistema di allerta e allarme (POLYALERT) è attualmente in fase di trasferimento verso una tecnologia a prova di crisi, basata sulla Rete radio nazionale di sicurezza (POLYCOM).

Settore Difesa

Il settore Difesa del DDPS è responsabile per la difesa, l'appoggio a favore delle autorità civili e il promovimento della pace.

Per i compiti di protezione attinenti alla difesa sono responsabili in particolare le organizzazioni seguenti:

Protezione delle informazioni e delle opere

La Protezione delle informazioni e delle opere, insediata presso lo Stato maggiore dell'esercito, si occupa della sicurezza integrale del DDPS. In particolare, è competente per le direttive nei settori della sicurezza delle persone, delle informazioni, dell'informatica e dei beni (materiale e immobili).

In questa funzione elabora prescrizioni in materia di sicurezza per garantire la confidenzialità, la disponibilità, l'integrità e la verificabilità di informazioni e dati nonché la disponibilità e l'integrità dei mezzi TIC.

Gestisce l'Organo di coordinamento per la protezione delle informazioni in seno alla Confederazione e funge da interlocutore per le richieste nazionali e internazionali riguardanti la protezione di informazioni classificate. Sulla base di alcuni accordi internazionali (in particolare con l'Unione europea), la Protezione delle informazioni e delle opere è considerata l'autorità nazionale di sicurezza per tutte le questioni inerenti alla sicurezza dell'informazione in seno alla Confederazione.

Dirige l'elaborazione della legge sulla sicurezza dell'informazione in seno alla Confederazione.

Base d'aiuto alla condotta

La Base d'aiuto alla condotta (BAC) fornisce all'esercito prestazioni di servizi nell'ambito delle TIC in tutte le situazioni: questo esige disponibilità e sicurezza elevate. Gestisce il Centro operazioni elettroniche, il quale fornisce prestazioni ai servizi informazioni. Il Centro operazioni elettroniche impiega crittologi ed è responsabile del settore *Computer Network Operations*, disponendo in tal modo di capacità tecniche finalizzate all'analisi della minaccia e degli eventi nonché alla condotta delle operazioni. La BAC gestisce inoltre il *Computer Emergency Response Team* militare (milCERT), incaricato di sorvegliare le infrastrutture TIC rilevanti per l'esercito. La BAC appoggia essenzialmente l'esercito, ma anche la condotta politica e mantiene pertanto a disposizione i mezzi necessari a tal fine.

Servizio informazioni militare

Nell'esercito e pertanto in seno al settore Difesa, il Servizio informazioni militare (SIM) è competente per l'acquisizione di informazioni a favore del richiedente militare. Con l'assistenza della rete informativa integrata nonché in stretta collabora-

zione con lo Stato maggiore dell'esercito e con le formazioni interessate, il SIM assicura le prestazioni di intelligence nel quadro degli impieghi.

Inoltre, cura i contatti internazionali con i servizi informazioni e le agenzie di intelligence militari (per es. NATO). Nei confronti del SIC funge pertanto da fornitore di informazioni e di supporto relativamente ai rischi informatici e agli aspetti inerenti al cyberspazio riscontrati in ambito militare. Infine, nel quadro dell'impiego di contingenti all'estero, è competente per il controspionaggio e le relative implicazioni a livello di cyberspazio.

Dipartimento federale delle finanze

Organo direzione informatica della Confederazione

L'ODIC emana direttive in materia di TIC e gestisce a livello centrale le prestazioni informatiche standard nell'Amministrazione federale (per es. telecomunicazione). Dirige il GovCERT e la parte strategica di MELANI. In caso di crisi dirige il SONIA e in caso di attacchi contro le infrastrutture di informazione e di comunicazione, può adottare ulteriori misure di sicurezza.

Ufficio federale dell'informatica e della telecomunicazione

L'Ufficio federale dell'informatica e della telecomunicazione fornisce all'Amministrazione federale prestazioni informatiche e di telecomunicazione e gestisce un proprio *Computer security incident response team* (CSIRT), che collabora strettamente con la centrale MELANI e altri servizi dell'Amministrazione federale. Sorveglia costantemente le risorse TIC dell'Amministrazione federale ai fini della detezione di segni di attacco e dispone di un'ampia esperienza nella gestione di attacchi di vasta portata alle infrastrutture della Confederazione. Se tuttavia il numero dei compiti o l'intensità degli attacchi oppure il potenziale di dannosità aumentano, l'Ufficio non dispone delle risorse di personale per fornire le prestazioni necessarie.

Gestione dei rischi Confederazione

La gestione dei rischi è stata implementata nella Confederazione nel 2005. Gli obiettivi e i principi della gestione dei rischi e le varie funzioni in seno all'unità «Gestione dei rischi Confederazione» sono attualmente disciplinati nelle Istruzioni del 24 settembre 2010[13] sulla politica della Confederazione in materia di gestione dei rischi. Per assicurare una concretizzazione omogenea della gestione dei rischi in seno all'Amministrazione federale, in data 21 novembre 2011 l'Amministrazione federale delle finanze ne ha disciplinato i dettagli in maniera vincolante e unitaria a livello di direttive.

Per rischi si intendono eventi e sviluppi suscettibili di insorgere con una certa probabilità e di presentare sostanziali ripercussioni negative di carattere finanziario e non finanziario sul raggiungimento degli obiettivi e sull'adempimento dei compiti dell'Amministrazione federale. L'individuazione tempestiva di tali rischi rientra nei compiti dei servizi specializzati in seno alle unità amministrative e ai dipartimenti. I rischi individuati sono oggetto di analisi e valutazioni. Sulla base dell'esposizione ai rischi individuata, sono adottate le misure necessarie per prevenire per quanto possi-

13 FF **2010** 5759

bile i rischi o perlomeno minimizzarne la portata. La concretizzazione della gestione dei rischi della Confederazione – orientata ai compiti – ha luogo sostanzialmente in maniera decentralizzata nelle unità amministrative e nei dipartimenti.

L'individuazione tempestiva e la difesa da attacchi informatici contro l'Amministrazione federale incombe ai servizi specializzati in seno alle unità amministrative e ai dipartimenti. Poiché concerne tutti i dipartimenti e tutte le unità amministrative della Confederazione, il rischio «Attacchi informatici ai sistemi TIC della Confederazione» è gestito a livello e sotto la direzione del Consiglio federale in qualità di rischio trasversale.

Dipartimento federale dell'ambiente, dei trasporti, dell'energia e delle comunicazioni

Ufficio federale delle comunicazioni

L'Ufficio federale delle comunicazioni (UFCOM) si occupa, tra l'altro, di questioni inerenti alle telecomunicazioni. In questo ambito assume tutti i compiti sovrani e regolatori. In particolare, ha il compito di vigilanza generale sulle telecomunicazioni (compresi i fornitori di servizi internet) ed è responsabile per gli elementi d'indirizzo nel settore delle telecomunicazioni. Tale responsabilità include il contratto di diritto amministrativo con il gestore dei registri Switch concernente l'amministrazione dei domini .ch, la relativa vigilanza e i principi in materia di firma elettronica. L'UFCOM svolge intense attività anche a livello internazionale, segnatamente nei settori «Internet governance» e «International policies». Inoltre, coordina le attività e livello nazionale e internazionale nel quadro della Strategia del Consiglio federale per una società dell'informazione in Svizzera.

Ufficio federale dell'energia

L'Ufficio federale dell'energia è il centro di competenza per le questioni concernenti l'approvvigionamento e il consumo energetici. Crea le premesse per un approvvigionamento energetico sufficiente, resistente alle crisi, ampio e diversificato, economico e sostenibile; inoltre provvede a standard di sicurezza elevati nel quadro della produzione, del trasporto e del consumo di energia.

Parallelamente al crescente impiego di mezzi TIC negli impianti di produzione di energia e nelle relative reti, assumono un'importanza crescente anche gli aspetti inerenti al cyberspazio rientranti in questi settori.

Ufficio federale dell'aviazione civile

L' Ufficio federale dell'aviazione civile è competente per la legislazione e le attività di vigilanza concernenti, tra l'altro, gli aeroporti, le compagnie aeree e la sicurezza del traffico aereo in Svizzera. Grazie alla crescente attenzione di cui sono oggetto le possibili ripercussioni di attacchi informatici contro il traffico aereo, è in aumento anche il numero di disposizioni confluite nella legislazione al fine di ridurre al minimo i rischi informatici. In tale contesto, l'Ufficio è competente per il recepimento di simili disposizioni nel Programma nazionale di sicurezza nell'aviazione (NASP) e provvede alla loro applicazione d'intesa con l'industria di settore.

Dipartimento federale dell'economia

Approvvigionamento economico del Paese

L'Approvvigionamento economico del Paese è un'organizzazione di milizia che dispone di uno stato maggiore e un segretariato a tempo pieno (Ufficio federale per l'approvvigionamento economico del Paese, UFAE). È dotata di un'organizzazione costituita da quadri provenienti dall'economia. Il settore dell'infrastruttura TIC dell'AEP è competente per garantire l'infrastruttura dell'informazione necessaria all'approvvigionamento del Paese (produzione, trasmissione, sicurezza e disponibilità dei dati) e i collegamenti delle telecomunicazioni, in particolare con l'estero. L'AEP definisce le infrastrutture di approvvigionamento di rilevanza sistemica per la Svizzera e stabilisce, al riguardo, una gestione della continuità operativa e delle crisi. Il settore dell'infrastruttura TIC osserva e analizza costantemente i rischi generali inerenti alla sicurezza e alla disponibilità della trasmissione di dati. Adotta, per i casi d'emergenza, provvedimenti atti ad assicurare telecomunicazioni adeguate con gli utenti mobili all'estero importanti per l'approvvigionamento del Paese. Prepara provvedimenti atti a garantire le infrastrutture vitali in materia di informazione e di comunicazione e allestisce la prontezza necessaria a garantire l'approvvigionamento di base. Tutela gli interessi dell'approvvigionamento economico del Paese specifici al settore in seno alle organizzazioni internazionali.

Dipartimento federale degli affari esteri

Il Dipartimento federale degli affari esteri (DFAE) definisce e coordina su mandato del Consiglio federale la politica estera della Svizzera.

La Direzione Politica in seno al Dipartimento segue gli sviluppi in materia di politica di sicurezza all'estero anche al fine di individuare le nuove forme di minaccia e intrattiene contatti con organizzazioni internazionali – quali l'ONU, l'OSCE, l'UE, l'Euro-Atlantic Partnership Council (EAPC) e la NATO – vieppiù interessate, relativamente ai propri compiti in materia di politica di sicurezza, alle minacce provenienti dal cyberspazio. La Direzione Politica cura i contatti con tali organizzazioni e discute la minaccia informatica a livello bilaterale con altri Stati, creando le premesse a livello politico per un contributo della Svizzera nell'ambito della cooperazione per la gestione di tali minacce.

La Direzione del diritto internazionale pubblico si occupa delle implicazioni delle minacce informatiche per il diritto internazionale.

Bilancio della situazione attuale

A livello di Confederazione le strutture finalizzate alla gestione dei rischi informatici sono a tutt'oggi organizzate in modo decentrato. I mezzi impiegati a tale scopo sono relativamente esigui e spesso le insufficienti risorse non consentono di assumere compiti supplementari. I pertinenti compiti sono generalmente attribuiti alle unità organizzative il cui mandato presenta numerose connessioni con il cyberspazio. Questo approccio presenta il vantaggio essenziale di consentire caso per caso di coinvolgere esattamente i servizi necessari per gestire un determinato evento. Poiché ogni attacco alle infrastrutture TIC ha luogo in maniera diversa, tale strutturazione flessibile dell'organizzazione d'emergenza risulta di primaria importanza ed è con-

forme al presupposto che la problematica del cyberspazio non rappresenta un fenomeno nettamente circoscritto e deve pertanto essere trattata nel quadro delle procedure esistenti; inoltre tale approccio favorisce le sinergie ed evita l'istituzione di organi consultivi dispendiosi prima che sia fatta la necessaria chiarezza sui problemi e sulla loro reale entità. Il sistema attuale funziona quindi bene sul piano reattivo. Nonostante esistano determinate capacità anticipatorie e preventive, esse sono tuttavia insufficienti (per es. risorse a livello di personale e finanziarie; scambio di informazioni di intelligence, tecniche e di polizia a sostegno dell'economia, dei gestori di infrastrutture critiche, dei fornitori di prestazioni TIC, dei fornitori di sistemi e della ricerca; analisi dei rischi e conseguente definizione di requisiti in materia di sicurezza; capacità di resistenza). Si constata pertanto che le strutture decentrate a livello di Confederazione devono essere potenziate e che le possibili sinergie devono essere meglio sfruttate affinché sia possibile individuare esaustivamente i rischi informatici e far fronte ad attacchi e turbative informatici di vasta portata.

3.3 Cantoni

Come nell'economia, anche tra i Cantoni si riscontra un'elevata eterogeneità. Dal punto di vista demografico, alcuni Cantoni sono poco più grandi di una città di dimensioni medie. Pure a livello economico e strutturale sono constatabili notevoli differenze. La diversità esistente sotto il profilo delle strutture, delle attività e delle modalità con cui sono forniti i servizi (per es. sanità pubblica, trasporti, energia), sussiste parimenti anche per quanto concerne le esigenze dei singoli Cantoni nell'ambito della gestione dei pericoli e delle minacce. È pertanto evidente che non tutti i Cantoni dispongono, qualitativamente e quantitativamente, delle medesime competenze necessarie per contrastare i rischi, segnatamente nel cyberspazio.

Sul loro territorio, i Cantoni sono responsabili della tutela della sicurezza e dell'ordine pubblici. Soltanto i Cantoni che dispongono di grandi corpi di polizia e intrattengono una stretta collaborazione con l'economia e altri organismi attivi nel settore della sicurezza (per es. dogane e servizi di sicurezza di Paesi limitrofi) sono in grado di anticipare i problemi nel settore della cibercriminalità, di acquisire le informazioni necessarie e di condurre indagini di maggiore spessore. Nessun Cantone, tuttavia, è in grado di svolgere tali attività in maniera sistematica. Tutti i Cantoni devono pertanto poter contare sull'appoggio sussidiario della Confederazione – segnatamente per quanto concerne le necessità di coordinamento e le questioni di intelligence.

I provvedimenti preventivi adottati dai Cantoni al fine di minimizzare i rischi informatici sono una componente necessaria di un approccio globale, poiché ogni Cantone gestisce infrastrutture critiche. La maggior parte dei Cantoni dispone di pertinenti strutture organizzative e di controllo, di incaricati della sicurezza nei diversi servizi interessati, di informatici forensi in seno alla polizia o di cellule di condotta specializzate in caso di crisi. Tuttavia, come a livello di Confederazione, tali mezzi sono spesso insufficientemente coordinati tra loro e non bastano per affrontare in maniera globale i rischi informatici attuali. Il problema è più acuto nei Cantoni di piccole dimensioni, che spesso sono costretti a delegare a terzi specifiche prestazioni.

Va inoltre osservato che le regolamentazioni giuridiche relative alle tecnologie dell'informazione spesso non sono sufficienti o non sono sufficientemente note. I sistemi di classificazione (ad uso interno, confidenziale, segreto) non sono praticamente mai utilizzati e i dati sensibili (dati personali, di polizia o giuridici) sono amministrati in sistemi non sufficientemente protetti.

Già oggi, ad esempio nelle scuole, alcuni Cantoni sensibilizzano la popolazione a fini di prevenzione mediante specifiche campagne d'informazione sui pericoli in Internet. A livello intercantonale sforzi simili sono messi in atto dalla Prevenzione Svizzera della Criminalità. Molti Cantoni tuttavia sono tuttora inattivi o fanno affidamento, in questo settore, sulle iniziative individuali, non coordinate tra loro, di insegnanti o istituzioni preposte alla formazione. A ciò si aggiunge che le offerte di corsi nel settore TIC sono poco sfruttate, in parte perché non note.

Per reagire, tra l'altro, agli attacchi informatici, i Cantoni dispongono di organizzazioni di condotta sotto forma di stati maggiori, oggetto di regolari esercitazioni congiunte con le organizzazioni partner (per es. comandi militari delle regioni territoriali) e in grado di gestire gli effetti di qualsivoglia genere di crisi. Tali stati maggiori non sono però orientati in maniera specifica ai rischi informatici; in caso di attacchi informatici, è probabile che spesso non sarebbero in grado di sostenere in modo competente l'economia e la popolazione.

In vista della concretizzazione della strategia nazionale per la protezione contro i rischi informatici, i Cantoni e la Confederazione hanno a disposizione diversi strumenti atti a fornire preziosi contributi in questo settore:

- la «Casa dei Cantoni», sede di numerose conferenze intercantonali, tra cui la Conferenza dei governi cantonali, conferenze dei direttori cantonali della giustizia, della polizia, della protezione della popolazione, della pubblica educazione, delle finanze, della sanità pubblica ecc. e di ulteriori istituzioni quali la Prevenzione Svizzera della Criminalità;
- la Rete integrata Svizzera per la sicurezza, in corso di allestimento, in seno alla quale saranno coordinate e raggruppate le attività dei Cantoni e della Confederazione nel settore della sicurezza;
- il programma per l'armonizzazione dell'informatica della polizia, volto ad armonizzare tra loro le applicazioni e, pertanto, a facilitare il lavoro della polizia;
- lo SCOCI, che sorveglia il cyberspazio fornendo ai Cantoni informazioni in funzione dell'eventuale avvio di indagini di polizia;

L'associazione Swiss Police ICT, istituita a complemento degli organi e dei consessi statali, consente contatti diretti a livello specialistico tra diversi corpi di polizia e le aziende del settore TIC. Tra le sue iniziative figura il Congresso informatico delle polizie svizzere (*Schweizer Polizei Informatik Kongress*, SPIK), che, fungendo da piattaforma, fornisce un importante contributo allo scambio di informazioni sull'informatica di polizia e sulla gestione di rischi informatici.

3.4 Popolazione

Nell'ambito dell'utilizzazione privata di sistemi d'informazione e di comunicazione, per i necessari provvedimenti di sicurezza sono responsabili in linea di principio i singoli utenti. Di regola questi ultimi impiegano gli strumenti di sicurezza ottenibili sul mercato degli utenti finali (per es. scanner antivirus, router con *firewall* incorporato e cifratura per *wireless local area network*).

Le misure volte a un generale miglioramento della sicurezza dei sistemi TIC privati e le offerte di formazione e di informazione individuale non sono oggetto di coordinamento e non sono orientate a uno standard di sicurezza comune. Una parte crescente della popolazione lavora professionalmente su computer in seno ad aziende o unità amministrative con accesso a dati particolarmente degni di protezione. Per minimizzare i rischi sono pertanto necessari a livello generale una maggiore sensibilizzazione e comportamenti corretti, analogamente a quanto avviene per altre attività di prevenzione.

3.5 Cooperazione internazionale

La Direzione politica del DFAE promuove i contatti internazionali della Svizzera con altri Stati nonché con organizzazioni internazionali che prestano particolare attenzione alle minacce informatiche, creando in tal modo le premesse per una cooperazione della Svizzera in questo ambito a livello internazionale.

La Direzione del diritto internazionale pubblico in seno al DFAE segue gli sviluppi a livello internazionale nell'ambito del diritto internazionale pubblico, segnatamente per quanto concerne la correlazione tra l'utilizzazione di mezzi informatici nel quadro di conflitti interstatali e il diritto internazionale umanitario.

In relazione con diverse iniziative, sono attualmente discusse regolamentazioni internazionali suscettibili di consentire un permanente scambio di informazioni sulle tecnologie, sulle misure di protezione, sull'evoluzione dei rischi e sugli autori di reati nonché una più efficiente assistenza amministrativa e giudiziaria nell'ambito di procedure penali, come pure lo sviluppo e la concretizzazione di misure di sicurezza congiunte.

Nel quadro della concretizzazione dei risultati del Vertice mondiale dell'ONU sulla società dell'informazione, l'Unione internazionale delle telecomunicazioni (UIT)[14] ha assunto il ruolo di organo direttivo dei lavori internazionali nel settore della sicurezza informatica; le attività e gli obiettivi perseguiti dall'Unione in questo ambito sono stati fissati in un'apposita tabella di marcia. La Svizzera partecipa ai lavori.

Negli scorsi anni hanno emanato strategie globali in materia di cibernetica molti Paesi che in passato avevano assunto, a livello bilaterale o multilaterale, impegni unicamente in un numero ristretto di attività e tematiche (per es. la Germania, la Francia e i Paesi Bassi). Per proteggersi dai rischi informatici, alcuni Stati hanno nel frattempo implementato una vasta gamma di strumenti (per es. strategie nazionali nonché apposite misure e centri di difesa dotati di strutture di condotta). Si impone

14 Per le attività dell'UIT nel settore della sicurezza informatica cfr.: www.itu.int/cybersecurity/

un confronto periodico con tali strategie. Segnatamente se si considera che, per quanto concerne le lacune in materia di collaborazione operativa e la mancata percezione, da parte degli attori, degli aspetti inerenti al cyberspazio che rientrano nei rispettivi processi aziendali, produttivi e amministrativi già esistenti, la Svizzera ha optato per un approccio nell'ambito del quale tali handicap non sono destinati a essere colmati semplicemente con la creazione di una piattaforma centrale di coordinamento, bensì, a tutti i livelli, direttamente in seno agli organi e alle strutture di volta in volta competenti e responsabili.

3.6 Basi legali

Le basi legali concernenti il cyberspazio figurano attualmente in una moltitudine di leggi federali e ordinanze. Si tratta essenzialmente di una logica conseguenza dell'incremento dell'interconnessione e dell'impiego dei mezzi di comunicazione: il conseguente accumulo, nei settori di compiti e di responsabilità già esistenti, di aspetti legati al cyberspazio, ha necessitato, di volta in volta per ogni settore interessato, un corrispondente adeguamento delle relative leggi e ordinanze. In questo ambito risultano problematiche la carente armonizzazione e il carattere ancora parzialmente lacunoso delle regolamentazioni.

Le direttive in materia di protezione delle informazioni per l'Amministrazione federale e l'Esercito svizzero sono state riassunte dal Consiglio federale nell'ordinanza del 4 luglio 2007[15] sulla protezione delle informazioni (OPrI), in vigore sino al 31 dicembre 2014. Tuttavia, i Servizi del Parlamento, i tribunali della Confederazione, il Ministero pubblico della Confederazione nonché i servizi cantonali che ricevono informazioni dalla Confederazione non sono o sono compresi soltanto in misura limitata nell'ordinanza.

La sicurezza informatica dell'Amministrazione federale è disciplinata soltanto in maniera sommaria nell'ordinanza del 9 dicembre 2011[16] sull'informatica nell'Amministrazione federale (OIAF). La maggior parte dei principi e delle direttive in materia di sicurezza sono definiti a livello di istruzioni (Istruzioni del Consiglio informatico della Confederazione del 27 settembre 2004[17] sulla sicurezza informatica nell'Amministrazione federale).

La legge federale del 19 giugno 1992[18] sulla protezione dei dati e l'ordinanza del 14 giugno 1993[19] relativa alla legge federale sulla protezione dei dati contengono requisiti minimi concernenti la sicurezza dei dati nell'ambito della gestione di dati personali – requisiti che hanno validità generale e sono applicabili sia alla Confederazione sia ai privati.

La legge federale del 21 marzo 1997[20] sulle misure per la salvaguardia della sicurezza interna, concernente soprattutto misure per l'individuazione e la lotta contro il terrorismo, lo spionaggio, l'estremismo violento e la violenza in occasione di mani-

15 RS **510.411**
16 RS **172.010.58**
17 Il testo delle Istruzioni sulla sicurezza informatica nell'Amministrazione federale è consultabile al sito www.isb.admin.ch/index.html?lang=it > Temi > Sicurezza – Basi per la sicurezza > Istruzioni sulla sicurezza informatica.
18 RS **235.1**
19 RS **235.11**
20 RS **120**

festazioni sportive, fornisce un contributo anche alla sicurezza dell'informazione in seno alle autorità federali, mediante i controlli di sicurezza relativi alle persone in essa previsti.

Una parte dei compiti del servizio informazioni civile della Confederazione è disciplinata nella legge federale del 3 ottobre 2008[21] sul servizio informazioni civile. Tra i compiti di quest'ultimo figurano l'acquisizione di informazioni rilevanti in materia di politica di sicurezza concernenti l'estero, l'analisi di tali informazioni all'attenzione dei Dipartimenti e del Consiglio federale nonché compiti di intelligence nel settore della sicurezza interna.

La legge militare del 3 febbraio 1995[22] (in particolare gli art. 99 e 100) e l'ordinanza del 4 dicembre 2009[23] sul Servizio informazioni dell'esercito (in particolare gli art. 4–6) costituiscono, tra l'altro, la base legale per la cura dei contatti con altri servizi informazioni militari attivi nel campo dei rischi informatici. Inoltre, costituiscono la base legale per il previsto settore Prevenzione e intervento della futura unità organizzativa addetta all'autoprotezione dell'esercito.

Con decisione del 12 maggio 2010, il Consiglio federale ha incaricato il DDPS di elaborare basi legali formali per la protezione e la sicurezza delle informazioni. In futuro la protezione delle informazioni e la sicurezza dell'informazione saranno disciplinate in maniera unitaria in una legge specifica. La futura legge sarà volta a proteggere non soltanto la confidenzialità delle informazioni, bensì anche la loro integrità, disponibilità e verificabilità nonché a garantire la sicurezza dei mezzi con cui le informazioni sono elaborate.

La legge del 30 aprile 1997[24] sulle telecomunicazioni (LTC) assicura, unitamente alle ordinanze d'esecuzione e alle corrispondenti prescrizioni e direttive, che sia offerta «alla popolazione e all'economia una vasta gamma di servizi di telecomunicazione di qualità, competitivi su scala nazionale e internazionale, a prezzi convenienti». Secondo l'articolo 1 LTC (Scopo), il servizio universale deve essere «affidabile». I requisiti qualitativi che devono essere soddisfatti dal servizio universale sono fondati sull'ordinanza del 9 marzo 2007[25] sui servizi di telecomunicazione (OST) e sulle corrispondenti prescrizioni dell'UFCOM. Del rimanente, la LTC è volta ad «assicurare un traffico delle telecomunicazioni esente da interferenze e rispettoso dei diritti della personalità e della proprietà immateriale».

La LTC comprende un capitolo concernente gli «Interessi nazionali importanti» e la OST un capitolo concernente gli «Interessi nazionali preponderanti»; i due capitoli summenzionati contengono diverse disposizioni rilevanti in materia di sicurezza. Sulla base di quest'ultime l'UFCOM ha emanato direttive nelle quali sono raccomandate misure per la sicurezza e la disponibilità delle infrastrutture e dei servizi di telecomunicazione.

Segnatamente per quanto concerne la sicurezza dei servizi di telecomunicazione, va inoltre rilevato che i provvedimenti richiesti per legge concernono soltanto l'ineccepibilità del funzionamento tecnico degli impianti. Benché nella LTC siano previste la «sicurezza e la disponibilità delle infrastrutture e dei servizi di telecomu-

21 RS **121**
22 RS **510.10**
23 RS **510.291**
24 RS **784.10**
25 RS **784.101.1**

nicazione» e benché nella legge e in ulteriori ordinanze siano disciplinati l'affidabilità e il traffico esente da interferenze, nella legislazione non sono state chiaramente definite le modalità esatte con cui debba essere assicurata la protezione dei servizi di telecomunicazione – e pertanto delle telecomunicazioni e delle tecnologie dell'informazione – da rischi esterni e da eventi naturali[26].

La legge dell'8 ottobre 1982[27] sull'approvvigionamento del Paese (LAP) e le relative ordinanze[28] disciplinano «i provvedimenti precauzionali in materia di difesa nazionale economica nonché quelli intesi a garantire l'approvvigionamento del Paese in beni e servizi d'importanza vitale in caso di grave penuria non rimediabile dall'economia stessa». In tale contesto il settore dell'infrastruttura TIC è competente per la garanzia dell'infrastruttura in materia di informazione (per es. sicurezza e trasmissione dei dati) e per le telecomunicazioni con l'estero. Attualmente è in fase di elaborazione un progetto di revisione globale della LAP. Con la nuova impostazione sono previsti il passaggio da un orientamento alla logica della sicurezza a un orientamento alla logica del rischio, l'incremento della capacità di resistenza di settori economici vitali e lo spostamento delle priorità dai beni ai servizi.

La legge federale del 6 ottobre 2000[29] sulla sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni e il Codice di procedura penale (CPP)[30] consentono, in caso di grave sospetto di reato, la registrazione delle comunicazioni postali e delle telecomunicazioni, posta elettronica compresa. Sono inoltre consentiti per legge il rilevamento retroattivo dei dati relativi al traffico e alle fatture nonché l'identificazione degli utenti.

Nel quadro della Convenzione del Consiglio d'Europa sulla cibercriminalità, entrata in vigore in Svizzera il 1° gennaio 2012, gli Stati firmatari si impegnano a punire la frode informatica, il furto di dati, la falsificazione di documenti mediante computer e l'intrusione in sistemi informatici protetti. Nella Convenzione sono disciplinate le modalità di «acquisizione delle prove elettroniche di un reato» nell'ambito di un'inchiesta penale nonché le modalità atte a garantire la sicurezza dei dati raccolti. Alle autorità inquirenti deve essere data la possibilità di accedere rapidamente a dati elaborati elettronicamente, per impedirne la falsificazione o la distruzione nel corso della procedura. Le norme penali del Codice penale[31] (in particolare gli art. 143, 144bis e 272–274, disposizioni inerenti al cosiddetto diritto penale informatico) sono applicabili a casi di cibercriminalità. La Convenzione disciplina inoltre la collaborazione internazionale tra singoli Stati nell'ambito di cause penali (per es. assistenza giudiziaria ed estradizione), in funzione di procedure di cooperazione rapide ed efficienti.

26 *Crisis and Risk Network* (CRN), *Center for Security Studies* (CSS) (2011): «Die rechtlichen Grundlagen zum Schutz Kritischer Infrastrukturen in der Schweiz» («Le basi legali della protezione delle infrastrutture critiche in Svizzera». In elaborazione, in lingua tedesca, su incarico dell'UFPP).

27 RS **531**

28 Ordinanza del 6 luglio 1983 sull'organizzazione dell'approvvigionamento economico del Paese (RS **531.11**); Ordinanza del 2 luglio 2003 sui provvedimenti preparatori in materia di approvvigionamento economico del Paese (RS **531.12**).

29 RS **780.1**

30 RS **312.0**

31 RS **311.0**

3.7 Conclusione

Dall'analisi delle strutture esistenti risulta che in seno all'economia (segnatamente presso i fornitori importanti di prestazioni TIC e i fornitori importanti di sistemi), alla Confederazione e ai Cantoni sussistono numerose capacità che consentono di rilevare gli aspetti inerenti al cyberspazio che rientrano nei settori di compiti e di responsabilità esistenti e di individuare i corrispondenti rischi. Sono pure disponibili approcci e documenti programmatici per un'ottimizzazione della situazione in materia di sicurezza informatica. Sono inoltre operativi organismi che consentono lo scambio di informazioni e il coordinamento tra i singoli attori. Le grandi aziende, i corpi di polizia cantonali e la Confederazione dispongono di servizi con apposite conoscenze specialistiche. Presso diversi istituti di ricerca svizzeri sono in corso progetti concernenti la sicurezza informatica nonché l'individuazione e la valutazione dei rischi informatici. Nelle procedure, tuttavia, spesso non sono coinvolti tutti i responsabili a tutti i livelli, a partire dal livello tecnico-operativo sino al livello strategico-politico; talvolta, addirittura, taluni responsabili si astengono consapevolmente da una partecipazione.

Da colloqui svolti con rappresentanti dell'economia e gestori di infrastrutture critiche risulta, tra l'altro, che nella gestione di attacchi informatici sussistono forti lacune e carenze. Ad esempio, si riscontrano notevoli differenze, ai diversi livelli, riguardo alle capacità di reazione e individuazione, spesso insufficienti, soltanto parzialmente coordinate e in buona parte determinate da interessi commerciali. Le misure di ottimizzazione adottate o pianificate per la sicurezza informatica rispecchiano differenti valutazioni dei rischi e presentano una corrispondente eterogeneità. Non conducono pertanto a procedure armonizzate tra loro e lo scambio di informazioni tra gli attori fatica a funzionare ed è spesso limitato alla rispettiva azienda.

Le carenze in materia di sicurezza informatica sono spesso ricondotte alla mancanza di pertinenti risorse finanziarie e di personale – non soltanto nell'economia, ma anche e in particolare nella Confederazione, in seno alla quale non sono nemmeno disponibili risorse di personale sufficienti per poter adempiere i compiti auspicati in situazione normale. Un altro problema è costituito dal fatto che, secondo la percezione comune, non vi è un numero sufficiente di specialisti TIC.

Per quanto concerne la cooperazione tra l'economia e le autorità, sono stati individuati diversi punti deboli a livello di ripartizione dei compiti, delle capacità e delle competenze, con conseguenti necessità di chiarificazione. Dall'analisi delle strutture esistenti risulta in particolare che l'Amministrazione federale non dispone in misura sufficiente dei mezzi necessari per l'individuazione dei rischi e per una valutazione globale – all'attenzione degli ambienti economici, dei gestori di infrastrutture critiche e delle autorità – delle informazioni e delle analisi della situazione. Ne consegue uno scambio di informazioni carente che non consente di realizzare un livello sufficiente di protezione contro i rischi informatici. Anche la collaborazione con i fornitori sensibili di prestazioni TIC e con i fornitori sensibili di sistemi non è sufficientemente sistematizzata. Si impongono inoltre un miglior sfruttamento delle sinergie tra gli organi amministrativi e una verifica dell'efficienza dei sistemi e dei canali di comunicazione necessari per lo scambio di informazioni. Infine, mancano analisi dei rischi che consentano, tra l'altro, di definire le esigenze in materia di sicurezza nell'ambito delle infrastrutture TIC e una conseguente ripartizione delle responsabilità e dei costi supplementari.

Internet è ancora oggi troppo spesso considerata da una larga parte degli attori come una zona di non-diritto e la sicurezza quotidiana dell'impiego della rete è garantita in maniera insufficiente. Segnatamente le autorità di perseguimento penale non dispongono sempre di mezzi e capacità sufficienti per poter perseguire efficientemente le infrazioni. Inoltre, nel settore della minimizzazione dei rischi informatici non vige sufficiente chiarezza riguardo alle interfacce e allo scambio di informazioni con gli organi di prevenzione; non è di conseguenza possibile realizzare un *mix* di misure preventive e repressive orientato agli obiettivi.

In generale, si può concludere che il sistema attuale non è praticamente in grado di contrastare attivamente attacchi informatici mirati e di notevole entità né, in caso di conseguenze gravi, di porvi rimedio con la necessaria rapidità. Nell'ambito dei colloqui, i rappresentanti di aziende e i gestori di infrastrutture critiche hanno pertanto formulato l'auspicio che siano definite e concretizzate, assieme alle autorità, prescrizioni minime in materia di sicurezza e che le misure volte all'ottimizzazione della situazione in materia di sicurezza, alla gestione di attacchi e alla sensibilizzazione siano meglio coordinate. Inoltre, si chiede alla Confederazione di istituzionalizzare lo scambio di informazioni, di mettere a disposizione una rappresentazione globale aggiornata della situazione cibernetica e di assicurare un più esteso appoggio sussidiario.

Le attuali variegate basi legali rispecchiano la specificità degli aspetti inerenti al cyberspazio che di volta in volta rientrano in settori di compiti e di responsabilità già definiti. Di conseguenza, una regolamentazione in un'unica legge speciale sul cyberspazio rappresenterebbe una soluzione inadeguata. Gli attuali atti normativi vanno pertanto costantemente adeguati, nel quadro del rispettivo campo di applicazione, all'evoluzione del cyberspazio.

Del rimanente, si constata che l'interconnessione e la collaborazione a livello internazionale per la minimizzazione dei rischi informatici sono in costante crescita.

Sulla base delle summenzionate necessità di intervento, la presente Strategia comprende una serie di proposte di misure concrete, illustrate qui di seguito.

4 Dispositivo per la protezione contro i rischi informatici

4.1 Obiettivi di ordine superiore

Il Consiglio federale ha preso atto che la problematica del cyberspazio è primariamente un fenomeno attinente a compiti e responsabilità già definiti a livello di autorità, economia e società. La minimizzazione dei rischi informatici compete di conseguenza agli attori di volta in volta responsabili.

Il Consiglio federale intende promuovere, a favore dell'economia, della politica e della popolazione svizzera, le opportunità e i vantaggi che offre il cyberspazio, ma è anche consapevole che gli sviluppi in questo settore sono accompagnati da rischi e dalla necessità di corrispondenti misure di minimizzazione.

Le misure descritte nella presente Strategia nazionale e la regolamentazione della loro concretizzazione concernono i tempi di pace; il caso di guerra è esplicitamente escluso dal campo di applicazione della presente Strategia.

Nel quadro della Strategia nazionale per la protezione della Svizzera contro i rischi informatici, il Consiglio federale persegue i seguenti obiettivi di ordine superiore:

- i rischi nel cyberspazio devono essere individuati e valutati tempestivamente affinché possano essere adottate, in collaborazione con tutti gli attori interessati dell'economia, della politica e della società, pertinenti misure di minimizzazione e prevenzione dei rischi;
- la resistenza (resilienza) delle infrastrutture critiche nei confronti di attacchi informatici – vale a dire la capacità di garantire il ripristino, in tempi il più possibile brevi, del funzionamento normale – deve essere incrementata in collaborazione con i rispettivi gestori, con i fornitori di prestazioni TIC, con i fornitori di sistemi e in coordinamento con il programma diretto dalla Confederazione per la protezione delle infrastrutture critiche (programma «PIC»);
- devono essere assicurati e, laddove necessario, creati, i presupposti per una riduzione efficace dei rischi informatici, in particolare per quanto concerne la cibercriminalità, lo spionaggio informatico e il sabotaggio informatico.

Tali obiettivi possono essere conseguiti in diversi modi nell'ambito delle attuali strutture decentralizzate. Un comportamento improntato alla *responsabilità individuale* nei vari settori economici nonché il *dialogo* e la *cooperazione* tra l'economia e le autorità costituiscono in ogni caso altrettanti presupposti essenziali. La *trasparenza* e la *fiducia* necessarie devono essere realizzate mediante un permanente *scambio di informazioni* e lo Stato deve intervenire soltanto nei casi in cui sono in gioco interessi pubblici, agendo conformemente al principio della *sussidiarietà*.

La gestione dei rischi informatici è un compito trasversale che va assunto dall'economia, dai gestori di infrastrutture critiche, dai fornitori di prestazioni TIC, dai fornitori di sistemi e dalle autorità a livello cantonale e federale. Tali attori devono essere intesi come componenti di un processo aziendale, produttivo o amministrativo integrale. Tutti gli attori devono essere coinvolti nel processo, dal livello tecnico-amministrativo sino al livello politico-strategico. Una gestione efficace dei pericoli e delle minacce provenienti dalla «rete» ha quale premessa la consapevolezza che nei compiti e nelle responsabilità attuali delle autorità, dell'economia e della popolazione sono compresi aspetti attinenti al cyberspazio. Ogni componente organizzativa a livello politico, economico e sociale è responsabile dell'individuazione di tali aspetti e deve rispondere dell'integrazione – e pertanto della riduzione – dei conseguenti rischi nei rispettivi processi. A tal fine, le attuali strutture decentralizzate devono essere dotate, se necessario rinforzandole, della capacità di far fronte agli specifici aspetti attinenti al cyberspazio compresi nei rispettivi compiti e nelle rispettive responsabilità.

4.2 Condizioni quadro e presupposti

Basi legali

Poiché la problematica del cyberspazio rientra in compiti e responsabilità già disciplinati, sarà necessario, in una prima fase, verificare se è sufficientemente inclusa nelle attuali basi legali. In caso di necessità d'intervento, si tratterà innanzitutto di integrare le pertinenti disposizioni nella legislazione vigente o pianificata (per es. legge sul servizio informazioni). Le regolamentazioni rese necessarie dal cyberspa-

zio andranno pertanto strettamente coordinate con progetti legislativi in corso e previsti (per es. legislazione in materia di sicurezza delle informazioni, legge sul servizio informazioni, legge sull'approvvigionamento del Paese, LSCPT, Convenzione sulla cibercriminalità ecc.).

L'adeguamento delle basi legali alla rapida evoluzione del cyberspazio e dei rischi informatici costituisce un processo permanente. Laddove necessario, per le questioni complesse saranno allestite perizie giuridiche. Le basi legali del perseguimento penale (segnatamente il Codice penale, il Codice di procedura penale, le leggi cantonali sulla polizia e il disciplinamento delle competenze) e delle unità attive nell'ambito della prevenzione (Servizio delle attività informative della Confederazione e corpi di polizia cantonali) devono essere verificate in ordine alle sfide specifiche del cyberspazio (per es. distanze geografiche, rapidità e caducità delle tracce e, di conseguenza, possibilità di utilizzo in tribunale degli indizi). Si tratta innanzitutto di capire in che modo possono essere tempestivamente individuati e impediti reati eseguibili mediante reti elettroniche e come possono essere svolte efficacemente le relative indagini. Particolare attenzione dovrà essere prestata alla ponderazione tra gli interessi in materia di protezione della personalità e le esigenze in tema di sicurezza pubblica e interna.

Vanno inoltre sottoposte a verifica le responsabilità dei gestori di reti e di sistemi informatici, le responsabilità dei fornitori di prestazioni e di infrastrutture di rete e infine, eventualmente, le responsabilità di ulteriori attori attivi in Internet. Anche in questo caso, al fine di consentire la cooperazione per la protezione sia di infrastrutture di informazione e di comunicazione sia di privati e di attori pubblici, va effettuata una ponderazione giuridica e politica tra gli obblighi e i diritti di tutte le parti interessate rispettivamente in materia di protezione dei dati e in materia di elaborazione dei dati.

Scambio di informazioni e prevenzione

Devono essere individuati e analizzati gli aspetti e i rischi del cyberspazio che rientrano in compiti e responsabilità già disciplinati. Ciò incombe di volta in volta alle pertinenti autorità e presuppone contatti e scambi con attori dell'economia e della società. In questo ambito, la stretta collaborazione tra attori pubblici e privati sotto forma di PPP[32] è stata confermata e giudicata adeguata dal Consiglio federale nel 2003 e 2007 e va pertanto ulteriormente perseguita.

Per allestire una rappresentazione globale della situazione, le pertinenti informazioni, tecniche e non, devono essere acquisite, analizzate e valutate in maniera coordinata. Le conoscenze risultanti da tali ricerche sono in seguito messe a disposizione di tutti gli attori. In questo ambito è importante approfondire ulteriormente nel quadro della centrale MELANI il già esistente partenariato tra capacità di intelligence e capacità tecniche a favore dei gestori di infrastrutture critiche e dell'economia.

Dallo Stato ci si aspetta che disponga di mezzi atti a consentirgli di appoggiare in via sussidiaria gli organismi responsabili qualora quest'ultimi venissero a trovarsi nell'impossibilità di adottare autonomamente le misure necessarie.

32 Cfr. DCF 2003 e 2007

Collaborazione con l'estero

I rischi informatici non si fermano ai confini dei singoli Stati. Per un'analisi dei rischi fondata e realistica è essenziale una cooperazione internazionale. È pertanto necessario intensificare lo scambio di informazioni concernenti esperienze, lavori di ricerca e di sviluppo, singoli eventi nonché la formazione e le esercitazioni.

Gli sforzi volti a proteggere da abusi il cyberspazio mediante regole e standard convenuti a livello internazionale sono nell'interesse della Svizzera in quanto Paese tecnologicamente altamente evoluto. La Svizzera partecipa pertanto, nel quadro di organizzazioni internazionali statali e non statali, all'elaborazione di soluzioni a livello politico, di possibilità di cooperazione e di accordi internazionali per la riduzione dei rischi informatici. I consessi di carattere globale sono la sede ideale per tematizzare i problemi strutturali inerenti all'interconnessione globale nonché la creazione e la promozione di standard, regole e norme internazionali. Gli interessi dell'economia, delle autorità e della società svizzere vanno di conseguenza promossi sin dalle prime fasi a partire da questo livello.

In conformità con quanto sopra esposto, il nostro Paese contribuisce agli sforzi volti a estendere la cooperazione nella gestione congiunta delle crisi. Una più intensa cooperazione nel settore dell'intelligence, nello scambio di informazioni con i fornitori determinanti di prestazioni TIC e con i fornitori determinanti di sistemi, nelle attività di analisi tecniche e nel perseguimento penale (assistenza giuridica e amministrativa) consentirà alla Svizzera di incrementare la propria capacità d'azione e l'efficacia delle proprie misure. In questo contesto è indispensabile coinvolgere ai rispettivi livelli anche attori non statali quali associazioni, organizzazioni d'interesse, gruppi di lavoro internazionali o organizzazioni non governative.

Perseguimento penale

Nel quadro del perseguimento penale, è necessario acquisire informazioni utilizzabili in tribunale in merito a reati nel cyberspazio, perseguire gli autori, punire i reati e garantire la collaborazione con autorità estere di perseguimento penale. Segnatamente in relazione con le priorità della strategia della Confederazione per combattere la criminalità nel periodo 2012–2015, definite dal Consiglio federale, le attività di perseguimento penale devono essere focalizzate sugli attacchi informatici in quanto reati gravi contro la protezione dello Stato nonché forma specifica di criminalità economica.

Esercito

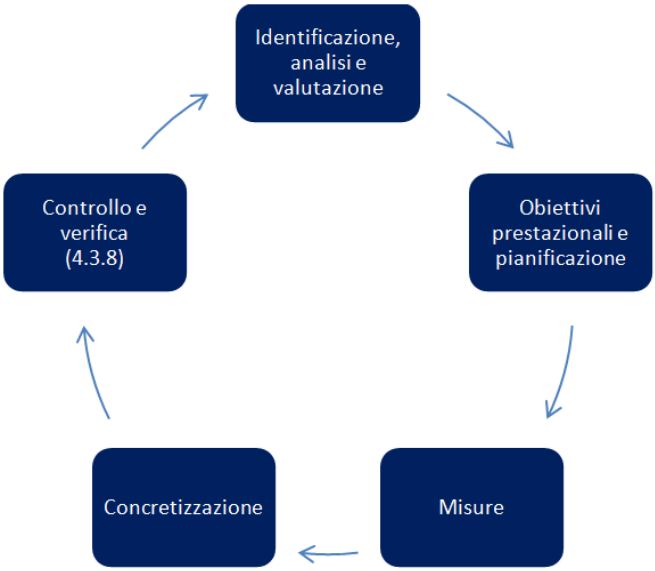
L'esercito, in quanto riserva strategica della Svizzera, deve assicurare l'adempimento dei suoi compiti in tutte le forme di impiego. Adotta pertanto misure volte alla protezione delle proprie infrastrutture e assicura la condotta in tempo di crisi mediante infrastrutture resistenti ai guasti. Su richiesta, le esperienze acquisite nelle attività dell'esercito e l'accesso alle summenzionate infrastrutture resistenti ai guasti possono essere messi a disposizione delle altre autorità e dei gestori di infrastrutture critiche.

In tal senso l'esercito è strettamente interconnesso con il settore civile e deve pertanto armonizzare con le altre autorità le misure di concretizzazione nell'ambito della realizzazione delle sue capacità di minimizzazione dei rischi informatici.

4.3 Campi d'azione e misure

Nell'ambito della concretizzazione delle misure di ottimizzazione della protezione della Svizzera contro i rischi informatici andranno debitamente contemplate l'opportunità, la proporzionalità e l'efficacia politiche ed economiche; inoltre, bisognerà tener conto della struttura decentralizzata dello Stato e dell'economia del Paese. Ciò presuppone che tutti gli attori sappiano quali aspetti inerenti al cyberspazio rientrano nei rispettivi compiti e nelle rispettive responsabilità e assieme a quali partner dell'economia, della politica e della società devono essere adottate corrispondenti misure di minimizzazione dei rischi.

Nel seguito sono illustrati i campi d'azione e le misure volti a ridurre i rischi informatici. I campi d'azione sono definiti sulla base di un ciclo di gestione dei rischi e di protezione[33]. Tale ciclo consta di cinque sottoprocessi (identificazione, analisi e valutazione; obiettivi prestazionali e pianificazione; misure; concretizzazione; controllo e verifica), di cui soltanto i primi tre (identificazione, analisi e valutazione; obiettivi prestazionali e pianificazione; misure) sono contemplati nella presente Strategia per ogni singolo campo d'azione.



La concretizzazione delle misure incombe agli attori competenti dell'Amministrazione, dell'economia e della società. Le fasi di concretizzazione sono descritte soltanto nei casi in cui sono coinvolti organi della Confederazione. Al riguardo, si tratta essenzialmente delle prime fasi di concretizzazione a livello di Confederazione

33 Il ciclo di gestione dei rischi e di protezione qui esposto è in gran parte analogo al ciclo di protezione implementato nell'ambito della Strategia nazionale per la protezione delle infrastrutture critiche (in seno all'UFPP) e utilizzato nel quadro dell'approvvigionamento economico del Paese.

per l'avvio della pianificazione della concretizzazione a tutti i livelli, in collaborazione con i rispettivi partner dell'Amministrazione, dell'economia e della società.

Il controllo e la verifica delle misure concretizzate incomberà, nell'ambito di una stretta collaborazione con gli organi responsabili, al futuro apposito organo di coordinamento.

4.3.1 Campo d'azione 1: Ricerca e sviluppo

Identificazione, analisi e valutazione

I nuovi rischi in relazione con la problematica del cyberspazio devono essere oggetto di un'apposita attività di ricerca affinché le necessarie decisioni in ambito politico, economico e scientifico siano adottate tempestivamente e con cognizione di causa. La ricerca sarà focalizzata sui trend tecnologici, sociali, politici ed economici suscettibili di presentare ripercussioni a livello di rischi informatici. Tanto la ricerca quanto lo sviluppo sono avviati o eseguiti in maniera autonoma dagli attori in ambito scientifico e a livello di economia, società e autorità.

Obiettivi prestazionali e pianificazione

Devono sussistere le capacità necessarie per identificare, analizzare e valutare, nel rispettivo settore di responsabilità, i rischi inerenti alla problematica del cyberspazio. Tale obiettivo deve essere perseguito in collaborazione con i responsabili della «Strategia per una società dell'informazione in Svizzera» (Dipartimento federale dell'ambiente, dei trasporti, dell'energia e delle comunicazioni [DATEC]-UFCOM), con i responsabili della «Strategia nazionale per la protezione delle infrastrutture critiche» (DDPS-UFPP) nonché con i responsabili della «Gestione dei rischi Confederazione».

Misure

Misura 1

Gli organi federali responsabili intrattengono regolari scambi tra di loro e con attori esterni all'Amministrazione federale riguardo agli sviluppi attuali e agli sviluppi da sottoporre a ricerca in relazione con i rischi informatici. Inoltre, se necessario, pertinenti attività di ricerca sono eseguite *intra muros* dagli organi federali responsabili o da essi assegnate all'esterno.

Concretizzazione

I singoli organi federali sono responsabili per la ricerca di settore nella propria sfera di competenza. Il «Comitato direttivo formazione, ricerca e tecnologia» incarica gli uffici di elaborare, per i rispettivi ambiti politici, programmi pluriennali in progress concernenti la ricerca di settore («concetti di ricerca»). Tali concetti di ricerca contengono informazioni sulle priorità pianificate nell'ambito della ricerca di settore e sono allestiti in considerazione, in particolare, delle attuali priorità di ricerca presso gli istituti universitari, dei programmi di promovimento svolti dal *Fondo nazionale svizzero* su mandato della Confederazione nonché delle attività della Commissione per la tecnologia e l'innovazione.

4.3.2 Campo d'azione 2: Analisi dei rischi e della vulnerabilità

Identificazione, analisi e valutazione

Tutte le autorità amministrative competenti, i gestori di infrastrutture critiche, i fornitori di prestazioni TIC, i fornitori di sistemi e le associazioni (nel senso di una concentrazione delle forze in seno al rispettivo ramo economico) devono identificare, al loro livello, i rischi risultanti dal cyberspazio nonché analizzarne e valutarne la probabilità di insorgenza e le potenziali ripercussioni.

Obiettivi prestazionali e pianificazione

Gli attori responsabili della politica, dell'economia e della società devono disporre dei mezzi e delle capacità necessarie per poter individuare tempestivamente i rischi informatici, valutare la situazione di minaccia e analizzarne le implicazioni per il rispettivo settore, sotto forma di analisi congiunte dei rischi. La concretizzazione ha luogo in collaborazione con i responsabili della «Gestione dei rischi Confederazione», con i responsabili della «Strategia nazionale per la protezione delle infrastrutture critiche» nonché con i responsabili dei lavori relativi al progetto «Rischi Svizzera».

Misure

Misura 2

A tutti i livelli (Confederazione, Cantoni e gestori di infrastrutture critiche) devono essere allestite analisi dei rischi e della vulnerabilità, con il coinvolgimento dei fornitori di prestazioni TIC e dei fornitori di sistemi. Ciò comprende la verifica autonoma e regolare dei sistemi da parte dei gestori. L'elaborazione di analisi (settoriali) dei rischi necessita una stretta collaborazione tra le autorità *(Dipartimento federale dell'economia [DFE], Dipartimento federale delle finanze [DFF], DATEC).*

Concretizzazione

Nel quadro della revisione della LAP, il DFE adegua le proprie competenze per poter eseguire, con tutti i sottosettori dell'approvvigionamento economico del Paese (UFAE), analisi dei rischi e della vulnerabilità orientate alle necessità, coinvolgendo in funzione delle circostanze le autorità competenti (in primo luogo DATEC e DFF). I gestori di infrastrutture critiche non compresi nel raggio d'azione dell'approvvigionamento economico del Paese devono essere integrati nelle pertinenti procedure tramite le autorità di volta in volta competenti, le quali, in caso di necessità, adeguano di conseguenza la rispettiva legislazione specialistico-settoriale. Le analisi dei rischi e della vulnerabilità devono aver luogo secondo un approccio il più possibile unitario. Nella concretizzazione dei risultati vanno coinvolte le autorità competenti (in primo luogo quelle in seno al DATEC e al DFF).

Il consolidamento dei risultati in un'analisi globale della situazione di minaccia ha luogo in collaborazione con la centrale MELANI.

Misura 3

Le autorità, i gestori di infrastrutture critiche e gli istituti di ricerca verificano, con il coinvolgimento dei fornitori di prestazioni TIC e dei fornitori di sistemi, la vulnera-

bilità delle rispettive infrastrutture TIC. Tale verifica comprende i punti deboli a livello di sistemi, di organizzazione e di caratteristiche tecniche. I risultati sono consolidati e valutati; in caso di interesse pubblico, sono pubblicati in relativi rapporti[34] *(DFE, DFF, DDPS, DATEC)*.

Concretizzazione

L'ODIC allestisce entro la metà del 2015, in collaborazione con i fornitori di prestazioni TIC, un documento programmatico («concetto») concernente la verifica periodica delle infrastrutture TIC dell'Amministrazione federale volta a individuare i punti deboli a livello di sistemi, di organizzazione e di caratteristiche tecniche. Tale concetto è concretizzato dai competenti fornitori di prestazioni e dalle persone di volta in volta responsabili in seno alle Segreterie generali dei Dipartimenti.

Il summenzionato concetto può essere trasmesso – con valore di raccomandazione oppure a fini di supporto – all'economia e ai gestori di infrastrutture critiche per l'esecuzione delle proprie verifiche.

Il consolidamento dei risultati in un'analisi globale della situazione di minaccia ha luogo in collaborazione con la centrale MELANI.

4.3.3 Campo d'azione 3: Analisi della situazione di minaccia

Identificazione, analisi e valutazione

Gli eventi di importanza nazionale e di particolare rilievo devono essere individuati, valutati e analizzati. I relativi risultati devono essere elaborati e messi a disposizione dei settori di volta in volta responsabili, conformemente ai rispettivi livelli.

Obiettivi prestazionali e pianificazione

Gli attori della politica, dell'economia e della società devono disporre dei mezzi e delle capacità necessarie per poter individuare, valutare e analizzare la situazione di minaccia in stretta collaborazione tra loro nonché unitamente alle autorità competenti. Per quanto necessario, va valutata l'opportunità di concedere ai servizi responsabili, ai gestori di infrastrutture critiche e all'economia un'autorizzazione in materia di notifica.

Misure

Misura 4

Da fonti pubbliche e non pubbliche sono acquisite, valutate e analizzate informazioni di intelligence, di polizia, forensi e tecniche sulla situazione di minaccia e in materia di rischi nel cyberspazio. Nel quadro del modello di PPP della centrale MELANI, tali informazioni sono centralizzate, globalmente valutate, analizzate, integrate in una rappresentazione costantemente aggiornata della situazione e provviste di indicazioni relative ai possibili sviluppi della situazione. I risultati sono

34 I metodi e prodotti crittografici per la protezione di informazioni classificate (CONFIDENZIALE o SEGRETO) secondo l'ordinanza sulla protezione delle informazioni devono essere messi a disposizione dal servizio specializzato del DDPS competente per l'ambito della crittologia.

messi a disposizione degli attori responsabili di volta in volta interessati *(DFF, DDPS)*.

Concretizzazione

Ai fini della gestione e dell'ulteriore elaborazione di eventi in relazione con i mezzi TIC e determinanti per la protezione dello Stato, nell'attività del SIC devono essere inglobate le componenti del suo mandato inerenti al cyberspazio. Questo obiettivo è perseguito con il coinvolgimento della BAC in qualità di fornitore di prestazioni tecniche a favore del SIC e, se opportuno, con il coinvolgimento del SIM. I risultati confluiscono, per il tramite della centrale MELANI, nell'analisi globale della situazione di minaccia.

Le capacità tecniche per la sorveglianza costante (24/7) delle reti della Confederazione vanno sviluppate presso i fornitori di prestazioni (CERT) entro la fine del 2015. I risultati confluiscono, per il tramite della centrale MELANI, nell'analisi globale della situazione di minaccia.

La centrale MELANI intensifica lo scambio di informazioni su base volontaria con i gestori di infrastrutture critiche e con i suoi partner internazionali. Ne conseguono un maggior fabbisogno di capacità forensi, un crescente flusso di informazioni e un'intensificazione dello scambio di informazioni con i gestori di infrastrutture critiche e con l'economia. Le capacità e le risorse supplementari sono create mediante una collaborazione sistematica con i fornitori determinanti di prestazioni TIC e con i fornitori determinanti di sistemi.

Misura 5

La Confederazione, i Cantoni e i gestori di infrastrutture critiche elaborano gli eventi rilevanti e verificano le possibilità di ulteriore sviluppo delle rispettive misure di gestione di eventi in relazione con i rischi informatici. Questo obiettivo è perseguito in linea di principio individualmente nel quadro del rispettivo mandato. Nel quadro della PPP della centrale MELANI, le conseguenti informazioni sono centralizzate, globalmente valutate e analizzate e i risultati sono messi a disposizione degli attori di volta in volta interessati, segnatamente degli attori competenti per le analisi dei rischi e della vulnerabilità *(DFF, DDPS)*.

Concretizzazione

La centrale MELANI intensifica lo scambio di informazioni su base volontaria con e tra i gestori di infrastrutture critiche, i fornitori determinanti di prestazioni TIC e i fornitori determinanti di sistemi e sostiene l'elaborazione di eventi rilevanti. Ne conseguono un maggior fabbisogno di capacità forensi, un crescente flusso di informazioni e un'intensificazione dello scambio di informazioni con i gestori di infrastrutture critiche e con l'economia.

Ai fini della gestione e dell'ulteriore elaborazione di eventi in relazione con i mezzi TIC e determinanti per la protezione dello Stato, nell'attività del SIC devono essere inglobate le componenti del suo mandato inerenti al cyberspazio. Questo obiettivo è perseguito con il coinvolgimento della BAC in qualità di fornitore di prestazioni tecniche a favore del SIC. I risultati confluiscono, per il tramite della centrale MELANI, nell'analisi globale della situazione di minaccia.

Le capacità tecniche per la sorveglianza costante (24/7) delle reti della Confederazione vanno sviluppate presso i fornitori di prestazioni (CERT). I risultati confluiscono, per il tramite della centrale MELANI, nell'analisi globale della situazione di minaccia.

scono, per il tramite della centrale MELANI, nell'analisi globale della situazione di minaccia.

Misura 6

A livello nazionale va gestita una panoramica per quanto possibile esaustiva dei casi (casi penali) e va assicurato il coordinamento nei casi di portata intercantonale. Le informazioni evinte dalla panoramica dei casi e i dati concernenti casi intercorrelati, segnatamente se risultanti dall'analisi tecnico-operativa del perseguimento penale nell'ambito delle procedure penali, devono confluire nella rappresentazione globale della situazione *(Dipartimento federale di giustizia e polizia (DFGP).*

Concretizzazione

Il DFGP, in collaborazione con i Cantoni, sottopone entro la fine del 2016 un documento programmatico («concetto») per la gestione di una panoramica globale dei casi (casi penali). Il concetto comprende anche la chiarificazione delle interfacce con ulteriori attori nell'ambito della minimizzazione dei rischi informatici, il coordinamento con i lavori per la rappresentazione della situazione nonché le risorse e gli adeguamenti giuridici necessari, a livello di Confederazione e Cantoni, per la concretizzazione del concetto medesimo.

Le informazioni evinte dalla panoramica dei casi (casi penali) e i dati concernenti casi intercorrelati risultanti dall'analisi tecnico-operativa del perseguimento penale nell'ambito delle procedure penali confluiscono, per il tramite della centrale MELANI, nell'analisi globale della situazione di minaccia.

4.3.4 Campo d'azione 4: Creazione di competenze

Identificazione, analisi e valutazione

Tutti gli attori a livello di economia, società e autorità devono essere sensibilizzati e formati in materia di rischi informatici, affinché possano individuare i rischi e adottare misure volte alla minimizzazione della loro esposizione ai rischi.

Obiettivi prestazionali e pianificazione

Per incrementare la consapevolezza in merito ai rischi informatici e alla loro gestione corretta, devono essere elaborate, tenendo conto di approcci e iniziative già noti, misure di sensibilizzazione e di formazione che saranno attuate nei rispettivi ambiti di competenza. Tale obiettivo è realizzato nel quadro di uno stretto coordinamento nell'ambito della concretizzazione della «Strategia per una società dell'informazione in Svizzera».

Misure

Misura 7

Deve essere allestita una panoramica delle attuali offerte in materia di creazione di competenze, quale base per individuare le lacune esistenti e informare gli attori dell'economia, dell'amministrazione e della società civile, in maniera conforme alle esigenze, riguardo alle offerte di formazione concernenti la gestione dei rischi informatici *(DFF, DATEC, DFAE).*

Concretizzazione

L'organo di coordinamento per la concretizzazione della strategia appoggia l'elaborazione della panoramica delle offerte di formazione, formali e informali, atte a rafforzare in maniera conforme alle esigenze le competenze nel settore informatico; inoltre, individua gli esempi di elevata qualità e le lacune a livello di offerte. L'elaborazione della panoramica e l'individuazione degli esempi di elevata qualità e delle lacune in materia di offerte hanno luogo entro la fine del 2013 in coordinamento, da un lato, con i lavori di concretizzazione della «Strategia del Consiglio federale per una società dell'informazione in Svizzera» e, dall'altro, con i Cantoni. Il DFAE provvede a comunicare informazioni concernenti le offerte disponibili nel quadro di organizzazioni e istituzioni internazionali. Le offerte in materia di creazione di competenze e gli esempi di elevata qualità sono pubblicati in forma adeguata entro la fine del 2014.

Misura 8

Sono avviati i lavori concernenti le lacune individuate a livello di offerte in materia di creazione di competenze per la gestione dei rischi informatici ed è promosso l'incremento dell'impiego delle attuali offerte di elevata qualità *(DFF, DATEC)*.

Concretizzazione

L'organo di coordinamento per la concretizzazione della strategia coordina in sintonia con la «Strategia per una società dell'informazione in Svizzera», con i Cantoni e con l'economia, l'elaborazione – entro la metà del 2014 – di un concetto di concretizzazione finalizzato, da un lato, a un maggiore impiego di offerte esistenti e di elevata qualità nell'ambito della formazione in materia di gestione dei rischi informatici e, dall'altro, alla creazione di nuove offerte di formazione, formali e informali, in tema di creazione di competenze. Le offerte comprendono i livelli amministrativi, tecnici e strategici e consistono, per esempio, in campagne e guide per la formazione.

4.3.5 Campo d'azione 5: Relazioni e iniziative internazionali

Identificazione, analisi e valutazione

Conformemente ai principi definiti dall'ONU nel quadro del Vertice mondiale dell'ONU sulla società dell'informazione (WSIS) tenutosi in due fasi a Ginevra (2003) e a Tunisi (2005), l'Internet governance[35] funziona secondo il cosiddetto approccio «multi-stakeholder», con il coinvolgimento di una gamma variegata di gruppi d'interesse e autorità amministrative agenti nei rispettivi ruoli. Tutti gli attori rilevanti e competenti (autorità, economia e società) possono partecipare a questo processo. Le condizioni per l'utilizzo e la gestione di Internet sono fondamentali per le opportunità, gli obblighi e i doveri di cittadini, imprese e Stati in un mondo interconnesso, libero e competitivo. A causa della natura globale e molteplice di Internet i disciplinamenti possono essere decisi e imposti unilateralmente da singoli Stati soltanto in misura estremamente limitata. La medesima considerazione si applica anche alla formulazione di politiche e cosiddette «migliori prassi» nonché all'istitu-

35 *Tunis Agenda for the Information Society* (WSIS 2005), § 34.

zione di organismi incaricati di elaborare norme che, di fatto, siano standard di sicurezza per prodotti e processi.

In particolare, gli interessi dei piccoli Stati come la Svizzera possono essere tutelati globalmente solo grazie a una diplomazia «proattiva» e una buona e coordinata comunicazione delle proprie posizioni nella rete di contatti globale.

Obiettivi prestazionali e pianificazione

Un approccio globale è la modalità ideale per affrontare i problemi strutturali inerenti all'interconnessione globale. Di conseguenza, gli interessi dell'economia, della società e delle autorità svizzere vanno, per quanto possibile, presentati in maniera coordinata.

La gestione delle risorse chiave di Internet continuerà ad avere luogo secondo principi liberali, ma dovrà essere meno dominata dagli interessi del limitato numero di Paesi che ospitano l'industria di Internet. Le linee direttrici comuni devono essere emanate e imposte congiuntamente dai governi. La stabilità e la disponibilità di Internet per tutti dovrà essere garantita e la libertà dei cittadini e delle imprese in Internet non dovrà essere limitata in modo sproporzionato.

In vista dell'implementazione di migliori prassi, politiche e accordi internazionali nel settore degli standard di sicurezza e di protezione nonché nell'ambito della politica di sicurezza, per la tutela degli interessi svizzeri è indispensabile un intervento coordinato segnatamente degli attori economici e degli organi amministrativi.

Misure

Misura 9

La Svizzera (economia, società, autorità) si impegna attivamente e, per quanto possibile, in maniera coordinata a favore di una Internet governance che sia compatibile con le concezioni svizzere in materia di libertà e responsabilità (personale), servizio universale, pari opportunità, diritti umani e Stato di diritto. Inoltre, il nostro Paese si impegna a favore di un'internazionalizzazione e una democratizzazione ragionevoli della gestione di Internet. Grazie alla sua esperienza nel processo decisionale democratico esso apporta un valore aggiunto nel processo di ricerca del consenso *(DATEC, DFAE, DDPS, DFF)*.

Concretizzazione

Il DATEC rappresenta la Svizzera e gli interessi del Paese nelle procedure e nelle istituzioni determinanti nel settore dell'Internet governance. Coordina e definisce gli interessi e le posizioni della Svizzera nel settore dell'Internet governance con gli organi determinanti della Confederazione. Il DATEC gestisce inoltre una piattaforma di scambio ad approccio multi-stakeholder («Piattaforma tripartita»), a disposizione di tutti gli attori interessati dell'amministrazione svizzera, dell'economia privata, della società civile e del mondo accademico, tenendo adeguatamente conto dei corrispondenti interessi.

Negli organismi internazionali e nelle manifestazioni in relazione con la politica di sicurezza che influiscono direttamente o indirettamente sull'Internet governance, la rappresentanza degli attori determinanti è assicurata dal DFAE e dal DDPS.

Il DATEC e il DFAE allestiscono, entro la fine del 2013, in collaborazione con i dipartimenti coinvolti, un compendio delle principali manifestazioni e iniziative

nonché dei principali organismi internazionali in relazione con l'Internet governance.

Misura 10

La Svizzera coopera al livello della politica di sicurezza internazionale per far fronte alla minaccia presente nel cyberspazio in collaborazione con altri Stati e organizzazioni internazionali. Segue i relativi sviluppi a livello diplomatico e promuove lo scambio politico nel quadro di conferenze internazionali e altre iniziative diplomatiche *(DFAE, DDPS)*.

Concretizzazione

Il DFAE rappresenta la Svizzera in collaborazione con il DDPS a livello diplomatico, tutela gli interessi in materia di politica di sicurezza del Paese nei confronti di organizzazioni internazionali e altri Stati e promuove iniziative di diritto internazionale volte a preservare il cyberspazio da conflitti.

Misura 11

Nel quadro di iniziative, conferenze e processi di standardizzazione privati e statali nel settore della sicurezza e della protezione, i gestori, le associazioni e le autorità coordinano la loro presenza in tali organismi *(DATEC, DFAE, DDPS, DFF)*.

Concretizzazione

MELANI e il DATEC intensificano lo scambio di informazioni tra i gestori di infrastrutture critiche, i fornitori di prestazioni TIC, i fornitori di sistemi e le pertinenti associazioni in merito agli approcci e alle iniziative internazionali. In questo modo MELANI e il DATEC appoggiano la presenza coordinata della piazza economica svizzera in tali organismi internazionali. Se auspicato, MELANI e il DATEC assicurano la partecipazione d'intesa con i dipartimenti, segnatamente con il DFAE.

4.3.6 Campo d'azione 6: Gestione della continuità operativa e gestione delle crisi

Identificazione, analisi e valutazione

Le attività dei diversi attori sono coordinate a tutti i livelli.

La quotidianità civile è caratterizzata dalla gestione ordinaria dell'intera infrastruttura TIC. In tale contesto l'Amministrazione federale, la società, l'economia e i gestori di infrastrutture critiche sono sottoposti ad attacchi continui che devono essere identificati risp. individuati e respinti mediante contromisure. Gli sforzi sono incentrati su misure preventive a livello di infrastruttura ed esercizio, con regolari interventi reattivi senza conseguenze rilevanti.

Una crisi è caratterizzata da un attacco riuscito o da un pregiudizio durevole con gravi conseguenze eventualmente estese, nei casi estremi, a tutto il territorio nazionale. Il ritmo di condotta in seno alle strutture esistenti per la gestione della continuità operativa e delle crisi è direttamente proporzionale all'intensità delle crisi. Gli sforzi sono incentrati su una combinazione di azioni da accompagnare, a seconda dei casi, con misure tecniche di carattere nazionale e a guida politica. Al riguardo va osservato che l'individuazione delle cause è parte integrante della gestione di una

crisi. I gestori di infrastrutture critiche, da un lato, e i fornitori determinanti di prestazioni TIC come pure i fornitori determinanti di sistemi, dall'altro, sono coinvolti nel processo decisionale sulla base di appositi accordi.

Obiettivi prestazionali e pianificazione

Le analisi individuali e settoriali dei rischi servono da base per accordi settoriali e la pianificazione della continuità operativa. Devono essere elaborate o coordinate in stretta collaborazione con i gestori e le autorità regolatorie. Le pianificazioni per casi di crisi devono essere elaborate in stretto coordinamento con le autorità e i rappresentanti dell'economia e, laddove necessario, devono essere conclusi accordi. Questo obiettivo è realizzato in collaborazione e d'intesa con i responsabili della «Gestione dei rischi Confederazione» e della «Strategia nazionale per la protezione delle infrastrutture critiche».

La Svizzera deve essere in grado, da sola o in cooperazione con partner esteri, di identificare e respingere attivamente attacchi che la concernono o che potrebbero concernerla e quindi di appoggiare la gestione reattiva delle crisi. Gli organi responsabili vanno abilitati a condurre operazioni mirate per acquisire informazioni sulle infrastrutture d'attacco. Quanto precede va previsto nelle basi legali determinanti (per es. legge federale sul servizio informazioni civile) e sottoposto ai decisori politici.

Misure

Misura 12

Grazie a una gestione della continuità operativa, gli attori a livello di economia, società e autorità devono rafforzare e migliorare in stretta collaborazione la resistenza (resilienza) nei confronti di perturbazioni e di eventi *(DFE, DFF, DDPS, DATEC).*

Concretizzazione

Nel quadro della revisione della LAP, il DFE adegua le proprie competenze per poter eseguire, con tutti i sottosettori dell'approvvigionamento economico del Paese, analisi dei rischi e della vulnerabilità orientate alle necessità, coinvolgendo in funzione delle circostanze le autorità competenti (in primo luogo DATEC e DFF). I risultati vanno concretizzati in corrispondenti piani di gestione della continuità operativa e delle crisi. I gestori di infrastrutture critiche non compresi nel raggio d'azione dell'approvvigionamento economico del Paese devono essere integrati nelle pertinenti procedure tramite le autorità di volta in volta competenti, le quali, in caso di necessità, adeguano di conseguenza la rispettiva legislazione specialistico-settoriale.

MELANI sostiene e intensifica lo scambio di informazioni su base volontaria con e tra i gestori di infrastrutture, i fornitori di prestazioni TIC e i fornitori di sistemi, al fine di sostenere la continuità operativa e la resilienza sulla base dell'autoaiuto. A causa del maggior fabbisogno di capacità forensi, del crescente flusso di informazioni e dell'intensificazione dello scambio di informazioni con i gestori di infrastrutture critiche e con l'economia, ulteriori capacità e risorse sono create mediante una collaborazione sistematica con i fornitori determinanti di prestazioni TIC e i fornitori determinanti di sistemi.

Misura 13

In caso di crisi è necessario in primo luogo coordinare attraverso MELANI le attività con gli attori direttamente interessati e appoggiare mediante competenze specialistiche i processi decisionali interni alle strutture esistenti per la gestione della continuità operativa e delle crisi, affinché sia garantita un'azione coerente per la gestione della crisi. A tal riguardo, va tenuto conto anche delle disposizioni legali concernenti il perseguimento penale. Lo scambio nazionale e internazionale di informazioni svolge un ruolo fondamentale per la gestione delle crisi e pertanto deve essere garantito e coordinato *(DFE, DFF, DDPS, DFGP)*.

Concretizzazione

In caso di crisi, a sostegno degli attori interessati MELANI sostiene e intensifica lo scambio di informazioni su base volontaria con i gestori di infrastrutture critiche e con i suoi partner internazionali e assicura il coinvolgimento degli organi di polizia. Ciò comporta un maggior fabbisogno di capacità forensi, un crescente flusso di informazioni e un'intensificazione dello scambio di informazioni con i gestori di infrastrutture critiche e con l'economia. Le capacità e risorse supplementari sono realizzate mediante una collaborazione sistematica con i fornitori determinanti di prestazioni TIC e i fornitori determinanti di sistemi.

Misura 14

Nel caso di una minaccia specifica sono previste misure attive per individuare gli autori e le loro intenzioni nonché per accertare le loro capacità e perturbare la loro infrastruttura *(DDPS, DFGP)*.

Concretizzazione

Ai fini della gestione e dell'ulteriore elaborazione di eventi in relazione con i mezzi TIC e determinanti per la protezione dello Stato, nell'attività del SIC devono essere inglobate le componenti del suo mandato inerenti al cyberspazio. Questo obiettivo è perseguito con il coinvolgimento della BAC, in qualità di fornitore di prestazioni tecniche a favore del SIC, e del SIM, in qualità di interfaccia con i servizi partner militari, le alleanze militari internazionali e le rispettive agenzie. Quanto precede va previsto nelle basi legali determinanti (segnatamente nella legge federale sul servizio informazioni civile) e sottoposto ai decisori politici.

I risultati dell'analisi della situazione di minaccia eseguita da MELANI e le possibilità previste nel quadro del mandato legale del perseguimento penale per l'individuazione e la traduzione davanti alla giustizia degli autori di reati sono integrati nelle misure.

Misura 15

Va fatto sì che gli aspetti inerenti al cyberspazio siano debitamente considerati nelle procedure e nei processi di condotta in seno alle strutture esistenti previste – ai fini di una tempestiva soluzione dei problemi – per far fronte a un aumento del ritmo di condotta in caso di crisi. Questo obiettivo è realizzato in coordinamento con la «Strategia nazionale per la protezione delle infrastrutture critiche» e i dipartimenti *(Cancelleria federale)*.

Concretizzazione

Qualora fosse incaricata di sottoporre al Consiglio federale, nel quadro della riforma del Governo, proposte relative alle tematiche «individuazione tempestiva delle crisi» e «gestione delle crisi», la Cancelleria federale deve coinvolgere i partner competenti per i rischi informatici.

4.3.7 Campo d'azione 7: Basi legali

Identificazione, analisi e valutazione

Le basi legali concernenti il cyberspazio figurano attualmente in una moltitudine di leggi federali e ordinanze. In questo ambito risultano problematiche la carente armonizzazione e il carattere in parte ancora lacunoso delle regolamentazioni.

Nel quadro della concretizzazione delle misure devono essere chiarite, laddove necessario, anche le possibilità per l'Amministrazione federale di emanare norme volte a minimizzare i rischi informatici e giuridicamente vincolanti anche al di fuori dei suoi organi.

Obiettivi prestazionali e pianificazione

Le basi legali vigenti tengono conto delle componenti inerenti al cyberspazio nei compiti e nelle responsabilità attuali. Per questo motivo, una soluzione nel quadro di un'unica legge speciale di portata nazionale non è appropriata. Pertanto, nel quadro di revisioni, i testi legislativi vigenti devono essere costantemente adeguati agli sviluppi nel cyberspazio rientranti nei rispettivi campi d'applicazione. Nondimeno, è assolutamente necessario garantire la coerenza dei relativi lavori.

Occorre inoltre chiarire quali basi legali applicabili agli attori rilevanti (segnatamente i Cantoni, i gestori di infrastrutture critiche e l'economia) già esistono oltre a quelle concernenti le autorità e quali chiarimenti giuridici debbano essere eseguiti per conferire, laddove necessario, la facoltà di emanare istruzioni.

Misure

Misura 16

In previsione delle misure devono essere verificate la coerenza e la completezza delle basi legali vigenti. In tale contesto occorre definire le priorità allo scopo di adeguare senza indugio le basi legali per la cui rielaborazione non è possibile attendere fino alla prossima revisione periodica *(DFF)*.

Concretizzazione

In collaborazione con i dipartimenti, l'organo di coordinamento per la concretizzazione della strategia elabora entro la fine del 2013, sulla base delle misure esposte, un primo compendio relativo alle necessità di legiferare o di rivedere con la massima urgenza basi legali inerenti al cyberspazio. A tal fine bisogna, tra l'altro, prestare attenzione acché lo scambio di informazioni con terzi e la gestione dei dati siano disciplinati in maniera il più possibile uniforme in tutti i testi di legge. Inoltre, gli eventuali vincoli supplementari per i Cantoni, i gestori di infrastrutture critiche e l'economia devono essere debitamente documentati. La costituzionalità delle rego-

lamentazioni proposte va assicurata in collaborazione con l'Ufficio federale di giustizia. Per le lacune legislative e i necessari adeguamenti giuridici identificati come prioritari, i dipartimenti competenti devono elaborare, entro la fine del 2014, un avamprogetto maturo per la procedura di consultazione accompagnato da un rapporto esplicativo.

4.3.8 Organo di coordinamento per la concretizzazione della strategia

L'elaborazione e la concretizzazione di misure adeguate ai differenti livelli incombe agli organi responsabili nel quadro del rispettivo mandato e avviene *in collaborazione* con i rispettivi partner competenti in seno alle autorità (a livello di Confederazione, Cantoni e Comuni), all'economia (gestori e associazioni) e alla società. Gli organi competenti assicurano il coinvolgimento di questi attori.

Un organo di coordinamento per la concretizzazione della strategia in seno al DFF appoggia in stretta collaborazione con gli organi competenti la costante concretizzazione e applicazione delle misure richieste. Ciò deve essere realizzato entro quattro a sei anni. Il suddetto organo di coordinamento deve collaborare strettamente con già esistenti organi di coordinamento e segretariati per ulteriori strategie della Confederazione e evitare doppioni.

Dopo la conclusione della concretizzazione, e pertanto al termine del trasferimento delle procedure e degli adeguamenti determinanti nell'esercizio ordinario, l'organo di coordinamento per la concretizzazione della strategia sarà disciolto. Al termine delle attività di concretizzazione, MELANI assumerà, se necessario, un ruolo di coordinamento e direzione.

L'organo di coordinamento per la concretizzazione della strategia ha i seguenti compiti:

- dirige un comitato interdipartimentale di pilotaggio per il coordinamento delle fasi di concretizzazione a livello di Confederazione. Detto comitato sarà costituito da rappresentanti dei servizi federali competenti. I dipartimenti provvedono essi stessi a designare i rispettivi rappresentanti;
- accompagna, in collaborazione con il Meccanismo di consultazione e di coordinamento «Rete integrata Svizzera per la sicurezza», un gruppo specialistico «Cyber» costituito da rappresentanti dei livelli Confederazione, Cantoni e Comuni nonché da rappresentanti dei gestori di infrastrutture, dell'economia e della società. Tale gruppo specialistico promuove la diffusione delle medesime informazioni presso tutti i partner nonché l'avvio e il coordinamento di soluzioni congiunte dei problemi;
- elabora un piano di concretizzazione dettagliato con i servizi competenti a livello federale; il piano comprende la concretizzazione nei rispettivi settori e contiene i relativi adeguamenti in materia di risorse e di basi legali;
- allestisce annualmente all'attenzione del Consiglio federale un rapporto sullo stato della concretizzazione;

- provvede al coordinamento delle procedure messe in atto dai dipartimenti competenti per la concretizzazione delle misure, nei casi in cui tali misure comportino ripercussioni in campo legislativo, segnatamente per quanto concerne progetti legislativi attuali e futuri (FOGIS, LCPol, LSIC, LAP, LSCPT);
- vigila sulla concretizzazione della Strategia nazionale per la protezione della Svizzera contro i rischi informatici, tenendo conto della politica della Confederazione in materia di rischi, della «Strategia nazionale per la protezione delle infrastrutture critiche» e del gruppo di lavoro «Rischi Svizzera» (DDPS-UFPP) nonché della «Strategia per una società dell'informazione in Svizzera» (DATEC-UFCOM);
- verifica con i servizi competenti la possibilità di semplificare e snellire gli iter e i sistemi per le notifiche;
- verifica con i servizi competenti le possibili sinergie (per es. nel settore tecnico-operativo);
- coordina la concretizzazione delle misure 7, 8 e 15 con gli uffici e gli attori competenti e fornisce assistenza, in caso di necessità, con contributi specialistici nella concretizzazione della misura 1;
- verifica dopo cinque anni la Strategia nazionale per la protezione della Svizzera contro i rischi informatici e il relativo piano di concretizzazione in considerazione dell'evoluzione generale nel cyberspazio e delle misure adottate. A tal fine realizza un benchmarking sistematico.