Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

Berna, 16 novembre 2022

Revisione dell'ordinanza sui servizi di telecomunicazione (OST)

Rapporto sui risultati della procedura di consultazione (dal 3 dicembre 2021 al 18 marzo 2022)

Indice

1 Situazione iniziale

L'articolo 48*a* della legge sulle telecomunicazioni conferisce al Consiglio federale la competenza di disciplinare la sicurezza delle informazioni nonché delle infrastrutture e dei servizi di telecomunicazione. Il 3 dicembre 2021, l'Esecutivo ha posto in consultazione una modifica dell'ordinanza sui servizi di telecomunicazione (OST), avvalendosi di questa facoltà. Gli adeguamenti proposti riguardano la segnalazione delle interferenze, la lotta contro le manipolazioni non autorizzate di impianti di telecomunicazione nonché la sicurezza delle reti di radiocomunicazione mobile di ultima generazione (reti 5G). I Cantoni, i partiti politici rappresentati nell'Assemblea federale e le cerchie interessate sono stati invitati a esprimere la propria opinione entro il 18 marzo 2022. Sono pervenuti 46 pareri. L'elenco dei partecipanti e delle relative abbreviazioni è riportato nell'allegato. I pareri sono disponibili sul sito Internet dell'UFCOM (www.ufcom.admin.ch > L'UFCOM > Organizzazione > Basi legali > Consultazioni [2021]).

I Cantoni **BL**, **JU**, **AI**, **AR**, **LU**, **TG**, **NW**, **FR**, **BE**, **TI**, **GR**, **AG**, **OW**, **GE**, **GL** nonché **IAS**, **CCPCS**, **KAPO AI**, **GVZG**, **CDDGP** e **CSP** condividono pienamente o in parte il parere di **CG MPP** o ne chiedono alcuni adeguamenti**.**

Nell'esprimere la sua opinione, **SUISSEDIGITAL** rinvia al parere del suo membro **Sunrise UPC** in merito a misure specifiche da applicare alle reti di telecomunicazione mobile di 5ª generazione.

2 Osservazioni generali

La **COMCO** e i Cantoni **UR**, **SH**, **BS, VS** nonché **FSC** e il **PS** si sono espressi a favore del progetto di ordinanza posto in consultazione o lo sostengono senza aggiungere commenti o proposte di modifica.

In linea di massima **CG MPP**, i Cantoni **JU**, **BL**, **TG**, **AI**, **AR**, **SO**, **SG**, **LU**, **NW**, **FR**, **BE**, **TI**, **ZG**, **GR**, **OW**, **GE**, **GL**, **VD**, **NE**, nonché **Internetverband für Rettungswesen**, **CCPCS**, **KAPO AI**, **GVZG**, **Staatskanzlei ZH**, **CCDGP**, **asut**, **Sunrise UPC**, **Swisscom**, **SSR**, **digitalswitzerland**, **Salt**, **FER**, **CSP**, **economiesuisse** approvano il progetto d'ordinanza ma hanno formulato dei commenti o delle proposte di modifica.

UDC Svizzera è d'accordo nel definire requisiti minimi nell'ambito della sicurezza delle infrastrutture di telecomunicazione, ma non approva il progetto di ordinanza in questa forma.

La questione della sicurezza delle informazioni e delle infrastrutture di telecomunicazione costituisce per **SUISSEDIGITAL** un tema strategico importante. Crede che le misure proposte per la gestione delle infrastrutture e dei servizi di telecomunicazione generino inevitabilmente elevati costi di investimento e d'esercizio per i suoi membri, che alla fine si ripercuotono anche sui rispettivi clienti.

L'**FSC** sostiene che le nuove norme contribuiscano a sostenere l'evoluzione digitale, in quanto stabiliscono standard e misure di sicurezza minime vincolanti, accrescendo così la fiducia nella digitalizzazione per gli utenti e le imprese, nonché promuovendo le applicazioni correlate.

Il **Centre Patronal** accoglie favorevolmente gli adeguamenti proposti, lasciando però ai rispettivi fornitori di servizi la possibilità di esprimersi in merito alla praticabilità o all'adeguatezza degli sforzi richiesti.

asut è favorevole alla proposta di revisione dell'OST. Ritiene che abbia il potenziale per rafforzare la fiducia dell'economia e della società nella sicurezza delle reti di telecomunicazione in quanto infrastruttura critica.

In linea di massima, secondo **Sunrise UPC** un adeguamento delle basi legali non è strettamente necessario. Con i vari strumenti in uso, ritiene di assicurare già elevati standard di sicurezza e garantire l'attuazione della maggior parte delle misure proposte.

Swisscom condivide l'opinione del Consiglio federale, secondo cui si deve prestare particolare attenzione alla sicurezza delle reti e dei servizi di telecomunicazione e adottare misure adeguate. Considera essenziale prevedere scadenze sufficienti per l'attuazione.

Per la **SSR** è importante emanare il secondo pacchetto di misure volto a garantire l'approvvigionamento elettrico.

3 Commenti sulle disposizioni del progetto

Art. 96 Segnalazione di interferenze

IAS, **CCPCS**, **CDDGP**, **CSP**, **GVZG**, **CG MPP**, **AG**, **AI**, **AR**, **BE**, **BL**, **FR**, **GE**, **GL**, **LU**, **NW**, **OW**, **SO**, **TG**, **TI**, **VD**, **ZG** e **KAPO AI** suggeriscono di definire più nel dettaglio i processi di allarme e di segnalazione nonché i ruoli dei singoli attori e organi.

Capoverso 1

CG MPP, **IAS**, **CCPCS**, **CDDGP**, **CSP**, **KAPO AI**, **GVZG**, **BL**, **AI**, **AR**, **TG**, **SO**, **SG**, **LU**, **FR**, **NW**, **BE**, **TI**, **AG**, **OW**, **GL**, **GR**, **ZG** e **GE** chiedono di ridurre il valore limite e di segnalare le interferenze che coinvolgono almeno 1000 clienti per 15 minuti (o per 10 minuti secondo il Cantone **JU**).

Swisscom vorrebbe mantenere il valore attuale di 30 000 clienti coinvolti per 1 ora.

IAS, **CCPCS**, **CDDGP**, **CSP**, **UDC**, **GVZG**, **economiesuisse**, **Swisscom**, **SO**, **SG**, **BE**, **OW** e **KAPO AI** chiedono che il valore limite relativo ai clienti coinvolti continui a essere regolamentato nelle prescrizioni tecniche e amministrative (PTA) e non a livello dell'OST. Ciò consente di adeguarsi rapidamente alle nuove circostanze.

Swisscom e **Salt** accettano il CENAL come servizio di segnalazione.

IAS, **CCPCS**, **CDDGP**, **CSP**, **GVZG**, **KAPO AI**, **SO**, **SG**, **BE**, **OW** e **VD**, invece, sono contrari al fatto che i fornitori di servizi di telecomunicazione siano tenuti a informare le centrali d'emergenza cantonali competenti prima di effettuare segnalazioni al CENAL o ad altri organi.

asut, **Sunrise UPC**, **Digital Switzerland** ed **economiesuisse** sottolineano che le responsabilità dei vari servizi incaricati di notificare l'accaduto al FST vadano definite in modo chiaro e devono essere ridotte al minimo. Propongono che il NCSC ricopra il ruolo di servizio di segnalazione al posto del CENAL. È importante che la revisione della OST e l'adeguamento della legge sulla sicurezza delle informazioni (LSIn) siano coordinati.

Capoverso 2

IAS, **CCPCS**, **CDDGP**, **CSP**, **SO**, **FR**, **TI**, **OW**, **GE**, **GL** e **VD** sono infastiditi dal fatto che la OST disciplina esclusivamente le informazioni dell'UFCOM relative alle interferenze notificate attraverso il CENAL. Occorre coinvolgere ad esempio anche il National Cyber Security Center (NCSC), la Centrale d'annuncio e d'analisi per la sicurezza dell'informazione (MELANI) nonché le centrali d'emergenza cantonali della polizia, dei pompieri e dei servizi sanitari. **Swisscom** ed **economiesuisse** sostengono l'informazione di altre autorità.

Salt chiede che i dati delle segnalazioni delle interferenze non siano resi pubblici, poiché potrebbero dare un'impressione sbagliata nei media. Le interferenze segnalate dovrebbero essere pubblicate soltanto in forma aggregata.

Art. 96*a* Manipolazione non autorizzata di impianti di telecomunicazione (misure di sicurezza)

Capoverso 1

IAS, **CCPCS**, **CDDGP**, **BE**, **SG**, **OW**, **VD**, **KAPO AI**, **GVZG** e **CSP** auspicano che la disposizione non si limiti esclusivamente agli attacchi DDoS, i quali dovrebbero piuttosto essere menzionati a titolo di esempio. Viene inoltre ribadito che i dettagli di eventuali meccanismi di attacco non sono da disciplinare in modo esaustivo nell'OST, bensì nelle PTA. Ciò consente di agire in modo adeguato e di adattarsi facilmente alle nuove disposizioni da prendere in considerazione.

GE è contrario al fatto che gli operatori sono tenuti a utilizzare tutti i mezzi tecnici appropriati per configurare le proprie reti secondo le migliori pratiche di sicurezza, incluso il controllo di elementi di indirizzo falsificati.

economiesuisse sostiene che debbano essere previsti scadenze e tempi di attuazione sufficienti da definire nelle PTA.

Capoverso 2

economiesuisse, **UDC** e **Swisscom** auspicano una chiara limitazione del campo di applicazione: l'aggiornamento degli smartphone deve spettare agli utenti finali e non rientrare in questa disposizione. Secondo **SUISSEDIGITAL** è necessario precisare che la disposizione vale soltanto per gli apparecchi forniti dagli IAP in quanto tali.

economiesuisse e **Swisscom** chiedono termini di attuazione sufficienti (minimo 6 mesi).

Secondo **economiesuisse**, il CPE deve essere regolamentato con uno standard di sicurezza di base. Inoltre i requisiti della regolamentazione devono essere vincolati maggiormente alla fattibilità tecnica.

FER è dell'opinione che la resilienza digitale possa essere raggiunta soltanto attraverso una visione globale di tutte le varie sfaccettature dei rischi informatici.

Salt chiede aggiornamenti «regolari» e non «immediati».

Per la **SSR** le misure di sicurezza non sono sufficienti poiché sono concepite su misura per il CPE e vincolano soltanto l'IAP. Si dovrebbe mirare alla protezione di tutti gli apparecchi terminali esposti.

Swisscom vorrebbe che siano gli IAP a valutare la necessità di aggiornare gli impianti di telecomunicazione.

Diverse prese di posizione si esprimono già in merito alla concreta attuazione tecnica della presente disposizione. In alcuni casi fanno esplicitamente riferimento ai principi per le PTA menzionati nel rapporto esplicativo.

asut, **digitalswitzerland** e **Sunrise UPC** sono dell'avviso che occorra riformulare il principio delle PTA relativo alla *end of life* dei CPE. Questi ultimi vanno cambiati quando non possono più ricevere gli aggiornamenti di sicurezza critici. **Swisscom** desidera che non siano i fabbricanti ma piuttosto gli IAP a valutare se gli impianti debbano essere sostituiti per importanti motivi di sicurezza.

asut e **Sunrise UPC** desiderano la soppressione del principio secondo il quale i servizi non necessari vanno disattivati sul CPE. Secondo **Swisscom** al momento della consegna alcune porte del CPE devono essere aperte in modo da garantire la manutenzione remota dell'apparecchio.

SUISSEDIGITAL e **Salt** auspicano che ci si basi su norme internazionali.

Swisscom ritiene importante discutere anticipatamente con l'IAP specifiche modifiche di sicurezza agli accessi del router, limitati nel tempo e nel contenuto, nel quadro del processo di supporto e valutare alternative possibili. In generale, le PTA devono essere presentate in anticipo all'IAP interessato. Inoltre le prescrizioni non devono essere così restrittive da complicare inutilmente, o rendere addirittura impossibile, la gestione del CPE da parte del FST.

Capoverso 3

CSP, **GVZG**, **BE**, **GE**, **OW**, **SO**, **SG**, **VD**, **KAPO AI**, **CDDGP**, **CCPCS** e **IAS** chiedono che i blocchi o le limitazioni nell'utilizzo di accessi Internet o di elementi di indirizzo si basino su criteri molto selettivi. Solo in casi eccezionali devono fare in modo che tramite i collegamenti in questione non sia più possibile selezionare i numeri di emergenza.

CSP, **GVZG**, **BE**, **OW**, **SO**, **KAPO AI**, **CDDGP**, **CCPCS** e **IAS** domandano che le centrali d'emergenza cantonali interessate siano informate nel caso in cui le limitazioni abbiano un impatto su oltre 1000 clienti per più di 15 minuti.

AG, **AI**, **AR**, **BL**, **GL**, **LU**, **NW**, **TI**, **TG**, **ZG** e **CG MPP** esigono che venga introdotto l'obbligo di bloccare gli accessi a Internet o gli elementi di indirizzo che rappresentano un rischio per le infrastrutture critiche.

BL ritiene che gli IAP debbano essere obbligati a sostenere i clienti toccati da un blocco o dall'utilizzazione limitata risolvendo il problema di sicurezza alla base. In generale, gli IAP devono ripristinare gli accessi a Internet nel minor tempo possibile.

TI auspica che le analisi dei dati dell'IAP in relazione al blocco degli accessi a Internet non compromettano la protezione dei dati.

ZG vorrebbe che si valutassero disposizioni supplementari per la vendita e la fabbricazione degli impianti di telecomunicazione al fine di evitare la produzione di rifiuti elettronici.

Swisscom è dell'idea che anche i collegamenti sorvegliati ai sensi della LSCPT possano causare attività dannose. Per proteggere reti e servizi anche questi collegamenti devono poter essere bloccati dall'IAP, in particolare nel caso di grave pericolo per la sicurezza e la stabilità dei sistemi di comunicazione. Per applicare le misure di sicurezza sia su rete fissa che mobile vanno previsti termini di attuazione adeguati e vanno coinvolti gli IAP. Per quanto riguarda l'accesso mobile a Internet devono ancora essere create le possibilità tecniche per il blocco. In questo contesto i sistemi operativi e i fabbricanti di terminali mobili rivestono un ruolo decisivo.

Art. 96*b* Manipolazione non autorizzata di impianti di telecomunicazione (servizio di segnalazione)

AG, **AI**, **AR**, **BE**, **BL**, **FR**, **GE**, **GL**, **LU**, **NW**, **OW**, **SO**, **TG**, **TI**, **VD**, **ZH**, **CSP**, **GVZG**, **IAS**, **KAPO AI**, **CDDGP**, **CCPCS**, **CG MPP** e **SKS** chiedono che i ruoli di tutti i servizi attivi nell'intero processo di segnalazione e allarme all'interno del ciberspazio figurino in modo dettagliato nel rapporto esplicativo. **SUISSEDIGITAL**, **asut** e **Sunrise UPC** auspicano che gli sforzi siano coordinati e armonizzati con altri progetti legislativi in seno all'Amministrazione per quanto riguarda la sicurezza.

Economiesuisse critica l'obbligo di gestire un servizio di segnalazione, in particolare perché impone prescrizioni organizzative concrete invece di limitarsi ai principi operativi. Secondo **Salt** i singoli fornitori di accessi a Internet devono occuparsi di organizzare il servizio di segnalazione. In vista della collaborazione tra UFCOM e NCSC, **Swisscom** sostiene che tale servizio di segnalazione debba essere unito a quello previsto nel quadro della revisione della LSI per le infrastrutture critiche.

ZH considera auspicabile definire con più precisione il termine per l'adozione di misure protettive più idonee.

Art. 96*c* Manipolazione non autorizzata di impianti di telecomunicazione (esecuzione)

Salt si chiede a cosa faccia riferimento questa disposizione d'esecuzione. **Swisscom** vorrebbe che si consultasse il rispettivo FST se nelle PTA fosse necessario definire requisiti supplementari.

Art. 96*d* Sicurezza delle reti e dei servizi esercitati dai concessionari di radiocomunicazione mobile (applicazione)

Per **ZG** sarebbe opportuno valutare la necessità di applicare le misure a tutti i servizi di radiocomunicazione mobile e non soltanto a quelli di quinta generazione.

ZH considera inappropriato limitare il campo di applicazione degli articoli 96*e*-96*g* ai servizi di radiocomunicazione mobile di quinta generazione. Visto che nei prossimi anni oltre al 5G resteranno attivi i servizi di radiocomunicazione mobile di terza e di quarta generazione nonché gli hotspot WiFi degli operatori di radiocomunicazione mobile, le disposizioni andrebbero formulate in modo neutrale dal punto di vista tecnico.

GE crede che questo articolo andrebbe applicato a tutti i servizi di radiocomunicazione mobile attuali e futuri.

Anche **Salt** sostanzialmente si domanda perché l'articolo non disciplini le reti mobili di tutte le generazioni.

Swisscom, invece, ritiene la limitazione al 5G proporzionata e adeguata.

Per **FER** occorre tener presente che il 5G è solo un vettore di diffusione che renderebbe possibile un aumento del furto di dati e delle estorsioni soltanto se gli apparecchi collegati sono guasti, mal configurati o se gli eventuali problemi di sicurezza o i rispettivi sistemi di sicurezza non sono pronti ad affrontare il rischio già noto. Ciò ne rende difficile la gestione e forza il legislatore a indicare i metodi di comunicazione, il tipo di crittografia, la protezione adeguata e il livello di sicurezza auspicato. Si tratta di un ampio processo che supera chiaramente i limiti federali, quelli dei fornitori di accessi e di altri intermediari della comunicazione. Il dibattito si concentra sui fornitori di apparecchi connessi e sui relativi obblighi, coinvolgendo senza dubbio organi di livello superiore, come l'IETF e i suoi Best Current Practice, gli accordi dell'Organizzazione mondiale del commercio e dell'ENISA.

Art. 96*e* Sicurezza delle reti e dei servizi esercitati dai concessionari di radiocomunicazione mobile (gestione della sicurezza)

Capoverso 1

Sunrise e **Swisscom** hanno già implementato un sistema di gestione della sicurezza. Secondo **Sunrise** la sicurezza deve essere e restare il compito di ciascun attore.

Salt non è in grado di valutare la portata di un simile SGSI. Tuttavia dispone già di un sistema di gestione dei rischi che costituisce un elemento del sistema di gestione.

asut e **Salt** sono dell'idea che una certificazione prescritta comporterebbe grandi sforzi e costi troppo elevati per i piccoli fornitori (unici o ricorrenti). Una disposizione concreta significherebbe una grave ingerenza nella libertà economica. Pertanto è necessario lasciare agli operatori la facoltà di attuare la gestione della sicurezza e rinunciare alla definizione di standard concreti nell'ordinanza e nelle PTA. L'UFCOM dovrebbe intervenire in caso di problemi e valutare la situazione sulla base dell'articolo 96*g*.

Capoverso 3

Secondo **FER** e il Cantone **VS** è necessario implementare un SGSI basato sulle norme ISO. **economiesuisse** è dell'avviso che il sistema di gestione richiesto vada accettato sulla base degli standard e delle certificazioni esistenti. A questo proposito il mercato ha già creato sufficienti basi per cui una regolamentazione specifica per la Svizzera non è efficace.

Per lo sviluppo di un sistema di gestione della sicurezza, **Swisscom**, **Sunrise** e **FER** fanno riferimento alla norma ISO/IEC 27001. **Swisscom**, **Salt**, il Cantone **VS** e **FER** sostengono il sistema di gestione della continuità e la gestione di incidenti di sicurezza.

Sunrise gestisce un Business Continuity Management System secondo la norma ISO/IEC 22301. Per realizzare un sistema di gestione della continuità, **Swisscom** e **Sunrise** menzionano tale norma come riferimento.

Art. 96*f* Sicurezza delle reti e dei servizi esercitati dai concessionari di radiocomunicazione mobile (esercizio degli impianti di telecomunicazione critici)

Capoverso 1

asut approva il progetto. Sostanzialmente si basa sulle misure che si applicano anche in altri Paesi (in particolare dell'UE) nonché su norme e iniziative in materia di sicurezza riconosciute a livello internazionale (ad es. ENISA, NESAS, GSMA knowledge base, SCAS, 3GGP, ISO). Per poter continuare a rinunciare a una soluzione straordinaria su scala nazionale, le misure potrebbero essere applicate in modo più efficiente e gli standard di sicurezza adeguati in funzione dei progressi tecnologici. Su questi standard si sono basate anche le aziende tecnologiche attive a livello internazionale nonché sempre più i clienti commerciali svizzeri (ad es. settore finanziario). Questi standard porterebbero a un incremento della sicurezza a livello intersettoriale e dimostrerebbero che il mercato e la concorrenza farebbero crescere il livello di sicurezza.

Swisscom comunica di aver già messo in atto le misure di sicurezza pertinenti stabilite a livello internazionale.

Salt è favorevole alla certificazione proposta basata su norme di sicurezza riconosciute. S'intende evitare la creazione di norme specifiche per la Svizzera. L'Ufficio federale per l'approvvigionamento economico del Paese (UFAE) considera le reti di radiocomunicazione mobile della Svizzera sistematicamente rilevanti e come un'infrastruttura critica. Sul piano della sicurezza gli impianti di telecomunicazione sono pertanto ritenuti critici. Per Salt non è quindi chiaro cosa l'UFCOM debba esattamente definire a questo proposito.

Capoverso 2

L'obbligo di ubicazione proposto dei centri operativi di rete e di sicurezza (in Svizzera, nello SEE o nel Regno Unito) è accolto favorevolmente da **IAS**, **CCPCS**, **CDDGP**, **SG**, **KAPO AI**, **GVZG**, **BE**, **OW**, **GE**, **GL**, **FKS**, **SO**, **VD**, **VS**, **ZH** e **Swisscom**. **Salt** vorrebbe estenderlo agli Stati con una protezione dei dati adeguata conformemente all'elenco dell'IFPDT. **IAS**, **CCPCS**, **CDDGP**, **SG**, **KAPO AI**, **GVZG**, **BE**, **OW**, **GE**, **GL**, **FKS**, **SO** e **VD** propongono anche di prescrivere una sede aziendale o una filiale in Svizzera.

Art. 96*g* Sicurezza delle reti e dei servizi esercitati dai concessionari di radiocomunicazione mobile (prescrizioni applicabili e vigilanza)

Capoverso 1

L'**UDC** parte dal presupposto che la realizzazione delle PTA secondarie da parte dell'UFCOM avvenga in stretta collaborazione con il settore.

Secondo **asut** vanno evitate delle norme specifiche per la Svizzera poiché rallenterebbero il progresso tecnologico e la capacità d'innovazione. Ciò vale anche per le PTA.

Sunrise UPC e **digitalswitzerland** ritengono opportuno che il progetto si basi sostanzialmente su misure dell'UE e su norme di sicurezza riconosciute a livello internazionale e che non preveda nessuna soluzione speciale nazionale. **Sunrise UPC** è dell'idea che questo approccio debba essere mantenuto anche per le PTA.

SUISSEDIGITAL sostiene che l'implementazione e l'attuazione di misure di sicurezza si debbano basare sull'esperienza dei fornitori dei servizi di telecomunicazione tenendo conto delle loro attività.

Dal punto di vista di **Swisscom**, gli operatori di radiocomunicazione mobile applicano già le norme di sicurezza stabilite. A causa del rischio che manchi un'armonizzazione internazionale vanno evitate prescrizioni specifiche per la Svizzera. Per le PTA future è necessario cooperare a stretto contatto con i fornitori interessati per definire altri aspetti relativi all'applicazione e all'attuazione.

Salt chiede di stralciare questo capoverso, poiché a seconda delle norme e delle certificazioni scelte, in particolare per i piccoli fornitori, potrebbero insorgere un onere maggiore e (dei) costi elevati.

Capoverso 2

L'**UDC**, **Swisscom** ed **economiesuisse** propongono di riformulare questo capoverso in modo che l'UFCOM possa richiedere una verifica adeguata in caso di «sospetto fondato», e quindi di sospetto qualificato e non solo in caso di un semplice momento di sospetto (cfr. ad es. art. 9 cpv. 1 LRD, art. 5 ODiT ecc.).

Salt è dell'avviso che la portata di un'eventuale analisi debba essere limitata agli impianti di telecomunicazione per cui si sospetta una violazione del diritto.

4 Altre osservazioni e proposte

In relazione al pericolo di attacchi informatici alle infrastrutture critiche, **CG MPP**, **BL**, **IAS**, **CCPCS**, **CDDGP**, **AR**, **TG**, **SG**, **KAPO AI**, **LU**, **NW**, **FR**, **GVZG**, **BE**, **TI**, **ZG**, **OW**, **FKS** e **SO** propongono di menzionare nell'OST anche i compiti dell'esercito.

IAS, **CCPCS**, **CDDGP**, **SG**, **KAPO AI**, **GVZG**, **BE**, **OW**, **GE**, **GL**, **FKS**, **SO** e **VD** sostengono che con la presente revisione d'ordinanza debba essere migliorato anche il disciplinamento in materia di chiamate d'emergenza (banca dati delle chiamate d'emergenza, LIS-Proxy, istradamento dinamico). Secondo **FR** è auspicabile che il Consiglio federale presenti una strategia globale sulla cibersicurezza. Inoltre la revisione proposta deve essere regolarmente sottoposta a revisione e se necessario completata con norme statali più severe.

Allegato: elenco dei partecipanti alla consultazione e abbreviazioni

Cantoni

AG	Cantone di Argovia
AI	Cantone di Appenzello Interno
AR	Cantone di Appenzello Esterno
BE	Cantone di Berna
BL	Cantone di Basilea Campagna
BS	Cantone di Basilea Città
FR	Cantone di Friburgo
GE	Cantone di Ginevra
GL	Cantone di Glarona
GR	Cantone dei Grigioni
JU	Cantone del Giura
LU	Cantone di Lucerna
NE	Cantone di Neuchâtel
NW	Cantone di Nidvaldo
OW	Cantone di Obvaldo
SG	Cantone di San Gallo
SH	Cantone di Sciaffusa
SO	Cantone di Soletta
TG	Cantone di Turgovia
TI	Cantone Ticino
UR	Canton di Uri
VD	Cantone di Vaud
VS	Cantone del Vallese
ZG	Cantone di Zugo
ZH	Cantone di Zurigo

Partiti politici rappresentati nell'Assemblea federale

SPS / PSS / PSS	Sozialdemokratische Partei der Schweiz / Parti socialiste suisse / Partito socialista svizzero
SVP / UDC / UDC	Schweizerische Volkspartei / Union Démocratique du Centre / Unione democratica di centro

Associazioni mantello

USC	Unione svizzera dei contadini
economiesuisse	

Altri partecipanti

asut	Schweizerischer Verband der Telekommunikation / Association Suisse des télécommunications / Associazione svizzera delle telecomunicazioni
Centre Patronal	
digitalswitzerland	
FER	Fédération des entreprises romandes Genève

FKS / CSP	Feuerwehr Koordination Schweiz / Coordination suisse des sapeurs-pompiers / Coordinazione Svizzera dei Pompieri
GVZG	Gebäudeversicherung ZUG-
IVR / IAS	Internetverband für Rettungswesen / Interassociazione di salvataggio
KAPO AI	Polizia cantonale Appenzello Interno
KKJPD / CCDJP / CDDGP	Konferenz der Kantonalen Justiz- und Polizeidirektorinnen und -direktoren / Conférence des directrices et directeurs / Conferenza delle direttrici e dei direttori dei dipartimenti cantonali di giustizia e polizia
KKPKS / CCPCS / CCPCS	Konferenz der kantonalen Polizeikommandanten der Schweiz / Conférence des commandants des polices cantonales de Suisse / Conferenza dei comandanti delle polizie cantonali della Svizzera
RK MZF / CG-MPS / CG MPP	Regierungskonferenz Militär, Zivilschutz und Feuerwehr / Conférence gouvernementale des affaires militaires, de la protection civile et des sapeurs-pompiers / Conferenza governativa per gli affari militari, la protezione civile e i pompieri
Salt Mobile SA	
SRG / SSR	Schweizerische Radio- und Fernsehgesellschaft / Société suisse de radiodiffusion et télévision / Società svizzera di radiotelevisione
SUISSEDIGITAL	Verband für Kommunikationsnetze / Association des réseaux de communication / Associazione degli operatori via cavo svizzeri
Sunrise	Sunrise UPC GmbH
Swisscom	Swisscom (Svizzera) SA
WEKO / COMCO / COMCO	Wettbewerbskommission / Commission de la concurrence / Commissione della concorrenza