Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

18.088

Messaggio concernente il credito d'impegno per il sistema nazionale per lo scambio di dati sicuro

del 21 novembre 2018

Onorevoli presidenti e consiglieri,

con il presente messaggio vi sottoponiamo, per approvazione, il disegno di un decreto federale concernente un credito d'impegno per il sistema nazionale per lo scambio di dati sicuro.

Gradite, onorevoli presidenti e consiglieri, l'espressione della nostra alta considerazione.

21 novembre 2018

In nome del Consiglio federale svizzero:

Il presidente della Confederazione, Alain Berset
Il cancelliere della Confederazione, Walter Thurnherr

Compendio

Durante le loro attività quotidiane, ma soprattutto in caso di catastrofe e situazioni d'emergenza, gli organi di condotta della Confederazione, dei Cantoni e dei Comuni, le autorità e le organizzazioni d'intervento responsabili della sicurezza e del salvataggio nonché i gestori di infrastrutture critiche devono poter contare su uno scambio di informazioni rapido e sicuro. Nell'ambito dell'esercitazione della rete integrata per la sicurezza 2014 è emerso che, in caso di panne elettrica, i sistemi di telecomunicazione civili esistenti non funzionerebbero più o funzionerebbero in misura notevolmente limitata. È stato inoltre rilevato che la mancanza di una presentazione della situazione generale con quadri della situazione, ossia l'analisi integrata della situazione, è un punto debole della gestione nazionale degli eventi. Questa constatazione è stata confermata nell'ambito dell'esercitazione di condotta strategica del 2017. Per colmare questa lacuna il Consiglio federale chiede, con il presente messaggio, un credito d'impegno di 150 milioni di franchi per la realizzazione di un sistema nazionale per lo scambio di dati sicuro.

Situazione iniziale

I mutati scenari dei rischi e delle minacce pongono nuove sfide per la protezione della popolazione. La dipendenza da una rete elettrica funzionante cresce costantemente. In caso di interruzione di corrente elettrica i sistemi di telecomunicazione non sono più disponibili. Nuovi rischi, come i ciberattacchi sferrati contro le autorità o i gestori di infrastrutture critiche, stanno aumentando a livello mondiale. La minaccia terroristica si è aggravata.

I sistemi di telecomunicazione attualmente disponibili presentano lacune nel campo della sicurezza. Nell'ambito dell'esercitazione della Rete integrata per la sicurezza 2014 (ERSS 14) è emerso che, in caso di penuria di elettricità, i sistemi di telecomunicazione non funzionerebbero più o funzionerebbero in misura chiaramente limitata. Ciò è dovuto soprattutto al fatto che le reti commerciali utilizzate presentano una resistenza scarsa o nulla alle crisi. I sistemi con un funzionamento limitato non consentono un flusso stabile, tempestivo e affidabile di dati e informazioni. Manca inoltre un sistema più sicuro che, nel caso di un terremoto, di un incidente in una centrale nucleare o di un attentato terroristico, garantisca la visione generale di una situazione complessa o consenta di elaborare un quadro comune della situazione. Questa constatazione è stata confermata nell'ambito dell'esercitazione di condotta strategica 2017 (ECS 17).

In caso di catastrofe e di situazioni d'emergenza gli organi di condotta, le altre autorità e organizzazioni coinvolte e i gestori di infrastrutture critiche devono poter contare su sistemi di comunicazione funzionanti e su un quadro consolidato della situazione per dare l'allarme alla popolazione, mantenere le prestazioni critiche e ordinare per tempo le misure di sicurezza atte a proteggere la popolazione. Essi necessitano di informazioni sulla situazione e di sistemi di condotta al fine di disporre in modo rapido e completo delle basi principali e di garantire in qualsiasi situazione l'attuazione delle misure di protezione.

Le lacune di sicurezza individuate possono essere colmate mediante nuovi sistemi di telecomunicazione per gli organi di condotta federali, cantonali e comunali, le autorità e organizzazioni d'intervento responsabili della sicurezza e del salvataggio e i gestori di infrastrutture critiche. Il 18 dicembre 2015 il Consiglio federale ha incaricato il Dipartimento federale della difesa, della protezione della popolazione e dello sport (DDPS) di effettuare una valutazione dello stato dei progetti di telecomunicazione rilevanti per la protezione della popolazione svizzera. Il rapporto illustra in particolare i sistemi indispensabili per una protezione efficace della popolazione e che devono essere realizzati o ulteriormente sviluppati a breve termine. Da settembre a dicembre 2016 il DDPS ha sottoposto il rapporto per consultazione ai Cantoni, agli uffici federali, ai gestori di infrastrutture critiche e ad altre organizzazioni e ricevuto 72 prese di posizione. La consultazione ha evidenziato che una rete di dati cablata, rafforzata e protetta contro le interruzioni di corrente e i ciberattacchi ha la massima priorità per gli organi federali, i Cantoni e i gestori di infrastrutture critiche.

Al fine di migliorare l'affidabilità dei sistemi di telecomunicazione e dello scambio su banda larga di informazioni e dati tra gli organi di condotta, le autorità attive nel campo della sicurezza, le organizzazioni d'intervento e i gestori di infrastrutture critiche, nonché di aumentare la protezione contro i ciberattacchi, occorre realizzare un sistema per lo scambio di dati sicuro cui partecipano Confederazione, Cantoni e terzi.

La regolamentazione delle competenze e del finanziamento del sistema tra Confederazione, Cantoni e terzi sono descritti nel messaggio concernente la revisione totale della legge sulla protezione della popolazione e sulla protezione civile (LPPC). La revisione totale della LPPC è sottoposta al Parlamento con un messaggio separato. Fatta salva la decisione del Parlamento, il Consiglio federale intende mettere in vigore la riveduta LPPC il 1° gennaio 2020. La soluzione proposta riflette un ampio consenso tra Confederazione e Cantoni.

Lo sviluppo e la realizzazione del sistema nazionale per lo scambio di dati sicuro contribuisce in modo determinante a colmare una lacuna individuata nella sicurezza e a migliorare pertanto la protezione della popolazione.

Contenuto del progetto

Con il decreto federale, il Parlamento stanzia un credito d'impegno pari a 150 milioni di franchi. La liberazione del credito d'impegno ha luogo in tre tranche. Per la prima sono liberati fondi pari a 14,7 milioni di franchi. Il Consiglio federale può decidere in merito alla liberazione della seconda tranche di 83,6 milioni di franchi e della terza tranche di 51,7 milioni di franchi sulla base dell'avanzamento del progetto.

Gli investimenti sono scaglionati fino al 2027. L'Ufficio federale della protezione della popolazione (UFPP) è responsabile della direzione del progetto, della sua gestione nonché degli acquisti su delega. Il credito d'impegno comprende la gestione del progetto, i lavori di sviluppo, l'acquisto di hardware e software, le licenze, le infrastrutture di rete nonché prestazioni per la gestione e la manutenzione della rete.

Al fine di garantire l'esercizio e la manutenzione del sistema per lo scambio di dati sicuro, le spese di funzionamento dell'UFPP aumenteranno nel 2020 di 100 000 franchi, nel 2021 di 600 000 franchi, nel 2022 di 1,5 milioni di franchi, nel 2023 di 7 milioni di franchi, nel 2024 di 10 milioni di franchi, nel 2025 di 12 milioni di franchi, nel 2026 di 13,9 milioni di franchi e dal 2027 di 15 milioni di franchi all'anno. Questi importi non comprendono le spese supplementari per il personale. Sono invece comprese le prestazioni per la manutenzione e l'esercizio della rete di base e delle 120 ubicazioni utenti pianificate, compresa la gestione dell'esercizio d'emergenza 24 ore su 24. In seguito alla disattivazione del sistema di messaggistica Vulpus, a partire dal 2026 le spese d'esercizio annue diminuiranno di 1,5 milioni di franchi.

Affinché il progetto possa essere realizzato nei tempi previsti conformemente alle direttive finanziarie e qualitative e possa essere garantito un esercizio sicuro del sistema, sono necessari fino a 30 posti di lavoro a tempo pieno. 15 di questi sono posti supplementari necessari durante la fase di progetto. Di questi 15 posti supplementari, 10 rimarranno necessari anche dopo la conclusione del progetto per l'esercizio tecnico e la manutenzione, la salvaguardia annuale del valore e la gestione dei beneficiari delle prestazioni. Questi 10 posti sono quindi durevolmente necessari.

Indice

Messaggio

1 Situazione iniziale e condizioni quadro

1.1 Situazione iniziale

Una comunicazione sicura e uno scambio garantito di informazioni e di quadri della situazione tra gli organi di condotta, le autorità responsabili della sicurezza e del salvataggio, le organizzazioni d'intervento e i gestori di infrastrutture critiche sono di fondamentale importanza al fine di gestire efficientemente gli eventi e di garantire un'adeguata sicurezza e protezione della popolazione in qualsiasi situazione.

Lo scambio di grandi quantità di dati e l'utilizzo di applicazioni presso la Confederazione e i Cantoni passa attualmente attraverso la KomBV-KTV, le reti delle polizie cantonali e le reti di operatori commerciali.

I sistemi d'informazione e di comunicazione civili attualmente utilizzati presentano lacune a livello di sicurezza. Nell'ambito dell'ERSS 14 è emerso che, se venisse a mancare l'elettricità, i sistemi di telecomunicazione esistenti funzionerebbero in misura chiaramente limitata e non sarebbero più in grado di far fronte alle situazioni con conseguenze complesse. Le reti utilizzate non offrono la sicurezza necessaria per un flusso di dati e di informazioni stabile, tempestivo e affidabile. In caso di evento potrebbero crollare a causa di sovraccarichi, interruzioni di corrente o ciberattacchi. Manca inoltre un sistema garantito per una visione generale di una situazione complessa, causata ad esempio da un terremoto, da un incidente in una centrale nucleare o da un attacco terroristico. L'ECS 17 ha confermato queste lacune rilevanti per la sicurezza. Il rapporto di valutazione dell'ECS 17 del 9 maggio 2018[1] evidenzia che la mancanza di un quadro congiunto della situazione è un punto debole della gestione delle crisi a livello nazionale. Oltre alle misure per la condivisione delle informazioni che consentono di tracciare un quadro generale della situazione, è indispensabile sviluppare ulteriormente gli strumenti tecnici. Ne consegue la raccomandazione di dare la priorità agli sforzi in corso che mirano a sviluppare ulteriormente la PES e l'analisi integrata della situazione in una presentazione della situazione generale con quadri della situazione specifici.

1.2 Problematica e motivo della richiesta di finanziamento

Il 1° dicembre 2017 il nostro Collegio ha preso atto della valutazione dello stato dei progetti di telecomunicazione rilevanti per la protezione della popolazione svizzera.

[1] Il rapporto è disponibile nel sito: www.bk.admin.ch/bk/it/home/documentazione/aiuto alla condotta strategica/esercizio di condotta strategica--ecs-.html.

Il rapporto del 29 settembre 2017[2] illustra in particolare quali sistemi sono indispensabili per un'adeguata protezione della popolazione svizzera e andrebbero quindi realizzati o ulteriormente sviluppati a breve termine. La valutazione delle 72 prese di posizione concernenti il rapporto ha evidenziato che una rete di dati cablata, rafforzata e protetta contro le interruzioni di corrente e i ciberattacchi e la sostituzione dell'obsoleto sistema di messaggistica Vulpus hanno la massima priorità per gli organi federali (p. es. fedpol, SIC, AFD, MeteoSvizzera, UFAM, UFE, SMFP o CENAL), i Cantoni e i gestori di infrastrutture critiche (per es. Swissgrid SA, FFS, Banca nazionale svizzera), i quali auspicano un accesso più rapido possibile al nuovo sistema.

Con la digitalizzazione della comunicazione tra le autorità e la popolazione sorgono nuove forme di vulnerabilità. La dipendenza da una rete elettrica funzionante cresce costantemente. I sistemi di telecomunicazione non sono più disponibili in caso di un'interruzione di corrente causata da guasti tecnici o da eventi naturali. Nuovi rischi, come i ciberattacchi alle autorità o ai gestori di infrastrutture critiche, stanno aumentando a livello mondiale. La minaccia terroristica si è aggravata. Nel contempo le tecnologie analogiche non sono più sottoposte a manutenzione; da ciò consegue, ad esempio, che il sistema di messaggistica Vulpus di diverse autorità civili responsabili della sicurezza in Svizzera dev'essere sostituito con un nuovo sistema.

Nella seduta del 1° dicembre 2017, il nostro Collegio ha dichiarato che occorre migliorare la disponibilità e quindi la protezione contro le interruzioni dei sistemi di telecomunicazione e dello scambio su banda larga dei dati tra gli organi di gestione, le autorità responsabili della sicurezza e i gestori di infrastrutture critiche nonché la protezione contro i ciberattacchi. A tal fine occorre realizzare un sistema nazionale per lo scambio di dati sicuro.

Il sistema nazionale per lo scambio di dati sicuro garantirebbe per almeno due settimane una connessione a banda larga tra gli organi federali, i Cantoni e i gestori di infrastrutture critiche anche in caso di una penuria prolungata di elettricità, di un'interruzione di corrente o di un disservizio delle reti di comunicazione commerciali migliorando in modo significativo l'integrità e la protezione dai ciberattacchi. Il sistema nazionale per lo scambio di dati è costituito dalla rete per lo scambio di dati sicuro, dal sistema d'accesso ai dati e da un'applicazione in sostituzione dell'obsoleto sistema di messaggistica Vulpus con un sistema che garantisce lo scambio di informazioni, compresi i quadri della situazione, per l'allestimento della presentazione della situazione generale.

Il sistema nazionale per lo scambio di dati sicuro si basa fondamentalmente sull'infrastruttura rafforzata (ubicazioni, rete in fibra ottica) della rete di condotta svizzera, che collega a banda larga circa 120 ubicazioni utenti e sfrutta a tal fine un'altra rete in fibra ottica già esistente che è di proprietà, diretta o in senso lato, del settore pubblico.

[2] Il rapporto è disponibile soltanto in tedesco e in francese. La versione francese è disponibile nel sito: www.admin.ch > Documentazione > Comunicati stampa > Selezionare: Divisione: DDPS, Data: 1.12.2017 > Sistemi d'allarme e comunicazione orientati al futuro per la protezione della popolazione > Documenti > «Rapport sur l'avenir des systèmes d'alarme et de télécommunication pour la protection de la population».

Il sistema di messaggistica Vulpus è attualmente gestito dall'esercito. Potrà essere interrotto dopo l'entrata in funzione del sistema per lo scambio di dati sicuro e del sistema di analisi integrata della situazione. Mediante la sostituzione dell'obsoleto sistema di messaggistica Vulpus con un sistema nazionale di analisi integrata della situazione, gli organi di condotta, le autorità responsabili della sicurezza, le organizzazioni d'intervento e i gestori di infrastrutture critiche avranno a disposizione una presentazione della situazione generale con quadri della situazione specifici, ossia una base di condotta fondamentale per gestire in modo rapido ed efficiente gli eventi con conseguenze complesse, intercantonali, nazionali o internazionali.

Il sistema nazionale per lo scambio di dati sicuro costituirà, per grandi volumi di dati, la base per tutti i sistemi di telecomunicazione rilevanti per la politica di sicurezza. Diventerà quindi la rete di trasporto centrale per i dati e le informazioni sulla protezione della popolazione e per la gestione delle crisi nazionali in qualsiasi situazione (p. es. anche in caso di attentati terroristici). Si prevede inoltre di migrare sul sistema per lo scambio di dati sicuro anche i sistemi di sicurezza Polycom, Polyalert e la radio d'emergenza IBBK. Sarà quindi a disposizione anche delle autorità per lo scambio di informazioni rilevanti per la sicurezza nell'attività quotidiana. Anche la KomBV-KTV potrà sfruttare la rete nazionale di dati sicura come rete di comunicazione separata, beneficiando così di una maggiore sicurezza dell'alimentazione con corrente elettrica nel settore condiviso.

Secondo la pianificazione attuale, si prevede di allacciare 120 ubicazioni utenti presso la Confederazione, i Cantoni e i gestori di infrastrutture critiche. In futuro potranno essere allacciate ulteriori ubicazioni secondo le necessità e nel rispetto delle direttive di connessione.

1.3 Importanza del progetto da finanziare

La vulnerabilità dello scambio su banda larga delle informazioni e dei dati tra organi di condotta, autorità responsabili della sicurezza, organizzazioni d'intervento e gestori di infrastrutture critiche costituisce un rischio elevato per la sicurezza.

La comunicazione e lo scambio rapido e sicuro di informazioni al fine di schizzare rapidamente una presentazione affidabile della situazione con quadri della situazione specifici assumono un ruolo fondamentale per la gestione efficiente degli eventi. La crescente importanza della collaborazione tra autorità, forze d'intervento e gestori di infrastrutture critiche è emersa in occasione di eventi maggiori come quelli che si sono verificati in Svizzera negli ultimi anni (Vivian 1990 o Lothar 1999, canicole del 2003 e del 2015, alluvioni del 2005 e 2007, interruzione delle FFS del 2005, influenza suina del 2009, incendio forestale di Visp del 2011, frana di Bondo del 2017). La collaborazione richiede una buona interconnessione e informazioni sulla situazione condivise con tutti i partecipanti. L'ERSS 14 e l'ECS 17 hanno confermato questa esigenza.

Le esperienze fatte all'estero hanno dimostrato che gli eventi con conseguenze complesse (p. es. terremoti, attentati terroristici) possono essere gestiti in modo efficiente evitando ulteriori morti, feriti e danni materiali soltanto se un quadro completo della situazione è reso rapidamente disponibile a tutte le parti coinvolte nell'intervento. A

tale scopo serve l'analisi integrata della situazione, che collega gli attuali sistemi d'analisi della situazione della Confederazione, dei Cantoni e dei gestori di infrastrutture critiche e riunisce le informazioni provenienti da diversi sistemi in una presentazione della situazione generale con quadri della situazione specifici. Essa può sostituire al contempo l'ormai obsoleto sistema di messaggistica Vulpus.

La realizzazione del sistema nazionale per lo scambio di dati sicuro colma le attuali lacune di sicurezza nello scambio di informazioni e di quadri della situazione tra le parti coinvolte, riduce significativamente il rischio d'interruzione dei sistemi e aumenta la sicurezza per la popolazione. Tale sistema aumenta inoltre significativamente la sicurezza anche nelle situazioni normali, permettendo ad esempio di scambiare con maggiore sicurezza e affidabilità le informazioni di MeteoSvizzera necessarie per l'esercizio degli aeroporti.

1.4 Interesse della Confederazione per il progetto

La Confederazione, i Cantoni e altri enti collaborano alla protezione della popolazione nell'ambito delle loro competenze, in particolare nel settore dei sistemi d'allarme e di comunicazione. L'interoperabilità di questi sistemi e la disponibilità di collegamenti sicuri tra questi enti sono nell'interesse di tutti. Con la messa a disposizione di componenti centralizzate per il sistema nazionale per lo scambio di dati sicuro, la Confederazione garantisce l'interoperabilità dei sistemi, offre ad altri organi federali, ai Cantoni e ai gestori di infrastrutture critiche la possibilità di collegare i loro sistemi al sistema globale e getta le basi per un'interconnessione garantita a banda larga. Ad esempio, nella sua presa di posizione sull'esposizione dei sistemi di telecomunicazione rilevanti per la protezione della popolazione, la Banca nazionale svizzera ha affermato che la realizzazione del sistema nazionale per lo scambio di dati sicuro contribuirebbe in modo significativo alla resilienza operativa della piazza finanziaria svizzera. Inoltre permetterebbe, unitamente al sistema di analisi integrata della situazione, di sostituire l'obsoleto sistema di messaggistica Vulpus.

In caso di catastrofi e di situazioni d'emergenza di portata nazionale, anche la Confederazione assume una certa responsabilità di condotta, che può esercitare in maniera molto più mirata se è connessa in modo garantito con gli organi cantonali di condotta e i gestori di infrastrutture critiche e se dispone di un quadro consolidato della situazione generale.

1.5 Prospettive per il futuro

La realizzazione di un sistema nazionale per lo scambio di dati sicuro favorisce l'utilizzo di strumenti digitali nella gestione degli eventi. Un sistema più protetto contro le interruzioni di corrente e i rischi cibernetici permette di sfruttare meglio ai fini della sicurezza i vantaggi degli sviluppi digitali nel campo della comunicazione e dello scambio di informazioni grazie alla sua maggiore resilienza. In tal modo si migliora l'efficienza degli interventi e la protezione della popolazione.

È ipotizzabile che il sistema di comunicazione Polycom verrà sostituito con un sistema di comunicazione mobile sicuro a banda larga non appena le applicazioni di radiocomunicazione a banda larga saranno standardizzate. Per soddisfare efficacemente l'esigenza di una comunicazione sicura e resiliente dei dati fino ai terminali mobili delle organizzazioni d'intervento sull'intero territorio nazionale, si potrebbe prendere in considerazione un'estensione mobile con capacità limitata del sistema per lo scambio di dati sicuro secondo le necessità. Visto che il sistema nazionale per lo scambio di dati sarà resiliente contro le interruzioni di corrente e i ciberattacchi, gli utenti avrebbero a disposizione una rete di trasporto sempre sicura e altamente disponibile con una componente mobile disponibile in qualsiasi situazione.

La rete per lo scambio di dati sicuro rappresenta un valore aggiunto per altri utenti che attribuiscono molta importanza alla disponibilità in caso di interruzioni di corrente o di interruzioni TIC. Può servire da piattaforma di trasmissione per vari altri sistemi e migliorare significativamente la loro affidabilità.

Grazie alla disponibilità di una rete per lo scambio di dati sicuro potranno inoltre essere valutate ed eventualmente eliminate ridondanze con altre reti. In settori quali l'approvvigionamento di energia o la piazza finanziaria svizzera, la rete per lo scambio di dati sicuro potrebbe essere utilizzata come una rete ridondante per il trasporto di dati, aumentando in tal modo la resilienza di questi settori critici. Esistono inoltre molte altre possibilità d'impiego rilevanti per la sicurezza.

Non è oggetto del presente messaggio l'esigenza di adottare misure periodiche di salvaguardia del valore del sistema con carattere d'investimento su alcuni degli investimenti effettuati. Questi sono stati addebitati alla Confederazione secondo la regolamentazione di finanziamento proposta nel messaggio del …[3] concernente la revisione totale della legge sulla protezione della popolazione e sulla protezione civile (messaggio LPPC). A tempo debito verrà chiesto un altro credito d'impegno a tal fine.

1.6 Coinvolgimento delle cerchie interessate

Secondo l'articolo 2 capoverso 1 della legge sulla consultazione del 18 marzo 2005[4] (LCo), la procedura di consultazione ha lo scopo di far partecipare i Cantoni, i partiti e gli ambienti interessati al processo di formazione dell'opinione e delle decisioni della Confederazione. Sebbene si tratti di un progetto di ampia portata finanziaria, si è rinunciato a una procedura di consultazione. In vista di questo messaggio sono infatti già state svolte ampie consultazioni sui sistemi. Non ci si aspettava quindi di raccogliere nuovi riscontri con una consultazione supplementare.

Nell'ambito della stesura e della consultazione del rapporto sul futuro dei sistemi di telecomunicazione nella protezione della popolazione, sono stati consultati gli organi competenti della Confederazione, dei Cantoni e dei gestori di infrastrutture critiche nonché associazioni e organizzazioni civili al fine di fissare le priorità per i sistemi. Sono pervenute complessivamente 72 prese di posizione. Dalla consulta-

3 FF …
4 RS **172.061**

zione è emerso che il sistema per lo scambio di dati sicuro, la sostituzione dell'obsoleto sistema di messaggistica Vulpus e la realizzazione di un sistema di analisi integrata della situazione hanno la massima priorità. È stato chiesto che, per tutti questi progetti, venissero specificati i costi non appena fosse stata presa la decisione di principio sulla realizzazione dei progetti.

Nell'ambito della specificazione del sistema di analisi integrata della situazione, nella fase d'inizializzazione sono stati effettuati vari lavori e accertamenti in collaborazione con gli organi federali e cantonali interessati. In tale operato rientrava anche un'indagine tramite questionario presso 18 organi federali e 59 organi cantonali. In cinque workshop plenari con più di 100 partecipanti ciascuno sono state discusse e approfondite le aspettative e le richieste di massima in relazione al sistema. I risultati sono poi stati trascritti in uno studio. Oltre allo studio sono state redatte una descrizione tecnica dell'architettura del sistema e una definizione dello scopo previsto del sistema. Un concetto d'attuazione descrive il progetto a livello strategico. Da ultimo l'UFPP ha condotto presso l'industria un sondaggio sulla realizzazione di un sistema di analisi integrata della situazione elettronica. I risultati dimostrano che l'industria reputa che il progetto sia utile dal punto di vista tecnico, operativo, organizzativo e di facile attuazione.

Gli accertamenti hanno evidenziato che la sostituzione del sistema di messaggistica Vulpus e la realizzazione di un sistema di analisi integrata della situazione presentano un grande potenziale di sinergie. Una soluzione moderna per la sostituzione del sistema di messaggistica Vulpus permetterà di soddisfare ampiamente anche le funzionalità richieste per il sistema di analisi integrata della situazione.

Per chiarire le responsabilità e le questioni di finanziamento, il 10 gennaio 2017 il capo del DDPS e i presidenti della CCDGP e della CG MPP hanno istituito un gruppo di lavoro composto da rappresentanti della Confederazione e dei Cantoni. È stata quindi trovata una soluzione consensuale ed è stato concordato il finanziamento di base con i Cantoni.

2 Contenuto del decreto di stanziamento

2.1 Richiesta del nostro Collegio

Il sistema nazionale per lo scambio di dati sicuro è un progetto chiave nel campo delle tecnologie dell'informazione e della comunicazione della Confederazione. Il nostro Collegio chiede un credito d'impegno di 150 milioni di franchi. La Confederazione si assume gli investimenti per lo sviluppo e l'acquisto delle componenti centralizzate del sistema, ossia di quelle componenti condivise da tutti gli utenti (organi federali, Cantoni, gestori di infrastrutture critiche).

Il credito d'impegno sarà liberato in tre tranche. Con l'approvazione del credito d'impegno il Parlamento libererà 14,7 milioni di franchi per la prima tranche. Da parte nostra decideremo in merito alla liberazione di 83,6 milioni di franchi per la seconda trance e di 51,7 milioni di franchi per la terza tranche, sulla base dei progressi del progetto.

2.2 Descrizione dettagliata del contenuto del progetto

Il sistema nazionale per lo scambio di dati sicuro comprende

a. la rete per lo scambio di dati sicuro,
b. il sistema di accesso ai dati e
c. il sistema di analisi integrata della situazione che sostituisce l'obsoleto sistema di messaggistica Vulpus.

2.2.1 La rete per lo scambio di dati sicuro

Quale rete di trasporto (layer 1 e 2) per la comunicazione di dati su banda larga, la rete per lo scambio di dati sicuro costituirà la base per tutti i sistemi di telecomunicazione della protezione della popolazione rilevanti per la politica di sicurezza. Essa garantirà per almeno due settimane una connessione a banda larga autonoma tra gli organi federali, i Cantoni e i gestori di infrastrutture critiche anche in caso di penuria prolungata di corrente, interruzione di corrente o disservizio delle reti di comunicazione commerciali. Con il credito d'impegno verranno collegate 120 ubicazioni utenti a questa rete sicura. Ogni ubicazione utenti sarà collegata ad almeno due nodi di rete rafforzati. Per gli organi federali quali fedpol, SIC, AFD, Cgcf, UFAM, UFE, MeteoSvizzera, SMFP e CENAL sono previsti 40 allacciamenti; per gestori di infrastrutture critiche quali gli aeroporti, le FFS SA, Swissgrid SA, la Banca nazionale svizzera, le emittenti radiofoniche e di radiodiffusione, le cooperative Migros, Coop SA ecc. e terzi, ad esempio il Principato del Lichtenstein, sono previsti 44 allacciamenti. Per i Cantoni sono previsti 36 allacciamenti (almeno un allacciamento per Cantone). Gli allacciamenti cantonali verranno di regola installati nelle centrali d'allarme e d'intervento della polizia cantonale, già protette contro le interruzioni di corrente.

Se le condizioni di sicurezza sono soddisfatte, gli utenti possono, secondo le loro esigenze, allacciare le proprie reti (p. es. reti cantonali) alla connessione e collegare così vari organi cantonali tra loro. Ciò permette l'accesso al sistema anche da parte di più organi specializzati all'interno del gruppo utenti, p. es. all'interno del Cantone, di un'azienda o di un'unità amministrativa. Gli utenti stessi sono responsabili di progettare queste componenti decentralizzate e di proteggere gli organi specializzati coinvolti contro le interruzioni di corrente.

Secondo il nostro decreto del 20 maggio 2015, la realizzazione della rete per lo scambio di dati sicuro si deve basare, nella misura del possibile, sulle infrastrutture fisiche della rete di condotta svizzera, ossia sulla rete in fibra ottica e sulle ubicazioni rafforzate. La realizzazione avrà luogo in modo da separare completamente il traffico dei dati dell'esercito dal traffico dei dati degli utenti del sistema nazionale per lo scambio di dati sicuro. In questo modo si tiene conto delle esigenze in materia di sicurezza dell'esercito e degli utenti del sistema. Per la connessione delle ubicazioni utente verranno utilizzate anche infrastrutture in fibra ottica della Confederazione (p. es. Strade nazionali), dei Cantoni o di gestori di infrastrutture critiche. Dove non è possibile collegare le ubicazioni utenti con le infrastrutture in fibra ottica

esistenti, si realizzano nuove linee in fibra ottica. Per la pianificazione si considerano soprattutto quelle infrastrutture di rete che già soddisfano le esigenze di protezione contro le interruzioni di corrente, ossia che dispongono di generatori d'emergenza. In alternativa viene verificata ed eventualmente migliorata la protezione contro le interruzioni di corrente delle reti di terzi coinvolte. La realizzazione su una rete commerciale sarebbe molto costosa poiché bisognerebbe rafforzare tutti i nodi della rete e una parte delle linee in fibra ottica ed eseguire onerosi lavori di giunzione. L'utilizzo delle infrastrutture fisiche della rete di condotta Svizzera, che già oggi presentano un'elevata robustezza e autonomia energetica, e la loro connessione ad altre infrastrutture in fibra ottica di proprietà pubblica già esistenti permette di sfruttare ampie sinergie e quindi di realizzare una rete relativamente economica che soddisfi le direttive di protezione contro le interruzioni di corrente.

2.2.2 Il sistema di accesso ai dati

Il sistema di accesso ai dati è una rete utenti chiusa (layer 3). Per reti utenti chiuse s'intendono reti logiche isolate senza alcuna connessione a Internet o ad altre reti. Il sistema di accesso ai dati fornirà in futuro agli utenti un accesso sicuro e garantito in qualsiasi situazione ai sistemi di allarme e di telecomunicazione rilevanti per la protezione della popolazione. Per l'utilizzo delle applicazioni vengono impiegati terminali dedicati. Dal momento che si tratta di una rete chiusa, un coordinamento con altre reti non è necessario. Sulla rete per lo scambio di dati sicuro è possibile, in combinazione con il sistema di accesso ai dati, gestire in sicurezza e in qualsiasi situazione tutte le applicazioni (esistenti e future) rilevanti per la protezione della popolazione. Le applicazioni su questa rete sono ad esempio Polycom per la radiocomunicazione e Polyalert per la diffusione dell'allarme, nonché altri sistemi e applicazioni rilevanti per la sicurezza. L'isolamento da tutte le altre reti, per esempio da Internet, aumenta sensibilmente la resilienza contro i ciberattacchi.

2.2.3 La sostituzione del sistema di messaggistica Vulpus e il sistema di analisi integrata della situazione

Detto in parole semplici, la rete per lo scambio di dati sicuro è costituita dall'hardware, mentre il sistema d'accesso ai dati dal sistema operativo. Per la comunicazione effettiva dei dati serve ancora un'applicazione. È previsto di realizzare questa applicazione per sostituire l'obsoleto sistema di messaggistica Vulpus. Quest'ultimo è un sistema civile protetto di messaggistica della Confederazione, dei Cantoni e di terzi, utilizzato da circa 70 enti. È impiegato da circa 30 anni per lo scambio di informazioni (soprattutto messaggi di testo) tra il Ministero pubblico della Confederazione, i corpi cantonali di polizia, la polizia della città di Zurigo, il Corpo delle guardie di confine, la Sicurezza militare, la CENAL, il SIC, vari stati maggiori speciali del nostro Collegio, l'UFPP e diverse formazioni d'allarme. Oggi viene impiegato per la diffusione dell'allarme, la ricerca di persone in seguito a un allarme e la trasmissione di comunicati d'allerta sui pericoli naturali della Confederazione con il coinvolgimento dei media (emittenti radiofoniche). Il sistema è utilizzato nelle attività quoti-

diane dalle organizzazioni e autorità citate. L'esercito e la RUAG provvedono attualmente alla gestione e alla salvaguardia del valore di questo sistema, che non è protetto contro le interruzioni di corrente. Esso si basa sulla rete di telefonia analogica di Swisscom. Il funzionamento delle connessioni può essere garantito, grazie a varie misure, al massimo fino al 2025. L'esercito e il SIC non hanno più bisogno del sistema di messaggistica Vulpus.

Le funzioni offerte dal sistema di messaggistica Vulpus sono fondamentali per la comunicazione tra le autorità e dovranno essere disponibili anche in futuro per le attività quotidiane, così come in caso di catastrofi e situazioni d'emergenza. Tale sistema è divenuto obsoleto e deve essere sostituito con un nuovo sistema di comunicazione di dati in grado di scambiare informazioni complesse sulla situazione, dati o quadri della situazione necessari per presentare la situazione generale.

Con la rete nazionale di dati viene quindi sviluppato un sistema che, non solo sostituisce le attuali funzioni del sistema di messaggistica Vulpus, ma offre anche la possibilità di scambiare informazioni complesse, come ad esempio la presentazione della situazione generale.

Le varie organizzazioni coinvolte nella gestione di catastrofi e situazioni d'emergenza utilizzano già sistemi elettronici per l'analisi della situazione (sistemi specialistici e di condotta). Tali sistemi includono ad esempio la PES, gestita dalla CENAL presso l'UFPP e utilizzata anche dal SIC, da fedpol e da organi cantonali. Concepiti su misura per i compiti e le esigenze specifici delle rispettive organizzazioni, questi sistemi non sono tuttavia interconnessi – o non lo sono sufficientemente. Ci sono però anche molte altre organizzazioni che attualmente non dispongono di un proprio sistema PES. Questo sistema di analisi integrata della situazione viene realizzato sulla rete per lo scambio di dati sicuro e sul sistema d'accesso ai dati. Contrariamente all'attuale sistema di messaggistica Vulpus, questo nuovo sistema garantisce la protezione contro le interruzioni e contro i ciberattacchi. L'esercito viene collegato al sistema tramite interfacce che gli consentiranno in particolare di ottenere informazioni sulla situazione civile e miglioreranno considerevolmente la collaborazione civile-militare, per esempio in caso di attacchi terroristici o catastrofi.

2.2.4 Investimenti

La realizzazione del sistema nazionale per lo scambio di dati sicuro richiede una stretta collaborazione con numerosi attori (enti federali, Cantoni, gestori di infrastrutture critiche), fornitori e proprietari di cavi in fibra ottica nonché proprietari di immobili. Nel credito d'impegno sono comprese anche le spese d'investimento per misure edilizie (principalmente nel settore dell'infrastruttura di rete e delle ubicazioni utenti della Confederazione). L'attuazione avviene in collaborazione con l'organo delle costruzioni e degli immobili della Confederazione.

Per gestire il progetto fino alla sua conclusione, il DDPS necessita quindi del supporto esterno di vari esperti. Quest'ultimi sostengono l'UFPP, responsabile del progetto, durante la fase di sviluppo, il coordinamento del progetto, la pianificazione e l'elaborazione di prodotti (p. es. requisiti, concetti di gestione delle parti coinvolte, pareri giuridici, contratti e accordi sul livello dei servizi, manuali per il progetto,

concetti di sicurezza, punti della situazione, documenti per gare d'appalto, realizzazione di strutture di *governance* per la gestione nella fase d'utilizzo, esecuzione di test, collaudo di sistemi, compiti di controllo). I costi di gestione del progetto preventivati sono relativamente elevati rispetto ad altri progetti. Da un lato, ciò è riconducibile al fatto che il progetto deve essere realizzato insieme a numerose parti interessate dell'Amministrazione federale, dei Cantoni e di terzi. Contemporaneamente il progetto sfrutta importanti sinergie con la rete di condotta Svizzera (backbone, connessioni ottiche, ubicazioni rafforzate, NCC, PRZ, SOC) che riducono i costi dell'infrastruttura di rete, ma aumentano i costi di gestione.

La parte principale dei lavori di sviluppo comprende lo sviluppo del software per il sistema di analisi integrata della situazione e la programmazione delle interfacce tra le componenti centralizzate del sistema e i sistemi decentralizzati di presentazione della situazione già impiegati dai Cantoni e dai gestori di infrastrutture critiche. Occorre elaborare un concetto dei nodi e delle connessioni per la rete e realizzare una rete IP per il sistema d'accesso ai dati. Oltre ai lavori di sviluppo tecnico, nell'ambito della fase concettuale di ciascuno dei quattro progetti occorre effettuare varie analisi (analisi del sistema, analisi tecniche, accertamenti legali ecc.) per concepire il sistema. Queste analisi serviranno da base per la realizzazione dei prodotti nella fase concettuale secondo il metodo di gestione dei progetti Hermes e per lo sviluppo di direttive e standard normativi.

Per realizzare il sistema occorre acquisire hardware per il NCC, il SOC e il centro di prova e di riferimento (Prüf- und Referenzzentrum, PRZ). Per l'esercizio del sistema d'accesso ai dati e del sistema di analisi integrata della situazione occorre acquistare un software configurato (sistema operativo) per il sistema d'accesso ai dati e le licenze necessarie per i software (p. es. programma antivirus). I costi sono bassi rispetto ai costi di sviluppo dato che è possibile sfruttare sinergie con la rete di condotta Svizzera nel campo degli hardware e dei software ed acquistare prodotti disponibili sul mercato.

L'infrastruttura della rete di condotta Svizzera (backbone) viene dotata di un'infrastruttura di rete supplementare (componenti attivi come multiplexer, router, switch) per la rete per lo scambio di dati e il sistema d'accesso.

Per una connessione ridondante delle ubicazioni utenti alla rete di condotta Svizzera (backbone), in pratica per l'«ultimo chilometro», vengono parzialmente realizzate nuove linee in fibra ottica poiché su questi tratti non è possibile utilizzare i cavi in fibra ottica esistenti.

Nelle 120 ubicazioni utenti vengono installate componenti di rete (switch, router) per tutti i progetti al fine di garantire la connessione della componente centralizzata con le componenti decentralizzate (allacciamento).

Per soddisfare le esigenze in materia di disponibilità e riservatezza poste all'infrastruttura, è necessario effettuare degli investimenti per rafforzare le ubicazioni utenti della Confederazione. In particolare, occorre garantire l'approvvigionamento elettrico tramite due linee d'ingresso indipendenti e, in caso di interruzione dell'approvvigionamento esterno, rendere disponibile un alimentatore di corrente autonomo in grado di garantire l'autonomia necessaria. Visto che la garanzia dell'approvvigiona-

mento di energia delle ubicazioni utenti spetta agli utenti allacciati, la Confederazione effettua questi investimenti per le proprie ubicazioni.

La gestione della rete comprende la gestione delle prestazioni, la gestione della configurazione e la gestione degli errori. Quale istanza centrale per la sorveglianza e il controllo permanenti e per il coordinamento dei processi e delle funzioni, servono due NCC tecnicamente, operativamente e geograficamente ridondanti. Nell'ambito della fase di progetto si verifica su quali NCC già esistenti ci si potrebbe appoggiare. Il compito di individuare e valutare potenziali ciberattacchi è assicurato dal SOC. Serve inoltre un PRZ per testare le modifiche prima che vengano introdotte nell'ambiente operativo e per poter simulare l'eliminazione dei difetti.

Dal punto di vista delle tecnologie dell'informazione, lo sviluppo e la realizzazione del sistema nazionale per lo scambio di dati sicuro si svolgono su un lasso di tempo relativamente lungo con il coinvolgimento di molti utenti. La realizzazione è associata a incertezze. Secondo Hermes il progetto è in fase di inizializzazione. L'UFPP non dispone di crediti di pianificazione per ridurre tali incertezze. Solo dopo la decisione politica di attuazione del progetto saranno disponibili le risorse necessarie per la fase di progetto in cui effettuare ulteriori accertamenti. Visto però che la proposta non si trova ancora nella fase di progetto, il corrispondente supplemento di rischio è attualmente preventivato al 15 percento.

Per gli investimenti nello sviluppo e nell'acquisto chiediamo un credito d'impegno pari a 150 milioni di franchi per il periodo 2020–2027. Il credito d'impegno si compone come segue:

Tabella 1

Panoramica dei costi d'investimento per lo sviluppo e l'acquisto

	in mio. fr.
Gestione del progetto	29,5
Lavori di sviluppo	17,7
Hardware, software, licenze	14,8
Infrastruttura di rete backbone	6,4
Infrastruttura di rete ubicazioni utenti	35,7
Gestione e manutenzione della rete	8,3
Ubicazioni utenti Confederazione	18,0
Supplemento di rischio (25 %)	19,6
Investimenti per sviluppo e acquisto	**150,0**

2.2.5 Scaglionamento e liberazione del credito d'impegno

Il credito d'impegno sarà liberato in tre tranche, conformemente alla raccomandazione all'attenzione del nostro Collegio formulata il 16 ottobre 2015[5] dal CFF nel suo rapporto «Verifica del progetto chiave TIC relativo alla piattaforma per le imposte di consumo», come pure a una domanda corrispondente della DelFin del marzo 2014 e al nostro decreto del 21 maggio 2014 concernente la lettera di risposta alla domanda.

Mediante la ripartizione in tre tranche viene liberata solo la parte che soddisfa i requisiti al momento della liberazione. Da parte nostra potremo in tal modo controllare efficacemente le risorse finanziarie e liberare i crediti necessari per il progetto in modo scaglionato per ogni tranche.

Obiettivo della prima tranche dal 2020 al 2021 è concretizzare i tre sottoprogetti. In questa fase vengono sviluppati i prodotti della fase concettuale secondo Hermes. Si tratta in particolare di confermare la fattibilità, precisare i costi del sistema e dei sottosistemi e il fabbisogno di personale nonché di ridurre i rischi. A tal fine si effettua un Proof of Concept (PoC). Si fissano inoltre le condizioni di sicurezza per gli allacciamenti. Dato che il sistema di messaggistica Vulpus verrà disattivato per ragioni tecniche alla fine del 2025, la gara d'appalto OMC necessaria per l'acquisto sostitutivo viene già preparata nell'ambito della prima tranche, in modo che l'appalto possa essere aggiudicato dopo la liberazione della seconda tranche.

5 Il rapporto è disponibile in Internet all'indirizzo www.efk.admin.ch > pubblicazioni > Progetti informatici > Archivio progetti informatici.

Con il decreto federale qui in esame le Camere federali decidono in merito alla liberazione dei mezzi finanziari per la prima tranche. I costi per la prima tranche ammontano a 14,7 milioni di franchi.

Obiettivo della seconda tranche dal 2022 al 2024 è effettuare una fase di prova e mettere quindi in servizio la rete. A tal fine si deve sviluppare il sistema d'accesso ai dati e metterlo in funzione. Gli utenti principali del sistema di messaggistica Vulpus saranno allacciati alla rete tra il 2024 e il 2025 per consentire la sostituzione del sistema all'inizio del 2026. Si prevede di disattivare il sistema di messaggistica Vulpus alla fine del 2025, dopo la conclusione della fase introduttiva e dell'esercizio parallelo del vecchio e del nuovo sistema, garantito per un anno per ragioni di sicurezza. Tale disattivazione è una condizione vincolante anche poiché il sistema ha raggiunto la fine del suo ciclo di vita. Un'ulteriore proroga dell'esercizio cagionerebbe costi supplementari sproporzionati. Gli ex utenti di Vulpus verranno istruiti sui nuovi sistemi nel 2023 e 2024.

La richiesta per la liberazione della seconda tranche di 83,6 milioni di franchi viene sottoposta alla Conferenza dei segretari generali per valutazione e quindi al nostro Collegio per decisione. I criteri per la liberazione sono i seguenti:

- la fase concettuale secondo Hermes è conclusa;
- la fattibilità è confermata, i costi per il sistema, i sottosistemi e il fabbisogno di personale sono precisati e i rischi d'introduzione sono valutati;
- il PoC per la rete e il sistema d' accesso è concluso;
- le condizioni d'allacciamento per la Confederazione, i Cantoni e i gestori di infrastrutture critiche sono definite;
- il bando di concorso OMC per la sostituzione del sistema di messaggistica Vulpus e la preparazione per l'aggiudicazione sono terminate.

Con la terza tranche dal 2025 al 2027 vengono allacciati alla rete gli utenti che non sono ancora stati allacciati nell'ambito della seconda tranche e viene ulteriormente sviluppato il sistema di accesso ai dati. Per l'integrazione dei diversi sistemi PES si sviluppano le interfacce da collegare al sistema di analisi integrata della situazione. Contemporaneamente viene ampliato il set delle funzionalità per l'analisi integrata della situazione, come ad esempio la funzione per la rappresentazione delle informazioni geografiche. Una volta concluso il progetto nel 2027, nel 2028 si eseguiranno i lavori conclusivi e di garanzia.

Anche la richiesta per la liberazione della terza tranche di 51,7 milioni di franchi viene sottoposta alla Conferenza dei segretari generali per valutazione, dopodiché al nostro Collegio per decisione. I criteri per la liberazione sono i seguenti:

- la rete per lo scambio di dati sicuro è operativa e i processi d'esercizio sono consolidati;
- l'infrastruttura delle ubicazioni originarie degli utenti principali è rafforzata e collegata al sistema di accesso ai dati;

– la sostituzione del sistema di messaggistica Vulpus è iniziata;
– un primo set di funzionalità per il sistema di analisi integrata della situazione è realizzato e in fase di prova.

Tabella 2

Ripartizione del credito d'impegno sulle tre tranche (in milioni di franchi)

	Tranche 1	Tranche 2	Tranche 3
Totale	14,7	83,6	51,7

2.2.6 Esercizio e manutenzione

Per garantire un livello ottimale di disponibilità e sicurezza sull'intero ciclo di vita, il sistema dovrà essere costantemente aggiornato agli standard più recenti e sottoposto a manutenzioni. Questo comporta la riparazione e la sostituzione di componenti hardware e software (p. es. in seguito a danni naturali o difetti tecnici), gli update di sicurezza e l'installazione di nuove versioni dei software. Le prestazioni necessarie quali ispezioni, manutenzioni, riparazioni e sviluppo di update saranno garantite in permanente sull'intero territorio della Svizzera da fornitori specializzati di servizi esterni e da organizzazioni field force. Gli specialisti lavorano secondo gli standard del settore informatico e i requisiti specifici del sistema.

Per la riparazione, la manutenzione e la sostituzione delle componenti, per le release e gli update del software e per le spese di locazione durante il ciclo di vita dei sistemi è preventivato il 15 percento dei costi annui d'esercizio e di manutenzione. I costi d'esercizio e di manutenzione dei vari elementi di rete nelle ubicazioni utenti sono stimati al cinque percento della base installata. A tale scopo sarà operativa 24 ore su 24 per 365 giorni all'anno una field force con vari ruoli. Con i fornitori di prestazioni e di prodotti andranno conclusi contratti esaustivi di manutenzione e d'assistenza. I collegamenti in fibre ottiche tra Cantoni e terzi sono prestazioni che richiedono contratti esaustivi di gestione di rete, di manutenzione e d'assistenza con i fornitori di servizi e prodotti e un elevato onere di coordinamento.

Secondo la regolamentazione delle competenze e del finanziamento, ogni utente devi assumersi l'esercizio delle componenti decentralizzate. Per la manutenzione delle ubicazioni utenti specifiche della Confederazione sono quindi preventivate annualmente spese complessive per 13,5 milioni di franchi dal 2023 fino al 2027. Con i fondi previsti verranno coperti i costi di manutenzione e d'esercizio specifici agli allacciamenti, per esempio la manutenzione dell'interfaccia tra le componenti decentralizzate e la componente centralizzata. Attualmente sono previsti 40 allacciamenti per la Confederazione. I costi per i 36 allacciamenti delle ubicazioni dei Cantoni, per i 43 allacciamenti delle infrastrutture critiche nonché per l'allacciamento del Principato del Liechtenstein sono, come per la Confederazione, a carico di questi enti.

Le spese funzionali dell'UFPP per l'esercizio e la manutenzione del sistema per lo scambio di dati sicuro aumentano nel 2020 di 100 000 franchi, nel 2021 di 600 000 franchi, nel 2022 di 1,5 milioni di franchi, nel 2023 di 7 milioni di franchi, nel 2024 di 10 milioni di franchi, nel 2025 di 12 milioni di franchi, nel 2026 di 13,9 milioni di franchi e dal 2027 di 15 milioni di franchi all'anno (cfr. tabella 4). Non sono inclusi i costi aggiuntivi necessari per il personale. I costi per i posti di lavoro ammontano a 1,7 milioni di franchi dal 2020 al 2028 (cfr. tabella 4).

2.2.7 Regolamentazione delle competenze e finanziamento

Il sistema nazionale per lo scambio di dati sicuro è un sistema di collegamento cui partecipano congiuntamente la Confederazione, i Cantoni, i gestori di infrastrutture critiche e terzi. Nei sistemi di collegamento si distingue tra componenti centralizzate e componenti decentralizzate. Le componenti centralizzate collegano tra loro gli utenti e sono condivise da tutti gli utenti. Le componenti decentralizzate sono utilizzate da organi federali (p. es. AFD), dai Cantoni e da terzi a titolo proprietario e permettono agli stessi di utilizzare le componenti centralizzate.

Il 10 gennaio 2017 il capo del DDPS e i presidenti delle conferenze governative CCDGP e CG MPP hanno indetto un gruppo di lavoro, composto da rappresentanti della Confederazione e dei Cantoni, incaricato di chiarire le competenze e le questioni finanziarie. In tale occasione è stata raggiunta una soluzione consensuale ed è stato concordato il finanziamento di base con i Cantoni. Quest'ultimi ordinano 36 allacciamenti alla Confederazione. Regolano tra loro la distribuzione dei 36 allacciamenti sui 26 Cantoni e la chiave di ripartizione intercantonale dei costi annuali d'esercizio e di manutenzione. Qui di seguito sono illustrate le regolamentazioni stabilite.

La Confederazione è responsabile delle componenti centralizzate dei sistemi di collegamento. Per le componenti decentralizzate sono invece responsabili la Confederazione (organi federali), i Cantoni, i gestori di infrastrutture critiche e terzi.

Per «investimenti» s'intendono tutte le spese necessarie per realizzare e introdurre un nuovo sistema. Per il sistema nazionale per lo scambio di dati sicuro si tratta di investimenti per edifici, cavi, hardware, software, gruppi elettrogeni d'emergenza, impianti di climatizzazione ecc. (vedi tabella 4). Le componenti centralizzate sono finanziate dalla Confederazione. Questi investimenti sono unici. In relazione al sistema per lo scambio di dati, vi rientrano gli investimenti per la rete di base (backbone) fino al punto di connessione a un'ubicazione utente (allacciamento), gli investimenti per il sistema di accesso ai dati e gli investimenti per la sostituzione del sistema di messaggistica Vulpus e per il sistema di analisi integrata della situazione. Gli investimenti delle componenti decentralizzate sono finanziati dai Cantoni, dai gestori di infrastrutture critiche e da terzi. Vi rientra anche la sicurezza dell'alimentazione con corrente elettrica delle ubicazioni utenti collegate. Gli allacciamenti delle componenti decentralizzate di organi federali sono finanziati dalla Confederazione. Nel presente messaggio si chiede il finanziamento dei costi associati.

L'esperienza insegna che, allo scadere del ciclo di vita di un sistema, si rendono necessarie misure di salvaguardia del valore. Queste hanno carattere d'investimento. Per «salvaguardia del valore» s'intendono pertanto reinvestimenti importanti che possono rendersi necessari entro sei–otto anni dopo il primo investimento. Questi costi corrispondono circa al 60 percento dei primi costi d'investimento rilevanti e sono finanziati dalla Confederazione per quanto concerne le componenti centralizzate. I Cantoni e terzi assumono da parte loro i costi di manutenzione per le componenti decentralizzate. Lo stesso vale per gli organi federali che dispongono di componenti decentralizzate.

Per «costi d'esercizio e di manutenzione annui» s'intendono le spese necessarie per garantire l'esercizio sicuro e privo di interruzioni dei sistemi. Vi rientrano ad esempio la manutenzione dei sistemi, la loro sorveglianza, la gestione dell'assistenza e delle emergenze, gli update dei software e le patch di sicurezza. Le spese d'ammortamento sono esplicitamente escluse. Si parte dal presupposto che, durante il ciclo di vita dei sistemi, circa il 15 percento dei costi d'esercizio e di manutenzione annui venga impiegato per misure di salvaguardia del valore. I costi annui d'esercizio e di manutenzione delle componenti centralizzate del sistema per lo scambio di dati sicuro sono proporzionalmente finanziati da tutti gli utenti allacciati. L'esercizio e la manutenzione delle componenti decentralizzate sono finanziati di tasca propria dai Cantoni, dai gestori di infrastrutture critiche e da terzi nonché dalla Confederazione per gli organi federali allacciati.

I costi annui d'esercizio e di manutenzione delle componenti centralizzate della rete per lo scambio di dati sicuro, del sistema d'accesso ai dati, della sostituzione del sistema di messaggistica Vulpus e del sistema di analisi integrata della situazione sono assunti per il 30 percento dai Cantoni, per circa il 40 percento dalla Confederazione e per circa il 30 percento dai gestori delle infrastrutture critiche. I Cantoni sono quindi autorizzati a realizzare al massimo 36 allacciamenti a questo sistema. Da parte loro, la Confederazione, i gestori delle infrastrutture critiche e terzi hanno diritto a circa 80 fino a 90 allacciamenti. Il finanziamento è ripartito proporzionalmente. Un'eventuale realizzazione di allacciamenti oltre ai 120 pianificati implica l'adeguamento della chiave di ripartizione secondo lo stesso principio.

Tabella 3

Investimento, salvaguardia del valore, esercizio e manutenzione

	Investimento	Salvaguardia del valore (reinvestimento)	Esercizio e manutenzione
Oggetti d'investimento	Edifici, impianti di climatizzazione, gruppi elettrogeni, hardware, software, licenze ecc.	Sostituzione ordinaria, hardware (p. es. router), software ecc.	Manutenzione, release/ update dei software, pezzi di ricambio, spese di locazione ecc.
Frequenza	unico[6]	ca. ogni 6–8 anni	annuale
Finanziamento	Componenti centralizzate: Confederazione Componenti decentralizzate: organi federali, Cantoni e terzi	Componenti centralizzate: Confederazione Componenti decentralizzate: organi federali, Cantoni e terzi	Componenti centralizzate: utenti (Confederazione con terzi[7]/Cantoni: 70/30) Componenti decentralizzate: organi federali, Cantoni e terzi

3 Ripercussioni

3.1 Ripercussioni per la Confederazione

3.1.1 Ripercussioni finanziarie

I costi d'investimento della Confederazione per lo sviluppo e l'acquisto ammontano a 150 milioni di franchi. Rimangono salve le nostre decisioni nell'ambito dell'aggiornamento dei prossimi preventivi con il piano integrato dei compiti e delle finanze.

Il credito d'impegno si fonda sull'indice nazionale dei prezzi al consumo del dicembre 2017 (100,8 punti; dic. 2015 = 100 punti). La stima si basa sulla previsione di un tasso di rincaro pari all'1 percento dal 2020.

Il credito sarà liberato in tre tranche. La prima tranche verrà liberata con il decreto federale relativo al presente messaggio. Il nostro Collegio deciderà in merito alla liberazione delle altre tranche sulla base dei progressi del progetto.

Nel 2020 e nel 2021 sono previste spese aggiuntive pari a, rispettivamente 100 000 e 600 000 milioni di franchi per l'esercizio e la manutenzione, poiché sin dalla fase di pianificazione si dovranno finanziare le spese d'esercizio nell'ambito del Proof of Concept e quelle necessarie per preparare la fase di prova negli anni successivi. Dal 2022 al 2027 aumenteranno progressivamente e dal 2028 ammonteranno a 15 milioni di franchi all'anno (senza prestazioni proprie) per il regolare esercizio. Le spese d'esercizio sono illustrate nella tabella 4.

6 Oppure cicli molto lunghi, nell'ordine di decenni, p. es. per la ristrutturazione di edifici.
7 Confederazione con gestori di infrastrutture critiche e terzi.

Le prestazioni proprie dell'Amministrazione federale sotto forma di spese per il personale ammonteranno in media a 4,3 milioni di franchi all'anno dal 2020 e a 4,1 milioni di franchi all'anno per il regolare esercizio dal 2028.

Le spese complessive della Confederazione per gli anni dal 2020 fino alla fine del progetto nel 2027 ammonteranno a 241,5 milioni di franchi lordi. Né gli investimenti, né l'esercizio potranno essere interamente finanziati con i mezzi attualmente disponibili del DDPS (UFPP).

Con la disattivazione del sistema di messaggistica Vulpus, a partire dal 2026 verranno a cadere costi d'esercizio pari a 1,5 milioni di franchi all'anno. Durante il cambio del sistema (2025) verrà garantito un esercizio parallelo.

A partire dalla piena operatività della rete di base nel 2026, i Cantoni saranno chiamati a partecipare ai costi d'esercizio e di manutenzione del sistema nazionale per lo scambio di dati sicuro con un contributo annuo di 4,5 milioni di franchi per 36 allacciamenti. Ciò corrisponde a un costo medio annuo di circa 125 000 franchi per allacciamento di ubicazione utenti. Vi rientrano i costi per le prestazioni proprie della Confederazione e le spese d'esercizio e di manutenzione. Non sono invece inclusi i costi d'allacciamento, che devono essere sostenuti dagli utenti stessi. Alla Confederazione vengono accreditati anche i contributi dei gestori di infrastrutture critiche e terzi che intendono usufruire del sistema. In caso di approvazione dei 120 allacciamenti complessivamente previsti (36 per i Cantoni, uno per il Principato del Liechtenstein, 40 per gli uffici federali e 43 per i gestori di infrastrutture critiche), ciò si tradurrebbe in contributi annui di dieci milioni di franchi a favore della Confederazione, escluso il supplemento di rischio.

Tabella 4

Spese complessive per il sistema nazionale per lo scambio di dati sicuro tra il 2020 e il 2027 in milioni di franchi

In mio. di CHF	2020	2021	2022	2023	2024	2025	2026	2027	Totale
Spese complessive	9,2	11,7	28,9	38,0	48,1	41,9	33,6	30,1	241,5
Investimenti	6,8	7,9	23,8	26,9	32,9	24,7	15,8	11,2	150,0
Gestione del progetto	3,1	3,4	4,8	4,8	4,5	3,7	3,4	1,8	29,5
Lavori di sviluppo	1,5	1,0	4,4	3,0	4,0	2,8	0,5	0,5	17,7
Hardware, software, licenze	0,8	1,0	1,0	2,0	2,5	2,5	2,5	2,5	14,8
Infrastruttura di rete backbone	0,0	0,0	1,5	2,8	1,6	0,5	0,0	0,0	6,4
Infrastruttura di rete ubicazioni utenti	0,0	0,0	4,0	6,8	8,0	8,0	5,5	3,4	35,7
Gestione della rete	0,0	1,0	2,0	1,0	1,0	2,0	0,8	0,5	8,3
Ubicazioni utenti Confederazione	0,5	0,5	3,0	3,0	7,0	2,0	1,0	1,0	18,0
Supplemento di rischio (25 %)	0,9	1,0	3,1	3,5	4,3	3,2	2,1	1,5	19,6
Spese d'esercizio e manutenzione	0,1	0,6	1,5	7,0	10,0	12,0	13,9	15,0	60,1
Esercizio e manutenzione	0,0	0,4	1,0	5,8	8,3	9,3	9,6	10,7	45,1
Costi per posti di lavoro	0,1	0,2	0,2	0,2	0,2	0,2	0,2	0,2	1,7
Ubicazioni utenti Confederazione	0,0	0,0	0,3	1,0	1,5	2,5	4,1	4,1	13,5
Prestazioni proprie	2,3	3,2	3,6	4,1	5,2	5,2	5,4	5,4	34,4
Personale (15 FTE esistente)	0,9	0,9	0,9	1,4	2,5	2,5	2,7	2,7	14,5
Personale (15 FTE supplementari)	1,4	2,3	2,7	2,7	2,7	2,7	2,7	2,7	19,9
Disattivazione del sistema di messaggistica Vulpus	0,0	0,0	0,0	0,0	0,0	0,0	-1,5	-1,5	-3,0

3.1.2 Ripercussioni sull'organico

Affinché il progetto possa essere realizzato nei tempi previsti e conformemente alle direttive finanziarie e qualitative e l'esercizio del sistema nazionale per lo scambio di dati sicuro possa essere garantito 24 ore su 24 su tutto il territorio nazionale in

collaborazione con i fornitori di prestazioni (BAC e fornitori esterni), dal 2028 saranno probabilmente necessari 25 posti di lavoro. Una buona parte di essi è indispensabile per garantire l'esercizio del sistema in situazioni particolari e straordinarie. La realizzazione e l'esercizio del sistema per lo scambio di dati sicuro richiedono 30 posti fissi a tempo pieno presso il DDPS (UFPP e BAC) nel periodo dal 2024 al 2027 in cui la fase di realizzazione e quella di esercizio si sovrapporranno fortemente. Di questi, 15 sono compensati in permanenza internamente al DDPS. Gli altri 15 posti a tempo pieno saranno aggiunti nella fase di progetto, di cui dieci rimarranno in permanenza a partire dal regolare esercizio. Senza questo rinforzo l'UFPP e la BAC non potrebbero gestire l'onere di lavoro supplementare.

Trattandosi di un progetto di portata nazionale molto complesso nel campo della sicurezza, è estremamente importante raggiungere la massima autonomia e garantire internamente il mantenimento del know-how e l'evoluzione tecnologica nelle competenze chiave. Nonostante si preveda di affidare compiti e perizie non essenziali e limitati nel tempo a fornitori di prestazioni esterni, secondo le raccomandazioni formulate nel rapporto del 24 giugno 2015[8] delle Commissioni delle finanze e della gestione delle Camere federali sul nostro parere del 25 febbraio 2015 e sul parere del CFF del 24 febbraio 2015 in merito al progetto informatico «Insieme», occorre tuttavia garantire che i ruoli chiave e il relativo know-how rimangano all'interno della Confederazione. Il nostro Collegio intende seguire tale raccomandazione nel limite delle risorse disponibili. Aumentando l'organico è possibile assumere la responsabilità interna delle applicazioni, garantire la gestione degli attori interessati e sviluppare le competenze necessarie per l'esercizio, la salvaguardia del valore e lo sviluppo.

Per realizzare, sviluppare e garantire la futura salvaguardia del valore della rete per lo scambio di dati, del sistema di accesso ai dati, del sistema di analisi integrata della situazione e della gestione dei beneficiari delle prestazioni (organi federali, Cantoni, gestori di infrastrutture critiche) nonché per fornire le prestazioni necessarie nella fase d'esercizio, l'UFPP necessita complessivamente di 10 posti di lavoro supplementari a tempo pieno, che dal 2028 saranno necessari per il regolare esercizio. Nella fase d'esercizio sono previsti sei posti per la rete per lo scambio di dati sicuro e il sistema d'accesso e quattro per l'analisi integrata della situazione. Questi saranno presi dal pool del personale della fase di progetto e trasferiti nella fase d'esercizio. Dal canto suo la BAC necessita di 5 posti supplementari a tempo pieno per l'esercizio in tutte le situazioni del sistema per lo scambio di dati sicuro e al fine di garantire un servizio d'emergenza 24 ore su 24 per 365 giorni all'anno. Questi saranno compensati internamente al DDPS a partire dal regolare esercizio nel 2028.

L'UFPP non necessita di spazi supplementari. Il fabbisogno di spazi per i posti supplementari richiesti nell'ambito del sistema per lo scambio di dati sicuro può essere compensato con la riorganizzazione dell'UFPP e il trasloco della CENAL da Zurigo a Berna tenendo conto delle postazioni di lavoro condivise e delle sinergie. Nemmeno la BAC necessita da parte sua di spazi supplementari.

Il coordinamento generale e la responsabilità del progetto competono all'UFPP.

8 FF **2016** 3737

Il DDPS dovrà assumere ulteriori compiti complessi e responsabilità in diversi ambiti: la realizzazione del sistema e il suo esercizio devono essere coordinati con i fornitori di prestazioni, per esempio con i proprietari di linee in fibra ottica e di infrastrutture e con i beneficiari di prestazioni. Occorre condurre negoziati e stipulare contratti. I prodotti forniti devono essere collaudati e testati. Si deve inoltre garantire la gestione dell'esercizio e la manutenzione, nonché la gestione della sicurezza e della qualità.

Per la direzione generale del progetto e il coordinamento dei sottoprogetti è designato un responsabile di progetto.

Per gestire i quattro sottoprogetti sono designati altrettanti responsabili di sottoprogetto. I responsabili di sottoprogetto assistono gli utenti e i gestori di infrastrutture critiche a livello federale e cantonale nella pianificazione, nell'attuazione presso le ubicazioni e nella messa in esercizio. Sono inoltre responsabili dell'interfaccia del sistema per lo scambio di dati sicuro con le reti delle organizzazioni utenti.

I responsabili della gestione dei mandati fungono da interlocutori per gli utenti in caso di domande sui mandati ricevuti e si occupano del disbrigo dei mandati.

I manager dei prodotti sorvegliano l'andamento del mercato ed elaborano previsioni rilevanti per la realizzazione e l'ulteriore sviluppo del sistema per lo scambio di dati sicuro. Accertano le esigenze degli organi federali, dei Cantoni e dei gestori di infrastrutture critiche per l'intera durata del progetto.

I manager d'esercizio provvedono, d'intesa con le autorità e le organizzazioni federali e cantonali ed i gestori di infrastrutture critiche, a coordinare l'esercizio, i test e i collaudi. Sono responsabili della gestione delle modifiche, delle release e della configurazione e introducono nuove versioni di software e hardware. Coordinano l'esercizio dell'intera rete con tutte le applicazioni degli utenti della Confederazione, dei Cantoni e dei gestori di infrastrutture critiche.

I responsabili del service management stipulano accordi di prestazione con i fornitori (BAC e industria) e ne verificano l'osservanza.

I network operation manager gestiscono e sorvegliano la rete per lo scambio di dati sicuro e il sistema d'accesso. Si occupano in tal senso della gestione degli errori, della gestione della configurazione, della gestione delle prestazioni e della gestione della sicurezza.

I service assurance manager garantiscono la fornitura delle prestazioni agli utenti. Assicurano e coordinano la gestione degli eventi e dei problemi con i fornitori delle prestazioni nonché la comunicazione con gli utenti.

I manager della sicurezza e della qualità elaborano direttive rilevanti in materia di sicurezza, applicano le direttive delle Strategie nazionali del 27 giugno 2012[9] e del 18 aprile 2018 per la protezione della Svizzera contro i ciber-rischi e sono garanti della qualità. Durante l'intero periodo d'esercizio individuano misure di miglioramento e ne verificano l'attuazione.

9 I testi delle strategie sono disponibili in internet all'indirizzo: www.isb.admin.ch > Temi > Ciber-rischi SNPC > Strategia SNPC 2012–2017 risp. Strategia SNPC 2018–2022.

I responsabili della gestione dei contratti conducono trattative e stipulano contratti con i fornitori di prestazioni (BAC e industria) e tutti gli utenti della Confederazione, dei Cantoni e dei gestori di infrastrutture critiche. Sbrigano inoltre le pratiche contrattuali e garantiscono il rispetto dei contenuti.

Per l'accompagnamento del progetto ci si avvale di un responsabile del controlling del progetto. Questo è responsabile del reporting ed assume contemporaneamente compiti trasversali. Si occupa inoltre del coordinamento con i settori Finanze, Acquisti e Diritto.

La sorveglianza degli eventi e delle minacce nel ciberspazio per l'intera infrastruttura TIC è assicurata dal fornitore di servizi del DDPS, ossia dalla BAC.

Nella fase d'esercizio, diverse funzioni richieste nella fase di progetto svilupperanno la gestione dei beneficiari delle prestazioni della Confederazione, dei Cantoni e dei gestori di infrastrutture critiche (cfr. tabella 6).

Tabella 5

Fabbisogno supplementare di personale e funzioni all'anno fino alla conclusione del progetto e per il regolare esercizio

Posti per il progetto	Progetto	2020	2021	2022	2023	2024	2025	2026	2027	2028
Responsabile di progetto	SSDS & SAD (UFPP)	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	
	SSDS & SAD (BAC)	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	
	AIS/Vulpus (UFPP)									
Responsabile di sottoprogetto	SSDS & SAD (UFPP)	3.0	3.0	3.0	2.0	2.0	2.0	1.5	1.5	
	SSDS & SAD (BAC)	1.0	2.0	2.0	2.0	2.0	2.0	1.0	1.0	
	AIS/Vulpus (UFPP)	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	
Responsabile della gestione dei mandati	SSDS & SAD (UFPP)	1.0	1.25	1.5	1.5	1.25				
	SSDS & SAD (BAC)									
	AIS/Vulpus (UFPP)	1.0	1.0	0.75	0.75					
Manager dei prodotti	SSDS & SAD (UFPP)	1.0	1.0	1.25	1.5	1.0	1.0	1.0	1.0	
	SSDS & SAD (BAC)									
	AIS/Vulpus (UFPP)	1.0	1.0	1.5	1.5					
Manager d'esercizio	SSDS & SAD (UFPP)	0.5	0.5	0.5						
	SSDS & SAD (BAC)									
	AIS/Vulpus (UFPP)		0.5	0.5						
Responsabile del service management	SSDS & SAD (UFPP)									
	SSDS & SAD (BAC)		0.5	0.5						
	AIS/Vulpus (UFPP)			1.0	1.0					
Network Operation Manager	SSDS & SAD (UFPP)									
	SSDS & SAD (BAC)		0.5							
	AIS/Vulpus (UFPP)									
Manager della sicurezza e della qualità	SSDS & SAD (UFPP)	1.0	1.0	1.0	0.75	0.75	0.75	0.75	0.75	
	SSDS & SAD (BAC)		1.0	1.0	1.0					
	AIS/Vulpus (UFPP)		0.5	0.25						
Responsabile della gestione dei contratti	tutti i progetti	0.25	1.00	1.25	1.00	0.75	0.25	0.25	0.25	
Responsabile del controlling	tutti i progetti	0.25	0.25	0.50	0.75	0.75	0.75	1.00	1.00	
Totale dei posti per il progetto		13	18	19.5	16.75	11.5	9.75	8.5	8.5	0.0

Continuazione della tabella 5

Posti per l'esercizio	Esercizio	2020	2021	2022	2023	2024	2025	2026	2027	2028
Responsabile di sottoprogetto	SSDS & SAD (UFPP)									1.0
	SSDS & SAD (BAC)									1.0
	AIS/Vulpus (UFPP)									
Responsabile della gestione dei mandati	SSDS & SAD (UFPP)						1.0	1.0	1.0	1.0
	SSDS & SAD (BAC)									
	AIS/Vulpus (UFPP)					0.5	0.5	0.5	0.5	
Manager dei prodotti	SSDS & SAD (UFPP)					1.0	1.0	1.0	1.0	1.0
	SSDS & SAD (BAC)									1.0
	AIS/Vulpus (UFPP)					1.25	1.25	1.25	1.25	0.75
Manager d'esercizio	SSDS & SAD (UFPP)				1.0	1.0	1.75	2.0	2.0	1.5
	SSDS & SAD (BAC)									
	AIS/Vulpus (UFPP)				0.5	1.0	1.0	1.0	1.0	1.0
Responsabile del service management	SSDS & SAD (UFPP)									1.0
	SSDS & SAD (BAC)				1.5	2.0	2.0	2.0	2.0	2.0
	AIS/Vulpus (UFPP)					1.0	1.0	1.0	1.0	1.0
Service Assurance Manager	SSDS & SAD (UFPP)									
	SSDS & SAD (BAC)					1.0	1.0	2.0	2.0	2.0
	AIS/Vulpus (UFPP)									
Network Operation Manager	SSDS & SAD (UFPP)									
	SSDS & SAD (BAC)			0.5	2.5	8.0	8.0	9.0	9.0	9.0
	AIS/Vulpus (UFPP)									
Manager della sicurezza e della qualità	SSDS & SAD (UFPP)				0.5	0.5	0.5	0.5	0.5	0.5
	SSDS & SAD (BAC)									
	AIS/Vulpus (UFPP)				0.25	0.25	0.25	0.25	0.25	0.25
Responsabile della gestione dei contratti	tutti i sistemi									0.25
Responsabile del controlling	tutti i sistemi									0.75
Totale dei posti per l'esercizio		0.0	0.0	0.5	6.25	17.5	19.25	21.5	21.5	25.0
Totale dei posti all'anno (progetto + esercizio)		**13**	**18**	**20**	**23**	**29**	**29**	**30**	**30**	**25**

3.2 Ripercussioni per i Cantoni

La Confederazione si fa carico dei costi d'investimento delle componenti centralizzate del sistema per lo scambio di dati sicuro. I Cantoni assumono invece i costi d'investimento delle componenti decentralizzate nei Cantoni, ad esempio per rafforzare le loro ubicazioni utenti. Essi assicurano l'allacciamento di uffici cantonali,

Comuni, città ecc. al sistema tramite le loro reti. L'allacciamento delle componenti decentralizzate dei Cantoni a quelle centralizzate avviene a tappe. I costi d'investimento e i costi d'esercizio annui nonché i costi di manutenzione per le componenti decentralizzate nei Cantoni dipendono dall'infrastruttura esistente e dalle esigenze dei singoli Cantoni. I dettagli relativi ai costi sono stati presentati nel numero 3.1.1.

3.3 Ripercussioni per l'economia

La realizzazione del sistema nazionale per lo scambio di dati sicuro porta notevoli vantaggi anche a livello economico. Un'interruzione delle prestazioni TIC su vasta scala potrebbe infatti paralizzare l'economia del Paese. Numerose aziende, in particolare i gestori di infrastrutture critiche, sono dotate di generatori di corrente d'emergenza per far fronte a eventuali interruzioni di corrente. L'alimentazione di corrente d'emergenza garantisce l'esercizio autonomo per un certo tempo ma non assicura il collegamento con le organizzazioni partner, le autorità ecc. Negli ultimi anni, lo scambio elettronico di dati tra le organizzazioni e le aziende è aumentato considerevolmente e continuerà a crescere per tenere il passo con la digitalizzazione. Con la realizzazione del sistema nazionale per lo scambio di dati sicuro si crea una piattaforma per le autorità e i gestori di infrastrutture critiche che vogliono o devono garantire la capacità di connessione dei loro sistemi anche in caso d'interruzione di corrente. Questa rete può e deve essere utilizzata anche in situazioni normali. Con la realizzazione del sistema per lo scambio di dati sicuro si evita che i diversi utenti attuino soluzioni individuali ridondanti. Tutto ciò rappresenta un notevole valore aggiunto per l'economia del Paese.

3.4 Ripercussioni per la società

La realizzazione del sistema nazionale per lo scambio di dati sicuro non solo migliora l'affidabilità dei sistemi di telecomunicazione e lo scambio sicuro dei dati tra organi di condotta, autorità e organizzazioni d'intervento ma aumenta in definitiva anche la sicurezza per la popolazione. In caso di catastrofe o di emergenza sarebbe possibile ridurre considerevolmente l'entità dei danni a persone, animali e beni materiali. In questo modo si colmerebbe una lacuna in materia di sicurezza nella protezione della popolazione.

3.5 Ripercussioni per l'ambiente

Oltre all'impatto ambientale della logistica dei trasporti, il progetto non ha ripercussioni significative sull'ambiente. La tecnologia è basata su una rete in fibra ottica e non richiede nuove antenne. Non è pertanto previsto un aumento delle radiazioni non ionizzanti.

4 Relazione con il programma di legislatura e le strategie del Consiglio federale

4.1 Relazione con il programma di legislatura

Il progetto è riportato nel numero 5.3.5 del messaggio del 27 gennaio 2016[10] sul programma di legislatura 2015–2019. La strategia del Consiglio federale intende perfezionare gli strumenti della politica di sicurezza in modo da garantire in qualsiasi momento una reazione efficace agli eventi. Questo presuppone anche una cooperazione ottimale tra tutti i partner e una collaborazione efficace tra tutte le parti coinvolte nella politica di sicurezza. Uno strumento essenziale a tal fine è costituito da uno scambio garantito d'informazioni e di quadri della situazione tra tutte le parti coinvolte. Ciò sarà reso possibile grazie al sistema per lo scambio di dati sicuro.

Secondo l'obiettivo 16 del decreto federale del 14 giugno 2016[11] sul programma di legislatura 2015–2019 «La Svizzera è al corrente delle minacce interne ed esterne alla propria sicurezza e dispone degli strumenti necessari per fronteggiarle in modo efficace». La misura 65 del programma prevede l'approvazione del messaggio concernente la modifica della legge federale sulla protezione della popolazione e sulla protezione civile. Il messaggio sulla LPPC comprende anche le basi giuridiche per la realizzazione del sistema nazionale per lo scambio di dati sicuro con l'analisi nazionale integrata della situazione.

4.2 Relazione con gli obiettivi del Consiglio federale 2018

Considerata l'urgenza dell'affare, il Consiglio federale ha inserito tra gli Obiettivi del Consiglio federale 2018 (parti I e II) del 23 novembre 2017[12] l'elaborazione di un messaggio al riguardo e il 1° dicembre 2017 ha incaricato l'UFPP di elaborarlo nel 2018.

4.3 Relazione con le strategie del Consiglio federale

A causa dei cambiamenti climatici si prevede che, in futuro, la frequenza e l'intensità[13] degli eventi naturali aumenteranno. Questa situazione richiede che siano prese misure di adeguamento.[14] La protezione delle infrastrutture di informazione e comunicazione contro il progressivo aumento dei ciber-rischi è diventata una preoccu-

10 FF **2016** 909
11 FF **2016** 4605
12 Il testo degli obiettivi è disponibile nel sito: www.bk.admin.ch > Documentazione > Condotta strategica > Obiettivi annuali.
13 Köllner P., Gross C., Schäppi B., Füssler J., Lerch J., Nauser M. 2017: Rischi e opportunità legati ai cambiamenti climatici. Sintesi nazionale. Ufficio federale dell'ambiente, Berna. Studi sull'ambiente n. 1706: 148 pagg.
14 Cfr. Strategia del Consiglio federale di adattamento ai cambiamenti climatici in Svizzera 2014–2019, disponibile in internet all'indirizzo www.bafu.admin.ch > Temi > Clima > Informazioni per gli specialisti > Adattamento ai cambiamenti climatici > Strategia del Consiglio federale.

pazione a livello nazionale.[15] Nel rapporto sulla Strategia della protezione della popolazione e della protezione civile 2015+, approvato dal nostro Collegio il 9 maggio 2012[16], è stato pertanto formulato l'obiettivo di acquisire sistemi di telecomunicazione affidabili. La strategia «Svizzera digitale» dell'aprile 2016[17] sostiene che nell'era digitale lo Stato deve essere in grado di proteggere efficacemente la popolazione e l'economia. In tal senso, il sistema nazionale per lo scambio di dati sicuro contribuirà in modo significativo a rafforzare la resilienza dei sistemi di telecomunicazione e dei gestori delle infrastrutture critiche nel campo della sicurezza. Il rafforzamento della resilienza è auspicato dalla «Strategia nazionale per la protezione delle infrastrutture critiche 2018–2022»[18] e dalla «Strategia nazionale per la protezione della Svizzera contro i ciber-rischi». Una rete di dati e di comunicazione garantita in caso d'interruzione della corrente elettrica, che permette di collegare i gestori delle infrastrutture critiche, è un obiettivo e una misura esplicita della Strategia per la protezione delle infrastrutture critiche 2018–2022, approvata dal nostro Collegio l'8 dicembre 2017. Il sistema nazionale per lo scambio di dati sicuro consente di mantenere, in caso d'interruzione delle telecomunicazioni pubbliche, i processi rilevanti per l'esercizio delle infrastrutture critiche e la comunicazione tra i gestori di infrastrutture critiche e le organizzazioni preposte alla gestione delle crisi a livello federale e cantonale. Anche il rapporto del nostro Collegio sui pericoli naturali in Svizzera[19] e la Strategia contro i pericoli naturali[20] propongono una rete di dati e di comunicazione a prova d'interruzione e di guasto come misura per aumentare la resilienza contro i pericoli naturali.

Il 4 dicembre 2015 il nostro Collegio ha approvato la Strategia TIC 2016–2019.[21] Nell'ambito dell'orientamento «S03 – Fornitura di prestazioni TIC» di questa strategia, è stata elaborata una strategia TIC per le reti della Confederazione «*Netzwerke des Bundes*», che abbiamo approvato contemporaneamente al presente messaggio. La stessa espone le esigenze poste alle reti della Confederazione e stabilisce con quali reti nazionali dovranno essere soddisfatte. Il progetto «Sistema per lo scambio di dati sicuro» è parte integrante della strategia TIC per le reti della Confederazione ed è pertanto armonizzato con essa. I dettagli saranno armonizzati nell'ambito dei prossimi lavori di progetto.

Per le reti ottiche di trasporto dei dati a lunga distanza, la Confederazione punta fondamentalmente su due infrastrutture, conformemente alla strategia per le reti della Confederazione. La prima è la rete di condotta Svizzera, che fornisce presta-

15 Strategie nazionali per la protezione della Svizzera contro i ciber-rischi 2012–2017 e 2018–2022, disponibile in Internet all'indirizzo: www.isb.admin.ch > Temi > Ciber-rischi SNPC > Strategia SNPC 2018–2022 o Strategia SNPC 2012–2017.
16 FF **2012** 4849
17 FF **2016** 3515
18 Il testo della Strategia dell'8 dic. 2017 è disponibile in Internet all'indirizzo: www.babs.admin.ch > Altri campi d'attività > protezione delle infrastrutture critiche > Strategia nazionale PIC.
19 Il rapporto è disponibile in Internet all'indirizzo: www.bafu.admin.ch > Temi > Tema Pericoli naturali > Dossier > Pericoli naturali in Svizzera: come agire per la nostra sicurezza? > Rapporto del Consiglio federale «Pericoli naturali in Svizzera 2016».
20 La strategia è disponibile in Internet all'indirizzo: www.planat.ch > Strategia 2018.
21 Il testo della Strategia è disponibile in Internet all'indirizzo: www.isb.admin.ch > Temi > Strategia e pianificazione TIC > Strategia TIC della Confederazione 2016–2019.

zioni solide e molto sicure a favore dell'esercito. La seconda è la cosiddetta rete ottica delle autorità federali (Optisches Behördennetz Bund), che offre connessioni ottiche resilienti in caso di interruzioni di corrente e altamente sicure agli organi federali, ai Cantoni, ai gestori di infrastrutture critiche e a terzi autorizzati che necessitano di connessioni dati per collaborare tra loro. Questa rete ottica delle autorità sarà realizzata in una prima fase nel quadro di tre progetti: il sistema nazionale per lo scambio di dati sicuro, l'interconnessione delle installazioni per l'esercizio e la sicurezza lungo le strade nazionali e l'interconnessione dei centri di elaborazione dati per scopi civili.

Queste reti di trasporto dati a fibra ottica sfruttano, per quanto possibile, l'infrastruttura di fibre ottiche esistente della rete di condotta Svizzera e delle strade nazionali. Questa soluzione permette di sfruttare diverse sinergie. Da un lato consente un uso multiplo di infrastrutture federali in gran parte già esistenti; dall'altro, le prestazioni d'esercizio per queste due infrastrutture vengono fornite da un unico fornitore di servizi (la BAC). La BAC dispone delle risorse e delle capacità necessarie per l'esercizio delle reti ottiche di trasporto dati e garantisce l'esercizio anche in situazioni particolari e straordinarie.

A medio-lungo termine occorre possibilmente realizzare e gestire una piattaforma IP integrata per le reti IP che sono necessarie per le connessioni tra Confederazione e Cantoni e le connessioni tra Cantoni. Ciò consente di evitare un aumento della complessità delle connessioni o delle interfacce con i Cantoni e di sfruttare le sinergie esistenti nel settore delle infrastrutture e dell'esercizio.

Su questa piattaforma IP sarà possibile implementare e gestire più sottoreti IP o connessioni tra loro isolate. Il ruolo operativo di questa piattaforma IP integrata e delle sottoreti basate su di essa deve ancora essere definito. La BAC e l'UFIT collaborano strettamente, coinvolgendo anche l'UFPP, alla realizzazione di un modello d'esercizio e di collaborazione entro la fine del 2019. A tal fine occorre definire anche i compiti organizzativi e procedurali, le interfacce, le competenze e le responsabilità, tenendo conto delle esigenze poste dalle diverse applicazioni rilevanti per la sicurezza (esercizio anche in situazioni particolari e straordinarie), delle condizioni vincolanti prescritte dalla nuova legge sulla protezione della popolazione e sulla protezione civile (LPPC) e dall'informatica federale nonché dalle normative stabilite nei servizi standard.

5 Aspetti giuridici

5.1 Costituzionalità e legalità

Conformemente all'articolo 167 della Costituzione federale[22] (Cost.), la decisione concernente il credito compete all'Assemblea federale.

Nel messaggio concernente la LPPC si è tenuto conto della proposta di ripartizione delle competenze e dei compiti tra Confederazione, Cantoni e terzi e della ripartizione dei costi (cfr. n. 2.2.7). Tale messaggio sarà presentato al Parlamento in una

22 RS **101**

domanda separata, parallelamente al presente messaggio. Per evitare che Cantoni e terzi realizzino sistemi propri implicanti, come con Polycom, un notevole dispendio di tempo e di risorse al fine di riunirli successivamente in un sistema nazionale, la Confederazione potrà definire degli standard per i sistemi. Essa avrà inoltre la possibilità di emanare direttive tecniche e temporali per questi sistemi di collegamento.

5.2 Forma dell'atto

Conformemente all'articolo 163 capoverso 2 Cost. e all'articolo 25 capoverso 2 della legge del 13 dicembre 2002[23] sul Parlamento, per l'atto normativo interessato è prevista la forma del decreto federale semplice che, pertanto, non sottostà al referendum.

5.3 Subordinazione al freno alle spese

Conformemente all'articolo 159 capoverso 3 lettera b Cost., l'articolo 1 del decreto federale concernente il credito d'impegno necessita del consenso della maggioranza dei membri di ciascuna Camera, dato che comporta uscite uniche che superano i 20 milioni di franchi.

23 RS **171.10**

Abbreviazioni

AFD	Amministrazione federale delle dogane
AIS	Analisi integrata della situazione
BAC	Base d'aiuto alla condotta dell'esercito
BCM	Business Continuity Management
CCDGP	Conferenza dei capi dei dipartimenti di giustizia e polizia
CENAL	Centrale nazionale d'allarme
CFF	Controllo federale delle finanze
Cgcf	Corpo delle guardie di confine
CG MPP	Conferenza governativa per gli affari militari, la protezione civile e i pompieri
DDPS	Dipartimento federale della difesa, della protezione della popolazione e dello sport
DelFin	Delegazione delle finanze
ECS	Esercitazione di condotta strategica
ERSS	Esercitazione della Rete integrata per la sicurezza
fedpol	Ufficio federale di polizia
FTE	Full Time Equivalent (equivalente a tempo pieno)
IBBK	Information der Bevölkerung durch den Bund in Krisenlagen (informazione della popolazione da parte della Confederazione in caso di crisi)
IP	Internet Protocol
KomBV-KTV	Kommunikationsnetz Bundesverwaltung–Kantonalverbund (rete di comunicazione tra i Cantoni e l'Amministrazione federale)
LPPC	Legge federale sulla protezione della popolazione e sulla protezione civile
MeteoSvizzera	Ufficio federale di meteorologia e climatologia
NCC	Network Control Center
PES	Presentazione elettronica della situazione
PRZ	Prüf- und Referenz Zenter (centro di prova e di riferimento)
RSDS	Rete per lo scambio di dati sicuro
SAD	Sistema di accesso ai dati
SIC	Servizio delle attività informative della Confederazione
SMFP	Stato maggiore federale Protezione della popolazione
SOC	Security Operation Center
SSDS	Sistema per lo scambio di dati sicuro
TIC	Tecnologie d'informazione e di comunicazione

UFAM	Ufficio federale dell'ambiente
UFE	Ufficio federale dell'energia
UFPP	Ufficio federale della protezione della popolazione
USTRA	Ufficio federale delle strade