Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

Berna, 16 novembre 2022

Modifica dell'ordinanza sui servizi di telecomunicazione (OST)

Sicurezza delle informazioni, delle infrastrutture e dei servizi di telecomunicazione

Rapporto esplicativo

Rapporto esplicativo

1 Contesto

La modifica dell'articolo 48*a* della legge sulle telecomunicazioni (LTC; RS 784.10) è entrata in vigore il 1° gennaio 2021 (RU 2020 pag. 6159). Conferisce al Consiglio federale ampie competenze nel campo della sicurezza delle informazioni, delle infrastrutture e dei servizi di telecomunicazione. Finora, in base al vigente articolo 48*a* LTC (RU 2007 pag. 921) il Consiglio federale ha disciplinato soltanto la segnalazione delle interferenze nell'esercizio della rete (cfr. art. 96 cpv. 1 dell'ordinanza del 9 marzo 2007 sui servizi di telecomunicazione [OST; RS 784.101.1]). Il presente progetto di modifica dell'OST intende completare questa disposizione con una prima serie di misure volte a precisare la regolamentazione relativa alla segnalazione delle interferenze, a combattere la manipolazione non autorizzata degli impianti di telecomunicazione commessa con trasmissione mediante telecomunicazione e a garantire un elevato livello di sicurezza nell'esercizio delle reti mobili di ultima generazione (reti 5G). In una seconda fase, seguirà un altro pacchetto di misure, il cui impatto deve ancora essere analizzato, sarà diretto in particolare a garantire l'approvvigionamento di energia elettrica alle reti radiomobili.

1.1 Necessità di agire e obiettivi

1.1.1 Sicurezza delle reti mobili a partire dalla quinta generazione

Problematica

Secondo l'Ufficio federale di statistica (UST), in Svizzera l'utilizzo di Internet su reti mobili, misurato in base al numero complessivo di utenti di Internet, è passato dal 43 per cento nel 2010 al 91 per cento nel 2019[1]. Allo stesso tempo, le reti mobili sono sempre più orientate verso la tecnologia 5G. Stando alla società di consulenza Gartner, nel 2020 il 21,3 per cento dei fondi mondiali investiti nelle infrastrutture di comunicazione mobile affluiva già nella tecnologia 5G[2]. Ericsson prevede che entro il 2026 la metà di tutto il traffico mobile si svolgerà tramite 5G[3]. Nell'UE, si aspira a una completa copertura 5G in tutte le aree popolate entro il 2030[4]. Questa tecnologia aprirà la strada ad applicazioni potenzialmente nuove o migliori in ambiti sensibili come la salute e l'energia[5] e giocherà un ruolo centrale nell'Internet delle cose[6]. Inoltre, le reti radiomobili fanno parte dell'infrastruttura critica delle telecomunicazioni, da cui dipendono altri sottosettori critici[7]. Di conseguenza, garantire reti sicure per la quinta generazione di telefoni cellulari e per quelle successive è di fondamentale importanza.

Con la crescente diffusione di questa tecnologia, le questioni relative alla sicurezza hanno acquisito importanza anche nelle discussioni di politica estera. Il Dipartimento di Stato americano considera infatti centrale garantire la sicurezza delle reti 5G[8]. Nell'UE, è stata effettuata nel 2019 un'analisi dei rischi ai quali potrebbe essere esposta la tecnologia 5G, che a sua volta si basa sulle analisi dei rischi dei Paesi membri9. Ne emerge che la disponibilità, la riservatezza e/o l'integrità dei dati trasmessi via 5G può essere compromessa da vari attori (tra cui singoli hacker, organizzazioni criminali, organizzazioni statali o parastatali). Le funzioni nella rete centrale e la gestione delle funzioni di rete virtualizzate sono particolarmente importanti per garantire la sicurezza. La 5G si trova al centro dell'attenzione poiché, rispetto alle reti di generazione precedente è

1 Ufficio federale di statistica (2020): *Mobile Internetnutzung (disponibile sono in tedesco e francese);* https://www.bfs.admin.ch/bfs/de/home/statistiken/kultur-medien-informationsgesellschaft-sport/informationsgesellschaft/gesamtindikatoren/haushalte-bevoelkerung/mobile-internetnutzung.html
2 Gartner (2020): *Gartner Says Worldwide 5G Network Infrastructure Spending to Almost Double in 2020;* https://www.gartner.com/en/newsroom/press-releases/gartner-says-worldwide-5g-network-infrastructure-spending-to-almost-double-in-2020
3 Ericsson (2020): *More than 1 billion people will have access to 5G coverage by the end of 2020;* https://www.ericsson.com/en/press-releases/2020/11/more-than-1-billion-people-will-have-access-to-5g-coverage-by-the-end-of-2020
4 Commissione europea (2021): *5G*; https://digital-strategy.ec.europa.eu/en/policies/5g
5 BAKOM (2020): *Mobile Kommunikation: Auf dem Weg zu 5G* von https://www.bakom.admin.ch/bakom/de/home/telekommunikation/technologie/5g.html
6 Commissione europea (2021): *5G*; https://digital-strategy.ec.europa.eu/en/policies/5g
7 UFCOM (2020): *Comunicazione mobile: evoluzione verso il 5G;* https://www.bakom.admin.ch/bakom/it/pagina-iniziale/telecomunicazione/tecnologia/comunicazione-mobile-evoluzione-verso-il-5G.html
8 US State Department (2021): *Department Press Briefing;* https://www.state.gov/briefings/department-press-briefing-february-22-2021/
9 NIS Cooperation Group (2019): *EU coordinated risk assessment of the cybersecurity of 5G networks;* https://digital-strategy.ec.europa.eu/en/news/eu-wide-coordinated-risk-assessment-5g-networks-security

la tecnologia più importante per il futuro. In termini di rischio, sono considerate rilevanti soprattutto le situazioni in cui le misure di sicurezza sono insufficienti o i dispositivi degli utenti finali non sono sicuri, o in cui i fornitori sono messi sotto pressione da autori di attacchi informatici.
Anche se gli scenari di rischio hanno probabilità di accadimento relativamente basse, è lecito attendersi impatti significativi qualora si verifichino, non da ultimo a causa della crescente importanza della 5G nelle comunicazioni mobili. Inoltre, gli scenari di rischio descritti nell'analisi dei rischi di cui sopra non sono affatto specifici a un Paese e sono quindi ipotizzabili per la Svizzera. Tuttavia, in Svizzera è diverso in quanto l'attuale base legale permette per ora solo un intervento limitato dello Stato; a breve termine sono attuabili soprattutto misure tecniche. Va però considerato anche che i concessionari di radiocomunicazione mobile hanno un certo interesse personale nella sicurezza delle loro reti. Un sondaggio[10] condotto dall'UFCOM presso i tre concessionari svizzeri mostra l'impegno profuso da questi ultimi per rendere più sicure le reti 5G.

Obiettivo
In Svizzera si mira a raggiungere un livello minimo generale di sicurezza della rete 5G e delle tecnologie future, basato in particolare su standard internazionali.

1.1.2 Manipolazioni non autorizzate degli impianti di telecomunicazione

Problematica
Gli attacchi informatici portano a elevati danni economici. Anche se le stime divergono molto, vi è un consenso generale sul fatto che l'entità dei danni abbia da tempo raggiunto l'ordine dei miliardi. Nel 2018, per esempio, l'Associazione svizzera d'Assicurazioni (ASA) ha stimato le perdite annuali a 9,5 miliardi di franchi[11]. È probabile che la cifra sia aumentata ulteriormente da allora. Vittime dei danni non sono solo le grandi aziende o i singoli settori, ma potenzialmente tutte le aziende[12] e i privati. In un sondaggio rappresentativo presso i direttori delle PMI, ad esempio, si è scoperto che una su tre delle circa 38 000 PMI che sono già state vittime di un grave attacco informatico ha subito danni finanziari[13]. Tuttavia, gli attacchi informatici non solo hanno un alto impatto economico, ma mettono anche in pericolo la sicurezza del Paese, in quanto possono portare a guasti o al funzionamento difettoso delle infrastrutture critiche. Vi è quindi un interesse in materia di sicurezza e di politica economica nell'attuazione di misure contro gli attacchi informatici.
I fornitori di accesso a Internet (*Internet Access Provider* IAP) giocano un ruolo centrale nella prevenzione degli attacchi informatici. Permettono ai propri clienti di comunicare via Internet e spesso forniscono loro anche l'attrezzatura necessaria. Questa posizione consente agli IAP di prendere misure preventive o reattive che hanno un impatto diretto e sono di grande importanza per la sicurezza informatica della Svizzera. Senza una stretta cooperazione con gli IAP, non sarà possibile ridurre significativamente il numero di attacchi informatici.
Poiché la minaccia degli attacchi informatici ha continuato ad aumentare negli ultimi anni, si teme che questa tendenza proseguirà[14]: l'adozione di misure di protezione diventa tanto più urgente. Lo Stato ha il dovere di promuovere tali misure. Sostiene quindi l'economia mettendo a disposizione punti di contatto e centri di competenza e potenziando il perseguimento penale. Crea inoltre condizioni quadro che consentano un'adeguata sicurezza informatica, queste devono essere ben coordinate tra loro. La definizione di obblighi per gli IAP è uno strumento molto importante in tale contesto. Non ha senso introdurre severe misure di protezione contro gli attacchi informatici in molti settori dell'economia se allo stesso tempo non vengono definite direttive concrete che chiariscono il ruolo degli IAP in questi sforzi di protezione.
Queste considerazioni hanno fatto sì che nel corso della revisione della LTC l'articolo 48*a* è stato modificato in modo tale che i fornitori sono ora tenuti a lottare contro gli attacchi informatici e a tal fine sono autorizzati a «deviare o a impedire le comunicazioni e a dissimulare informazioni». Tuttavia, la LTC non specifica le misure che i fornitori sono obbligati a prendere per proteggersi dagli attacchi informatici. Le attuali misure

10 UFCOM (2021): *Sondaggio sul toolbox 5G (risposte confidenziali).*
11 Associazione svizzera d'assicurazioni (2018): *documento sui rischi informatici* https://www.svv.ch/sites/default/files/2018-04/Grundlagenpapier%20CyberRisiken_DE.pdf
12 Secondo l'Ufficio federale di statistica (2021): *IKT Infrastruktur in den Unternehmen;* https://www.bfs.admin.ch/bfs/de/home/statistiken/kultur-medien-informationsgesellschaft-sport/informationsgesellschaft/gesamtindikatoren/unternehmen/ikt-infrastruktur.assetdetail.17784535.html il 100% delle imprese svizzere dispongono di un accesso a Internet.
13 Gfs-zürich (2020): *Digitalisierung und Cyber-Sicherheit in kleinen Unternehmen;* https://kmu-transformation.ch/wp/wp-content/uploads/2020/12/Schlussbericht_Studienergebnisse_Digitalisierung_Transformation_Homeoffice_Cybersicherheit_KMU_2020_12.pdf
14 Cfr. analisi delle tendenze effettuata dal World Economic Forum (WEF) in collaborazione con l'università di Oxford (2020): *Cybersecurity, emerging technology and systemic risk;* http://www3.weforum.org/docs/WEF_Future_Series_Cybersecurity_emerging_technology_and_systemic_risk_2020.pdf

dell'ordinanza sui servizi di telecomunicazione sono state elaborate sotto la direzione dell'UFCOM in collaborazione con il Centro nazionale per la cibersicurezza (NCSC).

Obiettivo
La presente proposta di regolamentazione riguarda principalmente l'attuazione degli interventi statali già decisi con la revisione parziale della LTC. Le misure servono ad attuare la LTC con l'obiettivo di stabilire regole uniformi e chiare per i vari IAP svizzeri che dovrebbero poi contribuire ad aumentare il livello generale di protezione nel settore della sicurezza informatica.

1.2 Alternative esaminate e soluzione scelta

1.2.1 Segnalazione di interferenze

I fornitori di servizi di telecomunicazione (FST) sono tenuti a segnalare senza indugio alla Centrale nazionale d'allarme le interferenze nell'esercizio dei loro impianti di telecomunicazione che possono toccare almeno 10 000 clienti e a pubblicare le informazioni in merito su un sito Internet liberamente accessibile. L'obbligo di segnalare le interferenze sarà ora eseguito congiuntamente dall'UFCOM e dalla Centrale nazionale d'allarme (CENAL). Le sinergie possono essere sfruttate coinvolgendo la CENAL, specializzata in eventi straordinari[15]. Inoltre, all'articolo 96 OST esisteva già una regolamentazione comparabile in materia di segnalazioni di interferenze e nelle prescrizioni tecniche e amministrative dell'UFCOM (RS 784.101.113/1.8) per quanto riguarda la soglia di segnalazione di 30 000 clienti. Pertanto, a livello di ordinanza, ai FST non incombono costi aggiuntivi rilevanti rispetto allo status quo. Di seguito gli effetti di questa misura non verranno quindi discussi in modo più approfondito. È stato rifiutato il mantenimento dello status quo con 30 000 clienti potenzialmente toccati. Nella consultazione pubblica, la maggioranza ha chiesto una soglia di segnalazione più bassa.

1.2.2 Sicurezza delle reti mobili a partire dalla quinta generazione

Di seguito sono riportati i punti chiave delle misure contenute nel progetto di legge in materia di sicurezza delle reti mobili:

- I concessionari di radiocomunicazione mobile sono tenuti ad esercitare un sistema di gestione della sicurezza delle informazioni (SGSI) in conformità con gli standard riconosciuti. Il sistema copre anche i piani di resilienza e di continuità e disciplina la gestione degli incidenti di sicurezza.
- I concessionari di radiocomunicazione mobile sono tenuti a impiegare solo impianti rilevanti per la sicurezza conformi alle norme di sicurezza riconosciute. La certificazione non è obbligatoria. I FST devono però assumersi la responsabilità di garantire che gli impianti siano conformi alle norme di sicurezza riconosciute.
- I concessionari di radiocomunicazione mobile sono obbligati ad esercitare i loro centri operativi di rete (Network Operations Centres) e i centri operativi di sicurezza (Security Operations Centres) esclusivamente in Stati la cui legislazione assicura una protezione adeguata dei dati.
- Se l'UFCOM sospetta una violazione della legge ed occorre un supporto esterno, può obbligare i concessionari di radiocomunicazione mobile a sottoporsi a proprie spese a un audit o a far testare gli impianti in questione da un organismo specializzato.

A causa della maggiore importanza dei servizi radiomobili e della rapida espansione della tecnologia 5G[16] si è evitato di continuare con lo status quo al fine di stabilire un certo livello minimo di sicurezza della rete (in) generale e vincolante per la Svizzera.
Nel presente caso non sono state considerate le misure previste dal *toolbox 5G* dell'UE: *Cybersecurity of 5G networks – EU Toolbox of risk mitigating measures*[17] per un'ampia riduzione del rischio nella catena di approvvigionamento delle aziende di radiocomunicazione mobile (ad es. esclusione dei fornitori ad alto rischio

[15] cfr. CENAL [2021]: la CENAL; https://www.naz.ch/naz/index
[16] Dati sull'avanzamento della tecnica 5G sono disponibili alle pagine web: http://map.funksender.admin.ch/ e https://map.geo.admin.ch/?topic=nga.
[17] NIS Cooperation Group (2020): *Cybersecurity of 5G networks EU Toolbox of risk mitigating measures;* https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures

o requisiti per la diversificazione dei fornitori), parte delle cosiddette misure strategiche, in quanto la legge sulle telecomunicazioni non fornisce la base giuridica necessaria.
In parte, le misure del *toolbox 5G* dell'UE si fondano anche su basi giuridiche inesistenti in Svizzera e non specifiche alle telecomunicazioni. Un esempio è il meccanismo di screening degli investimenti diretti esteri (IDE), entrato pienamente in vigore nell'UE nel 2020.[18]
Misure per una migliore protezione delle reti radiomobili[19] contro le interruzioni di corrente in situazioni speciali o straordinarie, e misure neutre dal punto di vista tecnologico, tese ad aumentare la sicurezza della rete anche al di fuori della tecnologia 5G e di quelle successive, sono attualmente oggetto di un esame approfondito e potrebbero essere integrate in una futura proposta.

1.2.3 Manipolazioni non autorizzate degli impianti di telecomunicazione

Quando si esaminano opzioni alternative occorre tenere presente che il margine d'azione è determinato dai parametri della revisione parziale della LTC. Nel messaggio sulla revisione parziale della LTC del 6 settembre 2017[20], il Consiglio federale ha già definito questo margine. Ha chiarito che l'obbligo di lottare contro qualsiasi manipolazione non autorizzata degli impianti di telecomunicazione commessa con trasmissione mediante telecomunicazione, consiste ad esempio nella prevenzione della diffusione di malware nel blocco degli attacchi alla disponibilità dei servizi web (attacchi DdoS) e non agli interventi fisici o «backdoor» nell'hardware e software.
La proposta di modifica dell'OST è quindi in linea con l'intento del messaggio. Le misure e le ragioni per cui dovrebbero essere introdotte sono presentate nei capitoli seguenti.

1.2.3.1 Misura 1: Diritto di bloccare o limitare l'accesso a Internet o elementi di indirizzo che rappresentano un rischio per gli impianti di telecomunicazione, e obbligo di informare il cliente

L'articolo 48*a* della LTC dà ai provider il diritto di bloccare le connessioni Internet o di limitarne l'uso se ciò è necessario per proteggere gli impianti. Tale diritto si applica solo finché il pericolo persiste. In questi casi, l'ordinanza obbliga i fornitori a informare i loro clienti in merito al blocco. Questo obbligo serve a garantire la trasparenza nei confronti degli utenti e crea comprensione per le necessarie misure di sicurezza.

1.2.3.2 Misura 2: Obbligo dei fornitori di filtrare i pacchetti IP il cui indirizzo IP sorgente è falsificato (*spoofing*)

I pacchetti IP inviati con indirizzi IP sorgente falsificati sono i fattori centrali degli attacchi alla disponibilità dei servizi web (attacchi DdoS). Questi attacchi sono ancora molto frequenti e generano grandi danni. Gli specialisti della sicurezza di NetScout hanno identificato più di 10 milioni di attacchi DdoS a livello globale per l'anno 2020[21]. Stimare i costi di tali attacchi è molto difficile, poiché dipendono fortemente dall'importanza dei relativi servizi web per le attività commerciali di un'azienda. Tuttavia, è chiaro che gli attacchi alla disponibilità possono avere un impatto finanziario significativo sulle vittime. Se colpiscono la disponibilità delle infrastrutture critiche, le potenziali conseguenze vanno ben oltre il possibile danno finanziario. Si pensi ad esempio, agli ospedali o alle aziende di approvvigionamento energetico: se la loro disponibilità è compromessa da attacchi informatici, non si possono escludere minacce alla vita e all'incolumità fisica.

18 EU (2019): *Screening of foreign direct investment;* http://trade.ec.europa.eu/doclib/press/index.cfm?id=2006
19 Consiglio federale (2020): *Reti mobili: migliore protezione contro i blackout;* https://www.admin.ch/gov/it/pagina-iniziale/documentazione/comunicati-stampa.msg-id-81445.html
20 Consiglio federale (2017): *Messaggio concernente la revisione della legge sulle telecomunicazioni;* https://www.fedlex.admin.ch/eli/fga/2017/1933/it
21 Netscout (2021): *Crossing the 10 Million Mark: DDoS Attacks in 2020*; https://www.netscout.com/blog/asert/crossing-10-million-mark-ddos-attacks-2020

Le possibilità tecniche di filtrare gli indirizzi IP sorgente falsificati, le quali rendono gli attacchi DdoS molto più difficili[22], sono note da anni ma non vengono applicate in modo abbastanza sistematico[23]. Questo può essere dovuto alla mancanza di incentivi economici[24]. I fornitori sostengono dei costi quando installano il filtraggio, ma l'effetto protettivo non può essere internalizzato (poiché gli attacchi DdoS sono generalmente più difficili da realizzare)[25]. Ci troviamo quindi di fronte a un classico problema legato all'utilizzo di «risorse comuni, anche se questo è mitigato dal fatto che i costi di implementazione dei filtri tendono a diminuire[26]. L'introduzione di un obbligo generale di filtraggio può ridurre il problema poiché tutti i fornitori devono contribuire a rendere più difficili gli attacchi DdoS.

1.2.3.3 Misura 3: Obbligo dei fornitori di configurare in modo sicuro i dispositivi terminali messi a disposizione dei clienti

A causa della loro ampia diffusione, i dispositivi terminali forniti dai provider ai loro clienti giocano un ruolo importante nella sicurezza informatica. Se molti di questi presentano vulnerabilità, ciò consente agli aggressori di accedere a migliaia di dispositivi e sfruttarne la potenza di calcolo, ad esempio per commettere attacchi DdoS[27]. Un classico esempio di questo problema sono i router che vengono forniti con una password standard. Una configurazione sicura dei dispositivi terminali diventa ancora più importante con la rapida diffusione degli apparecchi legati all'Internet delle cose[28]. Se i dispositivi terminali non sono configurati in modo sicuro, offrono agli aggressori un obiettivo molto facile da manipolare su vasta scala. Occorre un obbligo legale per i fornitori di configurarli in modo sicuro, poiché anche in questo caso i costi generati dalla mancanza di sicurezza non si ripercuotono su chi distribuisce i dispositivi non sicuri, bensì sulla collettività[29].
I fornitori aspirano ad avere i costi più bassi possibili all'acquisto e alla consegna dei dispositivi ma le norme di sicurezza possono aumentare i prezzi. Affinché i fornitori attenti alla sicurezza non siano penalizzati dal mercato, occorrono requisiti minimi per tutti i fornitori. Una regolamentazione è anche in linea con l'intenzione espressa dal Consiglio federale nel suo rapporto in risposta al Postulato 17.4295 Glättli, di sostenere standard di sicurezza per i dispositivi connessi a Internet, che costituiscono una delle maggiori minacce per la cyber-sicurezza.[30]

1.2.3.4 Misura 4: Obbligo dei fornitori di gestire un centro specializzato per la segnalazione delle manipolazioni e avviare misure difensive

La sicurezza informatica può essere migliorata solo se le autorità nazionali e internazionali, gli organismi specializzati e i fornitori di connessioni Internet cooperano attivamente. Considerato il gran numero di attori nazionali e internazionali, è importante che i punti di contatto possano essere gestiti in modo standardizzato. Per questo motivo, i provider dovrebbero essere obbligati ad istituire un servizio di segnalazione *abuse desk* e a depositare un contatto presso il *Regional Internet Registry* (RIR)[31] responsabile. Spetta ai fornitori scegliere se gestire loro stessi questo centro di segnalazione o se delegare il compito a terzi.
Poiché una connessione manipolata mette in pericolo la sicurezza di molti altri abbonati, è particolarmente importante reagire rapidamente. Gli IAP devono quindi avviare le dovute misure entro un periodo di tempo ragionevole. Il pericolo non potrà sempre essere sventato entro questo termine ma occorre garantire l'avvio di un intervento.

22 Lone et al. (2020): *SAVing the Internet: Explaining the Adoption of Source Address Validation by Internet Service Providers;* https://weis2020.econinfosec.org/wp-content/uploads/sites/8/2020/06/weis20-final31.pdf
23 Luckie et al. (2019): *Network hygiene, incentives, and regulation: Deployment of source address validation in the internet*; https://researchcommons.waikato.ac.nz/handle/10289/13176
24 Bauer ed Eeten (2009): *Cybersecurity: Stakeholder incentives, externalities, and policy options;* https://www.researchgate.net/publication/227426674_Cybersecurity_Stakeholder_incentives_externalities_and_policy_options
25 Christin (2011): *Network Security Games: Combining Game Theory, Behavioral Economics, and Network Measurements;* https://link.springer.com/chapter/10.1007/978-3-642-25280-8_2.
26 McConachie (2014): *Anti-Spoofing, BCP 38, and the Tragedy of the Commons;* https://www.circleid.com/posts/20140801_anti_spoofing_bcp_38_and_the_tragedy_of_the_commons/.
27 Vixie et al. (2014): *Abuse of Customer Premise Equipment and Recommended Actions;* https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=312647.
28 Vlajic e Zhou (2018): *IoT as a Land of Opportunity for DDoS Hackers;* https://ieeexplore.ieee.org/abstract/document/8423144
29 Il caso più eclatante è la botnet Mirai, che al suo apice nel 2016 comprendeva fino a 500 000 dispositivi IoT compromessi ed è stata utilizzata per attacchi DDoS molto potenti. Per una panoramica generale del ruolo dell'IoT negli attacchi DDoS, v. Vingau, Khoury e Hallé (2019): *10 Years of IoT Malware: A Feature-Based Taxonomy;* https://ieeexplore.ieee.org/abstract/document/8859496.
30 Consiglio federale (2020): *Standard di sicurezza per i dispositivi connessi a Internet;* https://www.efd.admin.ch/dam/efd/de/dokumente/home/dokumentation/berichte/internet-things.pdf.download.pdf/29042020%20Bericht%20IoT-d.pdf
31 Iana (2021): *Number Resources* di https://www.iana.org/numbers.

1.2.3.5 Varianti alternative

Rispetto allo status quo – definito dalla LTC riveduta – la modifica dell'OST introduce delle precisazioni in linea con le intenzioni esposte nel messaggio sulla revisione della LTC. Se si rinunciasse a tali precisazioni, l'obbligo dei fornitori derivante dall'articolo 48*a* LTC non verrebbe meno, ma rimarrebbe poco chiaro e si creerebbe un'incertezza giuridica.
In alternativa allo status quo, vi sarebbe la possibilità di prevedere misure concrete più restrittive di quelle descritte nel progetto. Secondo quest'ultimo, i provider non sono obbligati a bloccare l'accesso a Internet o agli elementi di indirizzo che rappresentano una minaccia, ma hanno solo il diritto di farlo. Si è deliberatamente rinunciato a un obbligo di blocco poiché ai fornitori deve essere data la libertà di giudicare liberamente e autonomamente in quali casi occorra un blocco; possono dunque garantire la sicurezza dei servizi offerti con i mezzi che più ritengono idonei. L'alternativa sarebbe di introdurre un blocco obbligatorio o su ordine delle autorità. È stata scartata anche l'introduzione di un obbligo per i fornitori di proteggere i loro clienti dagli attacchi DDoS[32]: per adempiervi i fornitori dovrebbero essere in grado di intercettare un volume di traffico Internet molto più elevato del normale e gli strumenti necessari sono relativamente costosi. Inoltre, il mercato offre già la protezione contro gli attacchi DDoS e i clienti possono acquistarla. Non è quindi necessario richiedere ai fornitori di proteggere tutti i loro clienti da questi attacchi.

2 Punti essenziali del progetto

2.1 Regolamentazione proposta

La regolamentazione proposta prevede una modifica dell'articolo 96 OST per istituzionalizzare la cooperazione tra l'UFCOM e la Centrale nazionale d'allarme nella ricezione e nel trattamento delle segnalazioni di interferenze sulle reti e sui servizi di telecomunicazione. Nuove disposizioni prevedono misure per combattere la manipolazione non autorizzata degli impianti di telecomunicazione commessa con trasmissione mediante telecomunicazione e per garantire la sicurezza delle reti radiomobili a partire dalla quinta generazione.

2.2 Questioni relative all'attuazione

2.2.1 Sicurezza delle reti mobili a partire dalla quinta generazione

Il progetto si limita in gran parte a misure attuate anche in altri Paesi, soprattutto nell'UE che sono perlopiù basate su standard internazionali (ad esempio 3GPP)[33] sviluppati anche con la partecipazione dell'industria della radiocomunicazione mobile[34]. Per quanto riguarda gli audit secondo l'articolo 96*g*, deve essere controllato in particolare il rispetto delle norme riconosciute, a tal fine esistono anche processi già collaudati.

2.2.2 Manipolazioni non autorizzate degli impianti di telecomunicazione

Quanto all'obbligo degli IAP di informare i clienti secondo la misura 1, si presuppone che i canali di comunicazione con il cliente siano oramai stabiliti. Il filtraggio dei pacchetti IP con un indirizzo IP sorgente falsificato (misura 2) è una procedura ben consolidata per la quale gli IAP possono ricorrere, se necessario, ad aiuti liberamente disponibili (cfr. numero 1.2.3.1). Nella maggior parte dei casi per l'obbligo di configurare correttamente e manutenere i dispositivi terminali (misura 3), dovrebbe essere possibile basarsi sulle relazioni contrattuali esistenti con i fornitori e adeguarle se necessario. Nel caso della misura 4, un IAP deve intervenire solo se viene contattato ad esempio dall'NCSC; quindi avvia le misure di difesa entro un periodo di tempo ragionevole.

3 Commenti agli articoli

Gli articoli 96 e seguenti sono ripartiti in tre sezioni in base al loro campo d'applicazione specifico. La se-

32 NIS Cooperation Group (2020): *Report on Member States' Progress in Implementing the EU Toolbox on 5G Cybersecurity;* https://digital-strategy.ec.europa.eu/en/library/report-member-states-progress-implementing-eu-toolbox-5g-cybersecurity
33 3GPP (2021): *Partners;* https://www.3gpp.org/about-3gpp/partners
34 GSMA | Network Equipment Security Assurance Scheme (NESAS) - Security

zione 3 (segnalazione di interferenze) riguarda, come avviene tuttora, tutti i fornitori di servizi di telecomunicazione. Le disposizioni sulla manipolazione non autorizzata degli impianti di telecomunicazione (sezione 4) si applicano a qualsiasi fornitore di accesso a Internet. L'articolo 5 è limitato ai fornitori di radiocomunicazione mobile titolari di una concessione, ossia Salt, Sunrise UPC e Swisscom. Inoltre, considerata la materia in questione, le disposizioni della sezione 5 si applicano unicamente alle reti mobili a partire dalla quinta generazione (cfr. art. 96*d*).

Sezione 3 Segnalazione di interferenze (art. 96)

L'obbligo dei FST di segnalare all'UFCOM le interferenze durante l'esercizio delle reti è stato introdotto il 1° aprile 2007 nell'articolo 96 OST. Le modalità per la segnalazione di interferenze sono disciplinate nelle prescrizioni tecniche e amministrative dell'UFCOM relative alla segnalazione di interferenze sulle reti (RS 784.101.113/1.8).
Le interferenze vanno segnalate all'UFCOM via modulo web o e-mail, in alternativa per telefono. Le segnalazioni vengono elaborate durante le ore di ufficio e inoltrate ai servizi interessati.
Al fine di migliorare il trattamento e l'inoltro delle segnalazioni di interferenze ricevute, in futuro si prevede di collaborare con la Centrale nazionale d'allarme (CENAL). La ricezione di tali segnalazioni è un compito fondamentale della CENAL, a tal fine dispone di un'infrastruttura informatica sicura ed è operativa 24 ore su 24. La CENAL sarà in grado di elaborare e inoltrare le segnalazioni di interferenze in tempo reale. Questo aumenterà l'utilità delle segnalazioni, soprattutto per quanto riguarda la gestione delle crisi.
Oggi, alcuni FST inviano segnalazioni di interferenze non solo all'UFCOM ma anche alla CENAL. La prevista collaborazione tra l'UFCOM e la CENAL eliminerà vie parallele ridondanti e semplificherà il sistema di segnalazione.
Per attuare quanto sopra esposto, l'articolo 96 OST viene completato specificando che le relative interferenze vanno segnalate alla CENAL. L'UFCOM sarà a sua volta informato in merito dalla CENAL. In particolare, sulla base dei commenti emersi dalla procedura di consultazione e dalle consultazioni sulle prescrizioni tecniche e amministrative, la portata delle interferenze, come motivo più importante per l'obbligo di segnalazione delle interferenze, sarà ridotta a 10 000 clienti. In futuro, questo obbligo sarà disciplinato nell'OST e non più nelle prescrizioni tecniche e amministrative.
Infine, si prevede che in futuro i FST debbano fornire informazioni in merito alle interferenze su un sito web liberamente accessibile, poiché queste sono un elemento di valutazione della qualità dei servizi di telecomunicazione proposti ai sensi dell'articolo 12a capoverso 2 LTC.

Sezione 4 Manipolazione non autorizzata di impianti di telecomunicazione

A titolo introduttivo, si sottolinea che le disposizioni di questa sezione si applicano unicamente ai fornitori di accesso a Internet poiché, in base all'esperienza raccolta, sono gli unici ad essere colpiti dalla manipolazione non autorizzata degli impianti di telecomunicazione.

Art. 96a Misure di sicurezza

Se degli impianti di telecomunicazione sono infettati da malware, possono metterne in pericolo altri con cui possono stabilire una connessione. Il malware può diffondersi ulteriormente attraverso la connessione, o essere utilizzato per altre attività dannose, ad esempio l'invio di spam, il phishing o la partecipazione a un attacco DDoS. Per questo motivo, al capoverso 1 è necessario prevedere misure affinché gli impianti di telecomunicazione non vengano infettati o resi vulnerabili. Sono ipotizzabili diverse misure. Nel caso di attività dannose, la connessione Internet può essere bloccata o limitata per interrompere l'attività. Il blocco può anche essere applicato se un dispositivo vulnerabile viene utilizzato per un periodo di tempo più lungo. Questo spesso serve non solo a proteggere gli altri utenti, ma anche a proteggere la persona/impresa colpita (parola chiave attacchi ransomware). I dispositivi infettati possono anche essere messi in modalità sandbox (walled garden), in cui la connessione Internet al fornitore di servizi di telecomunicazione viene preservata ma quella a Internet è notevolmente limitata o bloccata. In questo modo l'impianto di telecomunicazione non rappresenta più un rischio per gli altri. Se le attività dannose sono associate a certi elementi di indirizzo (indirizzi IP o nomi di dominio), il loro accesso può essere bloccato per i clienti. Ove tecnicamente possibile, l'accesso ai servizi di emergenza deve essere escluso da queste misure.
Poiché gli utenti sono gravemente colpiti da blocchi e restrizioni del loro accesso a Internet, è imperativo che

siano informati tempestivamente dai relativi fornitori. Questi dovrebbero quindi comunicare agli utenti in modo trasparente le misure da loro adottate.
I fornitori autorizzati a bloccare o limitare l'uso in base alla presente disposizione dovranno rinunciare alle relative misure o almeno contattare il Servizio Sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni SCPT se sanno che il relativo accesso a Internet o il relativo elemento d'indirizzo è oggetto di un ordine di sorveglianza. Ciò dovrebbe risultare già dall'articolo 26 capoverso 2 lettera a della legge federale sulla sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (LSCPT; RS 780.1) e dall'articolo 29 capoverso 2 e 3 dell'ordinanza sulla sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (OSCPT; RS 780.11).
Il capoverso 2 delle presenti disposizioni disciplina la lotta contro gli attacchi alla disponibilità dei servizi Internet causati da una moltitudine di richieste (attacchi noti come *distributed denial of service*, DDoS). Questo caso è anche esplicitamente menzionato nel messaggio sulla revisione della LTC. Un elemento importante nella lotta contro gli attacchi DDoS è di impedire l'utilizzo di indirizzi IP falsificati da chi perpetra l'attacco (*spoofing*). Questo rende impossibili gli attacchi DDoS in uscita basati sullo spoofing dell'IP. A questo scopo, i fornitori di accesso a Internet sono obbligati a impiegare mezzi tecnici appropriati per filtrare pacchetti IP con un indirizzo IP sorgente falsificato provenienti dalla loro rete. Per impostare tali filtri d'ingresso, i fornitori devono allestire una lista aggiornata delle reti autorizzate, la quale può essere generata automaticamente dalla tabella di routing. I passi tecnici necessari sono descritti dall'Internet Engineering Task Force (IETF) nelle *Best Current Practices* BCP38 per *single-homed network* (reti in cui ogni dispositivo ha un indirizzo IP) e BCP84 per *multi-homed networked* (reti in cui un dispositivo ha diversi indirizzi IP).
I fornitori di accesso a Internet spesso mettono a disposizione dei loro clienti dei dispositivi terminali. Considerato che sono molto diffusi, svolgono un ruolo importante nella lotta contro gli incidenti informatici. Il capoverso 3 stabilisce quindi che i parametri di sicurezza di tutti i dispositivi forniti ai clienti vanno configurati secondo le regole riconosciute della tecnica e aggiornati senza indugio, fintanto che i relativi fornitori continuano ad esercitarne il controllo. Ciò include la possibilità di colmare le loro lacune di sicurezza tramite aggiornamenti.
Nel caso dei terminali mobili - indipendentemente dal fatto che funzionino con Android, iOS o un altro sistema operativo - è l'utente a decidere se e quando aggiornare il sistema operativo. I sistemi operativi di tali terminali non sono considerati impianti di telecomunicazione nella sfera di influenza e responsabilità di un operatore.
La situazione è diversa per le schede SIM (o eSIM) che vengono inserite in tali dispositivi: queste possono essere configurate o aggiornate esclusivamente dagli operatori. Durante la configurazione delle schede, occorre inoltre osservare le regole di sicurezza conformi allo stato della tecnica.
Se gli aggiornamenti non sono più possibili e ciò comporta un rischio per la sicurezza, i rispettivi dispositivi vanno sostituiti. L'UFCOM determina i dispositivi interessati da questa disposizione ed emana le necessarie prescrizioni tecniche e amministrative affinché l'esposizione ai rischi dovuta a tali dispositivi possa essere mantenuta il più bassa possibile. In particolare, terrà conto dei seguenti principi:

- Nessun dato di accesso standard (nome utente, password) può essere usato per accedere ai dispositivi terminali. I dati di accesso devono essere assegnati individualmente per ogni dispositivo. Se questo non è possibile a livello tecnico, quando il dispositivo viene messo in funzione, occorre forzare un cambiamento dei dati di accesso.
- I servizi non utilizzati sul terminale devono essere disattivati di default.
- Il traffico SMTP in uscita sulla porta 25 deve essere bloccato di default per tutte le connessioni dei clienti nell'area clienti privata (connessioni «residenziali», di solito indirizzi IP dinamici). Se c'è una necessità specifica o su richiesta giustificata del cliente, è ipotizzabile uno sblocco.
- Allo stato di consegna, il dispositivo terminale non deve avere per default nessuna porta liberamente accessibile da Internet. Le porte aperte necessarie per il funzionamento del terminale devono essere protette da misure tecniche (ad es. restrizione IP, Access Control List o simili).
- Le porte usate per la manutenzione remota da parte del fornitore devono essere limitate il più possibile (ad es. a un segmento di indirizzo IP usato dal fornitore per questo scopo).
- Il protocollo utilizzato per l'accesso alla manutenzione remota deve essere protetto con una tecnologia di criptaggio moderna.
- I terminali devono essere prontamente dotati degli aggiornamenti di sicurezza classificati come critici dal produttore. Se il produttore non fornisce più aggiornamenti per i terminali, questi devono essere sostituiti.

Per l'attuazione dei capoversi 2 e 3 è previsto un periodo transitorio di un anno.

Art. 96b Servizio di segnalazione

L'articolo 96*b* prevede che i fornitori di accesso a Internet gestiscano un servizio specializzato per la segnalazione di manipolazioni non autorizzate di impianti di telecomunicazione commesse con trasmissioni mediante telecomunicazione (il cosidd. abuse desk), al quale possono essere segnalate le manipolazioni in questione (infezioni, hacking o vulnerabilità del sistema, attacchi DDoS, spam, phishing, ecc.). Questo servizio specializzato dell'IAP ha il solo compito di raccogliere le segnalazioni di manipolazioni non autorizzate e di adottare di propria iniziativa le misure di difesa adeguate. Spetta al fornitore di servizi Internet decidere se la responsabilità di adottare le misure è del servizio di segnalazione o di qualcun altro all'interno dell'azienda. L'obbligo di adottare misure spetta all'azienda nel suo complesso. Non esiste un obbligo specifico di comunicare le segnalazioni ricevute a un'autorità specifica o a un servizio specializzato come l'NCSC, poiché l'obbligo di segnalazione da parte degli IAP è disciplinato esclusivamente dall'articolo 96 dell'OST. I fornitori sono liberi di gestire loro stessi questo *abuse desk* o di incaricare terzi a tal fine, può essere strutturato in base alle esigenze dei fornitori, ad esempio integrato nelle hotline degli ISP. Tuttavia, occorre garantire che misure difensive adeguate possano essere avviate entro un periodo di tempo ragionevole. Inoltre, vanno soddisfatti i seguenti requisiti tecnici e amministrativi:

- In linea di principio, va indicato un contatto (indirizzo e-mail) per ogni *network range* (indirizzo IP) (*abuse-c*) presso il *Regional Internet Registry* competente (RIR). Se ciò non avviene, i fornitori devono indicare un contatto generale per le domande tecniche (*tech-c*). Devono assicurarsi che questo contatto possa svolgere la funzione dell'*abuse desk*.
- I fornitori assicurano che le segnalazioni di manipolazioni possano essere notificate all'indirizzo fornito e che si possa rispondere alla segnalazione entro i termini stabiliti.
- Siccome le segnalazioni di manipolazione contengono spesso modelli che vengono trattenuti dai filtri antispam, eventuali filtri vanno configurati minuziosamente e occorre assicurarsi che il messaggio venga elaborato in ogni caso.

Se il concetto giuridico di «entro un periodo di tempo ragionevole» si rivelasse troppo vago, l'UFCOM potrebbe eventualmente precisarlo nelle prescrizioni tecniche e amministrative, ad esempio prevedendo una durata specifica e/o adottando regole diverse a seconda della categoria di persone che effettuano la segnalazione. Le misure appropriate che un ISP può adottare non si limitano al blocco degli indirizzi IP e/o di altri elementi d'indirizzo, ma possono includere qualsiasi misura ritenuta opportuna contro le manipolazioni non autorizzate degli impianti di telecomunicazione.

Art. 96c *Esecuzione*

L'UFCOM esegue la presente disposizione ed emana le relative prescrizioni tecniche e amministrative. In tale ambito, riceve il sostegno tecnico dal NCSC.

Sezione 5 *Sicurezza delle reti e dei servizi esercitati dai concessionari di radiocomunicazione mobile*

Art. 96d *Applicazione*

Tutte le disposizioni riguardanti le funzioni di sicurezza saranno valide per le reti 5G Stand Alone (secondo le norme 5G 3GPP TS 33.501), per le reti 5G Non Stand Alone e per quelle delle generazioni future. Le attuali reti 5G non hanno una rete centrale 5G, si tratta di reti 5G Non Stand Alone con stazioni radio 5G che operano attualmente sull'infrastruttura di rete 4G esistente e non su un'infrastruttura 5G completa (5G Stand Alone).
Le funzioni di sicurezza 5G per il criptaggio del traffico dati, l'accesso alla rete e l'autenticazione (TS 33.501), standardizzate dal 3GPP, sono basate sulla sicurezza 4G, ossia molte funzioni di sicurezza 5G sono identiche alle funzioni di sicurezza dello standard 4G.
Le nuove funzioni di sicurezza aggiunte nello standard 5G (ad es. la protezione contro lo spoofing della rete centrale per le frodi in roaming, la protezione dal tracciamento degli utenti, l'autenticazione senza SIM dei dispositivi IoT) si basano sull'esistenza di una rete centrale 5G (funzioni logiche per gestire i nuovi accessi e il controllo delle stazioni radio 5G). Pertanto, le funzioni di sicurezza specificate nella norma TS 33.501 che

vanno oltre lo standard 4G non possono essere tecnicamente implementate prima dell'introduzione dello standard 5G (*Stand Alone*). Sembra logico mantenere le misure adottate per aumentare la sicurezza anche nelle reti delle tecnologie future.

Art. 96e *Gestione della sicurezza*

L'infrastruttura di radiocomunicazione mobile 5G e quella successiva, nonché le informazioni che genera ed elabora sono beni importanti che vanno gestiti in modo coscienzioso per garantire l'affidabilità e la disponibilità dei servizi.
Il capoverso 1 impone ai concessionari di radiocomunicazione mobile di sviluppare, implementare e verificare continuamente un sistema di gestione della sicurezza delle informazioni SGSI (*Information Security Management System*, ISMS), conformemente a quanto già realizzato dalla maggior parte di questi.
L'implementazione di un SGSI richiede una fase di pianificazione durante la quale vengono identificati e valutati i rischi posti dall'organizzazione in questione. Questa prima fase permette di definire una politica di sicurezza che tiene conto dei rischi da considerare, e poi di descrivere gli obiettivi di sicurezza da raggiungere e il perimetro da proteggere. Su questa base l'organizzazione infine determinerà i controlli corrispondenti alla sua politica di sicurezza e ai rischi da cui ha scelto di proteggersi.
Nel settore delle tecnologie dell'informazione e della comunicazione, i SGSI sono stati sviluppati sotto forma di standard. Si tratta segnatamente della serie di norme ISO/IEC 2700x (Information technology - Security techniques - Information security management systems – Requirements; ISO/IEC 27002:2005 Information technology – Code of pratice for Information Security Management; ISO/IEC 27011:2008 Information technology - Security techniques - Information security management guidelines for telecommunications organizations based on ISO/IEC 27002), a cui si deve fare riferimento nelle prescrizioni tecniche e amministrative secondo l'articolo 96*g* capoverso 1.
Queste norme coprono in particolare gli aspetti della sicurezza fisica, della gestione degli accessi e della sicurezza dei software. Sebbene la gestione della continuità operativa e la gestione degli incidenti di sicurezza siano solitamente incluse anche nel SGSI come descritte negli standard ISO/IEC 2700x, questi aspetti sono ancora menzionati al capoverso 2 poiché devono essere obbligatoriamente presi in considerazione quando si forniscono servizi al grande pubblico. Per precisare i requisiti per la gestione della continuità e degli incidenti, si prevede di fare riferimento allo standard ISO 22301:2019 *Security and resilience — Business continuity management systems — Requirements* nelle prescrizioni tecniche e amministrative.
Un SGSI è rivolto alla direzione dell'impresa, ai collaboratori responsabili della sicurezza e ai valutatori esterni. Una valutazione indipendente da parte di un organo di certificazione accreditato può portare a una certificazione riconosciuta della capacità della società in questione di gestire la sicurezza. Attualmente non si prevede di imporre tale certificazione ai concessionari di radiocomunicazione mobile. Nell'ambito dei suoi compiti di vigilanza, l'UFCOM può tuttavia chiedere al concessionario di fornire informazioni sull'implementazione del SGSI (cfr. art. 96*g* cpv. 2).
Un SGSI è sviluppato in funzione di obiettivi, necessità, requisiti e rischi associati alle attività dell'organizzazione in questione. Questo dipende anche dalle tecnologie utilizzate e dalla clientela, nonché dalle dimensioni e dalla struttura dell'organizzazione. Qualsiasi evoluzione di questi criteri deve portare ad un adeguamento del sistema di gestione della sicurezza. Lo sforzo richiesto per implementare un SGSI è quindi direttamente legato all'organizzazione e ai servizi proposti.

Art. 96f Esercizio degli impianti di telecomunicazione critici sul piano della sicurezza

Ai sensi del capoverso 1 della presente disposizione i concessionari di radiocomunicazione mobile devono garantire che gli impianti di telecomunicazione critici per la sicurezza da loro utilizzati siano conformi allo stato della tecnica. L'UFCOM può definire gli impianti critici per la sicurezza, se necessario, in collaborazione con l'industria. L'elenco degli impianti critici sarà riportato nelle relative prescrizioni tecniche e amministrative (art. 96*g* cpv. 1).
A livello europeo, e a seguito di una domanda della Commissione europea, l'ENISA (European Union Agency for Cybersecurity) preparerà un nuovo schema di certificazione della sicurezza informatica 5G. Questo passo fa seguito al *toolbox 5G* sviluppato dall'Unione Europea per la sicurezza delle reti 5G. Dovrebbe contribuire a migliorare la sicurezza informatica di questo tipo di rete poiché aiuta a eliminare alcuni rischi.
A tal fine, questo sistema di certificazione della sicurezza informatica 5G sarà basato su disposizioni e sistemi di certificazione della sicurezza informatica già esistenti, nonché sull'esperienza già acquisita

dall'ENISA da quando ha iniziato a impegnarsi nella certificazione della sicurezza informatica. Questo programma è ora in corso e all'inizio dell'estate 2021 è stato lanciato un bando di concorso per ricercare esperti. Non appena questo sistema di certificazione sarà disponibile per lo standard 5G, l'UFCOM esaminerà le possibilità di utilizzarlo.
Tuttavia, ci sono già altri standard riconosciuti in questo settore, come quelli prescritti dal GSMA NESAS (*Network Equipment Security Assurance Scheme*[35]). Il GSMA NESAS è un'iniziativa volontaria dell'industria della telefonia mobile volta a lanciare un programma di miglioramento continuo della sicurezza per le attrezzature e le infrastrutture delle reti mobili, copre i dispositivi che supportano le funzioni definite dal 3GPP e impiegate dagli operatori mobili nelle loro reti. Il GSMA NESAS sviluppa standard di sicurezza e certificazioni ampiamente riconosciuti in tutto il mondo e a cui partecipa l'intero settore delle telecomunicazioni. Quest'ultimo ha grande fiducia in queste specifiche, il che assicura che il progresso tecnico non sia rallentato[36]. Va notato che il GSMA NESAS non copre né la fornitura di apparecchiature di rete, né la configurazione e l'esercizio dei dispositivi di rete mobile.
La GSMA ha sviluppato i requisiti e i processi di sicurezza per il NESAS in collaborazione con il 3GPP, gli operatori e i venditori di apparecchi. La GSMA tiene aggiornata una lista di fornitori di apparecchiature che partecipano al programma e che sono stati sottoposti a una valutazione della sicurezza dei loro processi di sviluppo e del ciclo di vita, così come a una valutazione della sicurezza dei loro prodotti di rete.
Nella sua versione attuale, il GSMA NESAS include gli elementi necessari per sviluppare un sistema di certificazione. Nel quadro della progettazione di un sistema di certificazione, il GSMA NESAS definisce:

- La nomina di un organismo di controllo;
- L'accreditamento dei laboratori di prova;
- I requisiti di sicurezza legati ai processi dei fornitori e ai prodotti di rete, e i metodi per valutare i processi dei fornitori e i prodotti.

Alcuni fornitori di apparecchiature di rete mobile (in particolare cinesi) sono stati oggetto di una valutazione e di un controllo indipendente (laboratori di prova certificati dal GSMA NESAS) in merito ai loro processi di sviluppo e del ciclo di vita di certi prodotti. Questo per dimostrare come la sicurezza è stata integrata nei loro processi di progettazione, sviluppo, implementazione e manutenzione (ad es. per le linee di prodotti 5G gNodeB che sono stazioni base).
Nonostante il lavoro svolto finora, non è ancora chiaro quali standard e quale schema di certificazione saranno applicati nei Paesi europei. L'UFCOM specificherà questi punti non appena saranno definite le norme europee sulla certificazione degli impianti di telecomunicazione critici sul piano della sicurezza. L'armonizzazione delle normative svizzere con quelle dei Paesi dell'UE è sensata. Va evitata una soluzione puramente svizzera, bisognerebbe piuttosto sfruttare il peso del mercato europeo, perché è molto probabile che i prodotti utilizzati in Svizzera siano stati sviluppati, fabbricati e testati o certificati all'estero.
Il capoverso 2 della presente disposizione stabilisce che i concessionari di radiocomunicazione mobile esercitano i loro centri operativi di rete (*Network Operations Centres)* e i centri operativi di sicurezza (*Security Operations Centres)* esclusivamente in Stati la cui legislazione assicura una protezione adeguata dei dati. Secondo l'articolo 6 capoverso 1 della legge federale sulla protezione dei dati (LPD, RS 235.1) i dati personali non possono essere comunicati all'estero qualora la personalità della persona interessata possa subirne grave pregiudizio, dovuto in particolare all'assenza di una legislazione che assicuri una protezione adeguata. Ai sensi dell'articolo 7 dell'ordinanza relativa alla legge federale sulla protezione dei dati (OLPD, RS 235.11), l'Incaricato federale della protezione dei dati e della trasparenza pubblica un elenco degli Stati che dispongono di una legislazione che assicuri una protezione adeguata dei dati. Nella LPD completamente riveduta (entrata in vigore: 1° settembre 2023), la comunicazione di dati personali all'estero è disciplinata dagli articoli 16 e seguenti. Spetta al Consiglio federale valutare l'adeguatezza della legislazione straniera in materia di protezione dei dati. Sulla base dell'articolo 8 capoverso 1 della nuova ordinanza sulla protezione dei dati (OLPD), gli Stati, territori, determinati settori di uno Stato o di un organismo internazionale con una protezione adeguata dei dati sono elencati nell'allegato 1. Limitando le sedi dei centri operativi ai Paesi che figu-

35 https://www.gsma.com/security/network-equipment-security-assurance-scheme/.
36 Cfr. regolamento 2019/881 (UE) 2019/881 del Parlamento europeo e del Consiglio del 17 aprile 2019 relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 («regolamento sulla cibersicurezza»), GU L 151/15.

rano in questo elenco mira in particolare a garantire che il traffico transfrontaliero di dati nella radiocomunicazione mobile soddisfi i requisiti della legge svizzera sulla protezione dei dati.
Secondo l'Allegato 1B dell'Accordo che istituisce l'Organizzazione mondiale del commercio (General Agreement on Trade in Services; GATS, RS 0.632.20), articolo II, i servizi e i fornitori di servizi di ciascun membro dell'OMC devono essere trattati con ugual favore (clausola della nazione più favorita). Tuttavia, l'articolo XIV del GATS prevede delle eccezioni che possono giustificare misure in presenza di determinate condizioni. In particolare, l'articolo XIV lettera c) consente di adottare misure necessarie a garantire l'osservanza delle disposizioni di legge. L'attuale restrizione a Paesi che dispongono di un'adeguata protezione dei dati ai sensi della legge sulla protezione dei dati è quindi una misura compatibile con gli obblighi della Svizzera nell'ambito dell'OMC.

Art. 96g Prescrizioni applicabili e vigilanza

Per la sicurezza delle reti radiomobili a partire dalla quinta generazione, l'UFCOM può emanare prescrizioni tecniche e amministrative e dichiarare vincolanti le norme tecniche generalmente riconosciute sotto forma di riferimenti statici e diretti (art. 96g cpv. 1). I progetti di tali prescrizioni e norme sono notificati all'Organizzazione mondiale del commercio (OMC) e all'Associazione europea di libero scambio (AELS) nell'ambito degli accordi sugli ostacoli tecnici al commercio, conformemente alle disposizioni dell'ordinanza del 17 giugno 1996 (ON; RS 946.511) sulla notificazione delle prescrizioni e norme tecniche nonché sui compiti dell'Associazione Svizzera di Normazione. La prova della conformità a queste norme può essere presentata dai fornitori interessati ad esempio mediante certificazione da parte di un organo competente nel quadro del sistema di accreditamento svizzero (cfr. ordinanza del 17 giugno 1996 sull'accreditamento e la designazione; RS 946.512) o nel quadro di altri sistemi di certificazione (GSMA NESAS, sistemi europei di certificazione della sicurezza informatica[37]). In mancanza di una certificazione volontaria del loro sistema di gestione della sicurezza (art. 96e) o se vi sono dubbi quanto alla conformità degli impianti di telecomunicazione allo stato della tecnica (art. 96f cpv. 1), un concessionario di radiocomunicazione mobile può essere obbligato, nell'ambito della vigilanza, a sottoporsi a sue spese a un audit o a far verificare i suoi impianti di telecomunicazione e a presentare i risultati di tale audit o verifica all'UFCOM (cpv. 2). Tuttavia, una tale misura può essere adottata unicamente nell'ambito dell'articolo 58 capoverso 2 LTC se vi è il sospetto fondato che il concessionario non rispetti le prescrizioni degli articoli 96*e* e 96*f* e se l'UFCOM non è in grado di accertare direttamente i fatti rilevanti. In mancanza di un tale sospetto, questa misura sarebbe invece esclusa in particolare nel quadro di una vigilanza generale ai sensi dell'articolo 58 capoverso 1 LTC (campagne di vigilanza). Bisognerà anche assicurarsi che l'organo qualificato tratti in modo confidenziale le informazioni a cui ha accesso, in particolare quelle relative a un'eventuale misura di vigilanza ai sensi della LSCPT.

4 Ripercussioni

4.1 Ripercussioni sulla Confederazione

4.1.1 Sicurezza delle reti mobili a partire dalla quinta generazione

Le conseguenze sulla Confederazione, in merito alle finanze, al personale e ad altri aspetti sono state esaminate e non se ne prevedono in misura rilevante nella prima fase. L'attuazione e l'assunzione dei costi devono essere garantite inizialmente dalle aziende. L'UFCOM si aspetta tuttavia spese supplementari nel settore della standardizzazione e della sorveglianza in relazione alla sicurezza delle reti mobili 5G e future, difficilmente quantificabili al momento. In una prima fase, questi compiti supplementari dovranno essere integrati nei processi di lavoro dell'UFCOM, ma gli ulteriori sviluppi in questo senso dovranno essere seguiti da vicino.

37 Cfr. regolamento 2019/881 (UE) 2019/881 del Parlamento europeo e del Consiglio del 17 aprile 2019 relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 («regolamento sulla cibersicurezza»), GU L 151/15.

4.1.2 Manipolazioni non autorizzate degli impianti di telecomunicazione

Le conseguenze sulla Confederazione, in merito alle finanze, al personale e ad altri aspetti sono state esaminate e non se ne prevedono in misura rilevante per la Confederazione nel suo complesso. Il Centro nazionale per la cibersicurezza (NCSC) informa già i fornitori su possibili attacchi informatici diretti alla loro rete o perpetrati dalla loro rete, poiché questo è di grande importanza per la sicurezza informatica della Svizzera. Il compito del NCSC descritto nell'ordinanza può quindi essere svolto con le risorse esistenti. All'UFCOM, i nuovi compiti nel settore della sicurezza informatica e la collaborazione con il NCSC richiedono uno o due posti supplementari. Il NCSC dispone di un contingente di posti a tale scopo. In passato l'UFCOM aveva già espresso le sue necessità ma non era stato considerato. Con le attuali disposizioni, queste sono ora sufficientemente concrete. Nel complesso, non vi sono effetti rilevanti per la Confederazione, poiché il contingente di posti di lavoro esiste già.

4.2 Ripercussioni per l'economia

4.2.1 Sicurezza delle reti mobili a partire dalla quinta generazione

Le quattro misure proposte per la sicurezza delle reti 5G, implicano dei costi per i tre concessionari di radiocomunicazione mobile (*Mobile Network Operators,* MNO) attivi in Svizzera.
Tra fine marzo e metà di maggio 2021, l'UFCOM ha condotto un sondaggio presso questi tre operatori sulle misure tecniche provenienti dal *toolbox* 5G dell'UE che hanno adottato e/o prevedono di adottare e sui loro costi.
L'indagine ha mostrato che nel quadro dei loro sistemi di gestione della sicurezza delle informazioni (SGSI), i fornitori danno grande importanza allo standard ISO 27001. A questo standard e a norme comparabili dovrebbero riferirsi anche i requisiti specificati nelle prescrizioni tecniche e amministrative. I concessionari, quindi, non si devono aspettare grandi cambiamenti e costi rispetto alla situazione attuale.
Dai risultati del sondaggio emerge che, in linea di principio, i concessionari sostengono la certificazione degli elementi di rete ed esigono anche certi requisiti di sicurezza dai loro fornitori. Danno la priorità agli standard internazionali, soprattutto il GSMA NESAS, si suppone quindi che un regolamento in questo settore non porterà a costi aggiuntivi significativi.
L'obbligo di gestire i centri operativi di rete e di sicurezza esclusivamente in Stati la cui legislazione assicura una protezione adeguata dei dati è già fondamentalmente soddisfatto. I concessionari hanno descritto le misure adottate in modo più o meno dettagliato. La maggior parte ha fornito poche o nessuna informazione sui costi specifici associati alle misure. Di conseguenza, si possono fare solo affermazioni qualitative sui costi. Inoltre, agli operatori possono incombere costi a causa di possibili obblighi di audit. Tuttavia, soprattutto nel caso di un elevato grado di conformità agli standard pertinenti, gli audit dovrebbero essere pochi, poiché l'obbligo di audit a carico del rispettivo concessionario può essere imposto nel quadro dell'articolo 58 capoverso 2 LTC solo se vi è il sospetto fondato che un concessionario non rispetti le prescrizioni di cui agli articoli 96e o 96f e l'UFCOM non è in grado di accertare direttamente i fatti rilevanti. I costi di un audit individuale dipendono dal tipo di esame. Secondo le stime, nella maggior parte dei casi si tratta di un importo nell'ordine delle decine di migliaia[38].
Il beneficio per l'economia deriva dalla possibilità di evitare costi a carico delle economie domestiche, delle aziende e di altri gruppi sociali in caso di rischi legati alla sicurezza delle reti mobili. Per esempio, le panne a livello della copertura di radiocomunicazione mobile hanno un impatto potenzialmente significativo. La stessa radiocomunicazione mobile[39] sta giocando un ruolo sempre più importante tra gli utenti[40] di Internet e le aziende[41]. Nel dossier sui pericoli «Interruzione della telefonia mobile», l'UFPP calcola che tre giorni di

38 Questa stima si basa su valori di riferimento selezionati dal portale di offerte gryps.ch per le PMI con 60 dipendenti [GRYPS]2021]: *ISO Zertifizierung Kosten*; https://www.gryps.ch/produkte/iso-9001-zertifizierung-178/kosten/). Per un audit di certificazione iniziale, ad esempio, si stima un valore indicativo di 16 000 CHF. Tuttavia, i concessionari sono nettamente più grandi, il che significa che ci si deve aspettare costi molto più alti per un audit. Inoltre, l'ambito da sottoporre ad audit è di solito molto più piccolo che in un audit di certificazione iniziale, il che a sua volta ne riduce la stima dei costi. A causa di questi effetti opposti, sembra probabile che i costi risultanti saranno inferiori a 100 000 CHF.

39 Come descritto al n. 1.1.1 la radiocomunicazione mobile viene fornita sempre più via 5G.

40 Secondo l'UST(2020): *Mobile Internetnutzung* (disponibile solo in tedesco e francese)*;* https://www.bfs.admin.ch/bfs/de/home/statistiken/kultur-medien-informationsgesellschaft-sport/informationsgesellschaft/gesamtindikatoren/haushalte-bevoelkerung/mobile-internetnutzung.assetdetail.12307308.html, l'84% degli utenti svizzeri di Internet tra i 16 e i 74 anni hanno utilizzato un cellulare nel 2019.

41 Secondo l'UST (2019): *IKT Infrastruktur in den Unternehmen* (disponibile solo in tedesco e francese)*;* https://www.bfs.admin.ch/bfs/de/home/statistiken/kultur-medien-informationsgesellschaft-sport/informationsgesellschaft/gesamtindikatoren/unternehmen/ikt-infrastruktur.assetdetail.8486582.html, il 77% delle aziende ha utilizzato connessioni a banda larga mobile nel 2017.

panne totale di un grande fornitore di radiocomunicazione mobile comporterebbero perdite aggregate dell'ordine di nove miliardi di franchi. Tuttavia, un tale guasto molto improbabile[42] ma comunque rilevante a causa dell'impatto dannoso menzionato è solo uno degli effetti possibili. Le lacune di sicurezza nel funzionamento e nell'infrastruttura delle reti mobili possono aprire la strada a vari tipi di attacchi informatici contro le applicazioni e i dati trasmessi via 5G (e tecnologie successive), si pensi al furto di dati e al ricatto. Uno studio relativamente recente sulle piccole e medie imprese (PMI) mostra che un quarto delle PMI svizzere intervistate è già stato vittima di un attacco informatico e circa un terzo ha subito danni finanziari e, in misura minore, perdite di dati dei clienti e/o danni alla reputazione[43]. Secondo uno studio austriaco nonostante il periodo economicamente difficile della pandemia, quasi tre quarti delle aziende intervistate hanno aumentato il loro budget per la sicurezza informatica[44].
Tuttavia, come descritto, questi potenziali effetti vantaggiosi sull'economia sono indiretti. Inoltre, la probabilità di un'interruzione, ad esempio, difficilmente può essere imputata a singole misure di sicurezza e il potenziale di danno dei rischi informatici è difficile da misurare[45]. Di conseguenza, il beneficio delle misure proposte non può essere quantificato.

4.2.2 Manipolazioni non autorizzate degli impianti di telecomunicazione

Il beneficio per l'economia nazionale consiste nel fatto che possono essere evitati costi dovuti ad attacchi informatici che andrebbero poi a carico delle economie domestiche, delle aziende e di altri gruppi sociali. I costi economici degli attacchi informatici descritti ai numeri 1.1.2 e 1.2.3 e nei primi due punti di controllo AIR (analisi d'impatto della regolamentazione) sono elevati e sono aumentati notevolmente negli ultimi anni. Non è facile calcolarli, poiché non tutte le vittime di un attacco informatico rendono pubblica tale informazione ed è molto difficile quantificare i costi indiretti causati da questi attacchi (ad es. danni alla reputazione, perdita di fiducia, insoddisfazione dei clienti). Inoltre, i benefici difficilmente possono essere imputati a singole misure di sicurezza. Tuttavia, è indiscusso che il danno causato dagli attacchi informatici ha raggiunto da tempo una dimensione economicamente rilevante. Le misure per ridurre questi costi hanno quindi un impatto positivo diretto.
Si presume in generale che la sicurezza informatica diventerà sempre più un fattore competitivo nella digitalizzazione. Affinché la Svizzera possa sfruttare i suoi vantaggi dovuti alla sua competitività anche nell'economia digitale, occorre creare le condizioni necessarie a livello normativo. I requisiti minimi di sicurezza imposti ai fornitori di accesso a Internet contribuiscono a sfruttare il potenziale economico della digitalizzazione[46].
Pur avendo un effetto positivo sull'economia in generale e sulla politica sociale (cfr. n. 4.3.2), le misure proposte comportano costi per gli IAP. Non è possibile quantificare i costi, poiché molti fattori, come la portata delle misure già implementate dai fornitori o la riduzione dei costi dovuta agli sviluppi tecnici, sono molto difficili da rilevare. Questa sezione fornisce quindi una valutazione qualitativa dei costi e affronta in particolare gli effetti prevedibili, soprattutto sui fornitori più piccoli. Nel 2019, l'86 per cento della quota di mercato in termini di numero di clienti era concentrato su cinque grandi IAP. Allo stesso tempo, queste aziende rappresentano solo una frazione di tutti gli IAP operanti in Svizzera. In totale, circa 170 IAP sono attivi in Svizzera. Di questi, circa il 60 per cento ha tra 1 e 1000 clienti Internet, il 25 per cento tra 1000 e 10 000 e il 15 per cento ha oltre 10 000 clienti.[47]

42 La probabilità di una tale panne (scenario 2 - forte) è indicata come circa una volta in 30 anni. UFPP (2020). *Interruzione della telefonia mobile;* https://www.babs.admin.ch/it/aufgabenbabs/gefaehrdrisiken/natgefaehrdanalyse/gefaehrddossier.html. Le basi metodologiche sono descritte in UFPP (2020) Metodologia sull'analisi nazionale dei rischi; https://www.babs.admin.ch/it/aufgabenbabs/gefaehrdrisiken/natgefaehrdanalyse.html.

43 Peter et al. (2020): *Digitalisierung, Home-Office und Cyber-Sicherheit in KMU;* https://www.fhnw.ch/de/die-fhnw/hochschulen/hsw/media-newsroom/news/digitalisierung-home-office-und-cyber-sicherheit/media/digitalisierung-home-office-cyber-sicherheit-kmu-2020-12.pdf o rapporto finale del Gfs-zürich (2020) *Homeoffice-Welle in Schweizer KMU: Chancen wahrgenommen – Cyberrisiken unterschätzt;* https://gfs-zh.ch/homeoffice-welle-in-schweizer-kmuchancen-wahrgenommen-cyberrisiken-unterschaetzt/.

44 KPMG (2021): *KPMG Studie: Cyberrisiken werden durch die Pandemie beschleunigt;* https://home.kpmg/at/de/home/media/press-releases/2021/04/kpmg-studie-cyberrisiken-werden-durch-die-pandemie-beschleunigt.html.

45 Biener et al. (2015): *Cyber Risk: Risikomanagement und Versicherbarkeit;* https://www.kessler.ch/fileadmin/09_PDFs/Cyber_Risk_Risikomanagement_und_Versicherbarkeit_de.pdf

46 Bundesamt für Sicherheit in der Informationstechnik (2016), (Ufficio tedesco per la sicurezza nella tecnica dell'informazione): *Cyber-Sicherheit als Wettbewerbsvorteil in der Digitalisierung,* https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Cyber-Sicherheit_als_Wettbewerbsvorteil.pdf?__blob=publicationFile&v=3

47 UFCOM (2021 in base alle cifre della statistica delle telecomunicazioni 2019): V. anche *Internet Service Provider;* https://www.bakom.admin.ch/bakom/de/home/telekommunikation/zahlen-und-fakten/sammlung-statistischer-daten/internet-service-provider.html

4.2.2.1 Costi della misura 1: Diritto di bloccare o limitare l'accesso a Internet o elementi di indirizzo e obbligo di informare il cliente

Dal momento che il blocco o la restrizione della connessione a Internet rimane a discrezione dei fornitori, tale misura genera costi solo se questi decidono di bloccare o limitare la connessione. Anche qui, i costi sono bassi e nell'interesse del fornitore. Per quanto riguarda l'obbligo d'informazione, il fornitore sostiene almeno gli stessi costi come per informare attivamente i clienti del blocco o della limitazione delle loro connessioni, perché si può supporre che in tal caso i clienti contatterebbero il loro fornitore di propria iniziativa. In entrambi i casi il servizio clienti deve sostenere un onere.

4.2.2.2 Costi della misura 2: Obbligo dei fornitori di filtrare i pacchetti IP il cui indirizzo IP sorgente è falsificato (*spoofing*)

L'introduzione di metodi per filtrare i pacchetti IP che hanno un indirizzo IP sorgente falsificato comporta uno sforzo tecnico e amministrativo per i fornitori. Devono implementare tecnicamente i filtri e identificare le reti autorizzate oltre che aggiornare costantemente i filtri in modo da non trattenere nessun pacchetto IP legittimo. Dal momento che la metodologia di filtraggio dell'ingresso è stata sviluppata 20 anni fa, gli ostacoli tecnici alla sua implementazione sono ora notevolmente ridotti, vi sono anche numerosi strumenti e guide liberamente disponibili[48].
Quando si valutano i costi, è importante notare che rispetto ai fornitori più grandi, quelli più piccoli devono sostenere spese nettamente inferiori e sforzi molto minori nel determinare quali reti sono autorizzate, necessitano inoltre di filtri meno complessi [49]. Inoltre, le connessioni in uscita con elementi di indirizzo falsificati dovrebbero essere impedite solo se questo è tecnicamente realizzabile per l'IAP con uno sforzo ragionevole.

4.2.2.3 Costi della misura 3: Obbligo dei fornitori di configurare in modo sicuro i dispositivi terminali messi a disposizione dei clienti

A seconda degli accordi contrattuali che i fornitori hanno con i produttori, la misura 3 può comportare prezzi più alti per l'acquisto e la manutenzione dei dispositivi terminali. I requisiti tecnici dei dispositivi possono essere soddisfatti dai produttori sostenendo costi minimi, ma i fornitori devono assicurarsi che questi ultimi siano contrattualmente obbligati a farlo. Le misure di sicurezza per la manutenzione a distanza, l'installazione tempestiva degli aggiornamenti di sicurezza e la sostituzione del terminale giunto a fine vita sono invece responsabilità dei fornitori. I produttori forniscono però gli aggiornamenti necessari, questo riduce in generale gli oneri per i fornitori. A lungo termine i rischi e la manutenzione di terminali non sicuri od obsoleti comportano probabilmente più costi rispetto a una corretta configurazione e manutenzione dei dispositivi. Anche la misura 3 tenderà ad essere più costosa per i fornitori più grandi piuttosto che per quelli più piccoli, questi hanno meno terminali in uso e possono quindi garantirne una configurazione e una manutenzione sicura con meno risorse.
Va notato che l'articolo 96*a* capoverso 3 disciplina solo il caso in cui i dispositivi sono forniti al cliente dall'IAP. Se il cliente acquista il suo dispositivo presso un fornitore terzo, l'IAP non sostiene alcun costo di regolamentazione. Dopo la consegna dei dispositivi, eventuali costi aggiuntivi, ad esempio per l'installazione di aggiornamenti di sicurezza, sono sostenuti solo se l'IAP detiene ancora il controllo sui dispositivi.

4.2.2.4 Costi della misura 4: Obbligo dei fornitori di allestire un centro specializzato per la segnalazione delle manipolazioni e avviare misure difensive

L'obbligo di allestire un centro per la segnalazione che assicuri una risposta entro i termini previsti comporta dei costi per i fornitori che non dispongono ancora di un tale servizio. Tuttavia, la richiesta di rispondere entro un periodo ragionevole evita che i fornitori debbano mantenere un servizio di picchetto durante la notte o il fine settimana. Inoltre, possono consultare il NCSC per sapere se la segnalazione dell'NCSC può passare anche attraverso altri canali, permettendo così ai fornitori di garantire la capacità di rispondere entro un periodo di tempo ragionevole al minor costo possibile. I costi per l'IAP sono compensati da un alto beneficio nella protezione delle altre connessioni, poiché solo una risposta rapida può ridurrne i rischi. I costi legati

48 MANRS (2016-2021): *Anti-Spoofing;* https://www.manrs.org/isps/guide/antispoofing/
49 Lone et al. (2020): *SAVing the Internet: Explaining the Adoption of Source Address Validation by Internet Service Providers;* https://weis2020.econinfosec.org/wp-content/uploads/sites/8/2020/06/weis20-final31.pdf

all'intervento o alle misure difensive sono difficili da quantificare, poiché variano molto a seconda del fornitore e, soprattutto, in funzione della minaccia. I possibili rischi e le appropriate misure difensive intraprese dagli IAP sono in continua evoluzione.

4.3 Ripercussioni sulla società

4.3.1 Sicurezza delle reti mobili a partire dalla quinta generazione

Tra le ripercussioni positive di questa misura figura anche l'impatto sulla società, in particolare sulla salute e la sicurezza. Ad esempio, il dossier sui pericoli dell'UFPP menzionato al numero 4.2 (Ripercussioni sull'economia) parla anche di morti, feriti e restrizioni nelle attività delle organizzazioni di pronto intervento come possibili conseguenze di una panne nei servizi di radiocomunicazione mobile.

4.3.2 Manipolazioni non autorizzate degli impianti di telecomunicazione

La digitalizzazione incide fortemente sulla società, poiché tocca direttamente la vita quotidiana delle persone. Gli incidenti informatici creano insicurezza presso le persone quando usano i servizi digitali. Affinché i cittadini abbiano fiducia nelle tecnologie digitali è importante che queste soddisfino uno standard minimo di sicurezza. Quando i consumatori acquistano un dispositivo da un IAP, dovrebbero quindi poter assumere che sia configurato secondo la misura 3, ossia dotato di una protezione minima contro gli attacchi informatici.

4.4 Ripercussioni in altri settori esaminati

4.4.1 Sicurezza delle reti mobili a partire dalla quinta generazione

Sono stati esaminati i possibili effetti su Cantoni e Comuni, nonché su centri urbani, agglomerati e zone di montagna, sull'ambiente e altro. Delle reti 5G e future sicure possono avere risvolti vantaggiosi indiretti. Tuttavia, non sono specifici e non riguardano particolari applicazioni e utenti della tecnologia 5G. Pertanto, gli effetti non possono essere approfonditi singolarmente per ogni settore. I benefici generali previsti sono descritti ai numeri 4.2 (Ripercussioni sull'economia) e 4.3 (Ripercussioni sulla società).

4.4.2 Manipolazioni non autorizzate degli impianti di telecomunicazione

Sono stati esaminati i possibili effetti su Cantoni e Comuni, nonché su centri urbani, agglomerati e zone di montagna, sull'ambiente e altro. Un maggiore livello di protezione nel settore della sicurezza informatica può avere risvolti positivi indiretti. Tuttavia, non sono specifici, motivo per cui tali effetti non possono essere approfonditi singolarmente per ogni settore. I benefici generali previsti sono descritti ai numeri 4.2 (Ripercussioni sull'economia) e 4.3 (Ripercussioni sulla società).

5 Aspetti giuridici

Le disposizioni proposte attuano l'articolo 48*a* LTC. Il capoverso 2 di questa disposizione delega al Consiglio federale ampie competenze legislative nel settore della sicurezza dell'informazione, delle infrastrutture e dei servizi di telecomunicazione. Secondo l'articolo 62 capoverso 2 LTC, il Consiglio federale può delegare all'UFCOM il compito di emanare le necessarie prescrizioni tecniche e amministrative (cfr. art. 105 cpv. 1 LTC). Nel fare ciò, l'UFCOM deve tenere conto delle norme applicabili a livello internazionale. In particolare, l'Unione europea sta istituendo un sistema di certificazione della sicurezza informatica per le reti 5G (cfr. commento all'art. 96*g*), che dovrebbe per quanto possibile essere utilizzato come base per gli articoli 96*d* a 96*g*.
L'obbligo di localizzare i centri operativi di rete e i centri operativi di sicurezza in determinati Paesi ai sensi dell'articolo 96*f* capoverso 2 è compatibile con l'articolo XIV lettera c, ii e iii dell'allegato 1B dell'Accordo che istituisce l'Organizzazione mondiale del commercio (Accordo generale sul commercio dei servizi, GATS) (vedi commenti sull'art. 96*f* cpv. 2).

Lista delle abbreviazioni

API	*Application Programming Interface*
AIR	Analisi d'impatto della regolamentazione
ASA	Associazione svizzera d'Assicurazioni
BCP	*Best Current Practices*
CENAL	Centrale nazionale d'allarme
CPE	*Customer Premises Equipment*
DDoS	*Distributed Denial Of Service attack*
ENISA	*European Union Agency for Cybersecurity*
ETIS	*The Community for Telecom Professionals*
FST	Fornitori di servizi di telecomunicazione
IAP	*Internet Access Provider* - fornitore di accesso a Internet
IETF	*Internet Engineering Task Force*
IP	*Internet Protocol*
ISO	*International Organization for Standardization*
LTC	Legge sulle telecomunicazioni
M3AAWG	*Messaging Malware Mobile Anti-Abuse Working Group*
MANRS	*Mutually Agreed Norms for Routing Security*
MNO	*Mobile Network Operator*
NCSC	Centro nazionale per la cibersicurezza
NOC	*Network Operation Center* – Centro operativo di rete
PMI	Piccole e medie imprese
RIR	*Regional Internet Registry*
SANS	*SysAdmin, Audit, Network, Security Institut*
SGSI	Sistema di gestione della sicurezza delle informazioni *(Information Security Management System – ISMS)*
SOC	*Security Operation Center – Centro operativo di sicurezza*
UFCOM	Ufficio federale delle comunicazioni
UFPP	Ufficio federale della protezione della popolazione
UIT	*Unione internazionale delle telecomunicazioni*