Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Il Consiglio federale

Berna, 15.12.2023

Infrastruttura digitale. Minimizzare i rischi geopolitici

Rapporto del Consiglio federale in adempimento del postulato 20.3984 Pult del 14.9.2020

Sintesi

Il postulato Pult 20.3984 chiede al Consiglio federale di presentare un rapporto su come minimizzare i rischi geopolitici legati alle infrastrutture digitali quali il 5G, e a fornitori di apparecchiature come l'azienda cinese *Huawei*.

La Svizzera è indubbiamente esposta a rischi tecnici con una componente geopolitica poiché molti dei suoi processi economici, sociali e politici sono gestiti da reti e sistemi digitali che possono presentare vulnerabilità o subire attacchi informatici. Nell'attuale contesto geopolitico diviso, la Svizzera incorre anche potenziali rischi geopolitici (ad es. blocco dell'accesso al suo mercato da parte dell'UE) legati a infrastrutture digitali e di telecomunicazione provenienti da fornitori considerati a rischio o controllati da uno Stato che presenta un rischio geopolitico.

Per rafforzare la resilienza delle telecomunicazioni, il Consiglio federale propone nuove misure basate su una strategia multi-vendor, sulle apparecchiature ritenute a rischio e sul prossimo bando per le frequenze. Per il resto, l'ecosistema svizzero della cibersicurezza dovrebbe essere in grado di fornire gli organismi nazionali di controllo e certificazione di cui il nostro Paese ha bisogno.

Seguendo l'esempio di quanto previsto dall'UE nel toolbox 5G e in altri progetti normativi, in particolare sulla ciber-resilienza, il Consiglio federale ritiene necessario inserire nella legge sulle telecomunicazioni (LTC; RS 784.10) una nuova disposizione che in caso di rischio geopolitico gli dia la possibilità di adottare le dovute misure. Si pensi a strumenti che gli permettono di vietare l'acquisto, l'installazione e l'esercizio di apparecchiature di fornitori ritenuti una minaccia per la sicurezza della Svizzera o che sono di proprietà, sotto il controllo o l'influenza di uno Stato estero che rappresenta un rischio geopolitico per la Svizzera. A tale proposito, la libertà economica e il corretto funzionamento della concorrenza devono essere garantiti nella misura del possibile.

La collaborazione internazionale rimane essenziale per garantire la sicurezza delle reti e delle infrastrutture digitali, data la loro interconnessione su scala globale.

Indice

Sintesi **2**
Abbreviazioni **5**
1 Il postulato 20.3984 ..... **6**
2 Infrastruttura svizzera di telecomunicazione **6**
2.1 Una panoramica del 5G 6
2.2 Rischi tecnici con una componente geopolitica 8
2.3 Rischi geopolitici veri e propri 9
3 L'attuale regime giuridico e politico **10**
3.1 Obblighi internazionali 10
3.2 Diritto delle telecomunicazioni e sicurezza delle reti 11
3.3 Resilienza delle infrastrutture critiche 12
3.4 Protezione degli impianti di telecomunicazione e di altri prodotti TIC 13
3.5 Strategia nazionale per la protezione della Svizzera contro i ciber-rischi 13
3.6 Misure adottate all'estero 14
3.7 Sintesi dell'attuale regime giuridico e politico 15

Abbreviazioni

3GPP	The 3rd Generation Partnership Project
5G	Rete di comunicazione mobile di quinta generazione
Cost.	Costituzione federale della Confederazione Svizzera
CSN	Ciberstrategia nazionale CSN
CYD	Cyber Defense
DDoS	Attacco DDoS (Distributed Denial of Service)
DFAE	Dipartimento federale degli affari esteri
EMPA	Istituto interdisciplinare di ricerca per le scienze dei materiali e lo sviluppo delle tecnologie all'interno del settore ETH
ENISA	Agenzia dell'Unione europea per la cibersicurezza (European Union Agency for Cyber-security)
ETHZ	Politecnico federale di Zurigo
ETSI	European Telecommunications Standards Institute (Istituto europeo delle norme di telecomunicazione)
FIRST	Forum of Incident Response and Security Teams
GATS	Accordo generale sul commercio dei servizi, AGCS (OMC) (General Agreement on Trade in Services)
GATT	Accordo generale sulle tariffe doganali e sul commercio (General Agreement on Tariffs and Trade)
GSMA	The GSM Association
LSIn	Legge federale sulla sicurezza delle informazioni in seno alla Confederazione
LTC	Legge sulle telecomunicazioni
n.	numero
NatCSIRT	National Computer Security Incident Response Team
NCSC	Centro nazionale per la cibersicurezza (National Cyber Security Center)
NESAS	Network Equipment Security Assurance Scheme
NOC	Network Operation Center (centro operativo di rete)
NTC	Istituto nazionale di test per la cibersicurezza (Nationales Testinstitut für Cybersicherheit)
OMC	Organizzazione mondiale del commercio
ONU	Organizzazione delle Nazioni Unite
OOIT	Ordinanza dell'UFCOM sugli impianti di telecomunicazione
O-RAN	Open Radio Access Network
OSCE	Organizzazione per la sicurezza e la cooperazione in Europa
OST	Ordinanza sui servizi di telecomunicazione
OTC	Accordo sugli ostacoli tecnici agli scambi (OMC)
RAN	Rete di accesso radio (Radio Access Network)
SCION	Scalability, Control, and Isolation on Next-Generation Networks
SGSI	Sistema di gestione della sicurezza dell'informazione
SOC	Security Operation Center (centro operativo di sicurezza)
SIC	Servizio delle attività informative della Confederazione
SSFN	Secure Swiss Finance Network
TF-CSIRT	Task Force Computer Security Incident Response Team
TIC	Tecnologie dell'informazione e della comunicazione
UE	Unione europea
UFAE	Ufficio federale per l'approvvigionamento economico del Paese
UFCOM	Ufficio federale delle comunicazioni
UIT	Unione internazionale delle telecomunicazioni

1 Il postulato 20.3984

Conformemente al postulato Pult 20.3984 del 14 settembre 2020, adottato il 17 giugno 2021 dal Consiglio nazionale, il Consiglio federale è incaricato di analizzare in un rapporto come ridurre al minimo i rischi geopolitici inerenti al potenziamento e allo sviluppo delle infrastrutture digitali come il 5G. Nella scelta dei fornitori di tecnologia, occorre tenere conto degli aspetti relativi alla qualità dei prodotti, all'affidabilità delle catene di fornitura della tecnologia, alla struttura aziendale dei fornitori e al quadro giuridico, a cui è soggetta la sede centrale dell'azienda. In particolare va anche chiarito quali rischi derivino da fornitori come Huawei, domiciliati in Paesi che non sono fondati né sull'economia di mercato né su uno stato di diritto. Infine, si tratta di rispondere alla domanda su come garantire che l'infrastruttura tecnologica svizzera non sia pregiudicata dalla concorrenza geoeconomica tra gli USA e la Cina, che si verificherà nel prossimo futuro.

Il postulato rientra in una serie di interpellanze parlamentari sui rischi geopolitici che la Svizzera incorre a livello delle catene di approvvigionamento e delle infrastrutture. Un rapporto del Consiglio federale del 24 novembre 2021 concernente la Sicurezza dei prodotti e il supply chain risk management nei settori della cibersicurezza e della ciberdifesa risponde ai postulati Dobler 19.3135 e 19.3136. In adempimento della mozione 20.3268 Häberli-Koller, il 31 agosto 2022 il Consiglio federale ha inoltre pubblicato il rapporto "Beni essenziali. Ridurre la dipendenza economica".

La mozione del Gruppo socialista 22.3414 "Protezione dell'infrastruttura critica della Svizzera dall'influenza di altri Stati" è stata adottata il 2 maggio 2023 dal Consiglio nazionale e sospesa il 3 luglio 2023 dalla Commissione per la politica di sicurezza del Consiglio degli Stati in attesa del rapporto del Consiglio federale in risposta al presente Postulato Pult 20.3984. Inoltre, entro la fine del 2024 il Consiglio federale adotterà un rapporto in risposta al postulato Z'graggen 22.4411 "Strategia per la sovranità digitale della Svizzera". Quest'ultimo definirà il concetto di "sovranità digitale", valuterà il grado di tale sovranità per la Svizzera e proporrà le misure necessarie in materia.

2 Infrastruttura svizzera di telecomunicazione

2.1 Una panoramica del 5G

Gli operatori di radiocomunicazione *Salt*, *Sunrise* e *Swisscom* gestiscono in Svizzera reti di telefonia mobile di quinta generazione (5G) tesa a fornire servizi di telecomunicazione. I produttori presso cui acquistano attrezzature 5G sono numerosi e di diversa provenienza: *Ericsson* (SE), *Nokia* (FIN) *Huawei* (CN), *Microsoft (eSPIN & Services*) (UK), *A10 Networks* (USA), *Cisco* (USA), *Juniper* (USA), *Commscope* (USA) e *Ceragon* (ISR).

La rete centrale (Core Network) è un elemento essenziale di una rete 5G e comprende le seguenti funzionalità principali: gestione dell'accesso e della sicurezza, autenticazione degli abbonati, instradamento delle chiamate e dei dati, gestione dei servizi agli abbonati, controllo e priorità dei flussi, gestione dell'interazione con altre reti, controllo della comunicazione durante tutta la durata della trasmissione garantendo la

continuità, in particolare quando gli utenti sono in movimento (handover), e gestione della qualità del servizio e della fatturazione. Un solo operatore segue una strategia multi-vendor per quanto riguarda la rete centrale. Gli altri due utilizzano esclusivamente apparecchiature di un unico fornitore, o solo *Huawei* o solo *Nokia*.

La rete d'accesso radio (Radio Access network, RAN) di una rete mobile collega i dispositivi degli utenti finali, come gli smartphone, alla nuvola informatica (cloud). Trasmette le informazioni via radio, prima dai dispositivi dell'utente finale ai ricetrasmettitori RAN, poi da questi alla rete centrale, a sua volta collegata a Internet o ad altri operatori. Le reti RAN svolgono compiti complessi di elaborazione delle connessioni e il loro sviluppo si basa sempre più sulla virtualizzazione delle loro funzioni. Per quanto riguarda le reti RAN utilizzate in Svizzera, un operatore utilizza esclusivamente apparecchiature *Huawei*, un altro per l'80% quelle di *Huawei* e per il 20% quelle di *Nokia* e l'ultimo utilizza quasi solo apparecchiature *Ericsson*[1].

Nelle reti di telefonia mobile, il termine "backhaul" si riferisce alla rete di trasmissione e ai collegamenti tra la rete centrale e le antenne relè della rete di accesso radio (RAN). I collegamenti che compongono una rete di backhaul possono essere in fibra ottica, in rame o in ponte radio. Presso il primo dei tre operatori questa rete di trasmissione è composta da apparecchiature di fornitori americani e di *Ericsson*, il secondo fa capo a *Huawei*, *Ericsson* e *Nokia*, mentre il terzo si rifornisce solo da *Huawei*.

Per quanto riguarda le interfacce con altri operatori o servizi (ad es. interconnessione con un altro operatore, operazioni di manutenzione, fatturazione, accesso a Internet), un operatore utilizza apparecchiature *Cisco* ed *Ericsson*, un altro quelle di *Cisco* e *Huawei* e l'ultimo esclusivamente apparecchiature *Huawei*.

Un'analisi globale delle apparecchiature utilizzate nelle reti 5G in Svizzera mostra che solo uno dei 3 operatori di telefonia mobile svizzeri è estremamente dipendente dal produttore cinese *Huawei*. Nella misura in cui uno degli altri operatori ricorre in parte ad apparecchiature *Huawei*, occorre notare che ogni elemento dell'infrastruttura 5G ha accesso a una parte significativa dell'infrastruttura complessiva, a differenza delle precedenti generazioni di telefonia mobile che separavano l'infrastruttura periferica da quella centrale. Ciò significa che qualsiasi vulnerabilità o backdoor in un'apparecchiatura 5G può potenzialmente compromettere l'intera rete 5G (cfr. sezione 2.2 sui rischi tecnici).

I centri operativi degli operatori sono infrastrutture centralizzate essenziali per le reti di telecomunicazione, la cui posizione geografica contribuisce a garantire la sicurezza delle reti 5G (cfr. sezione 4.1). Il Network Operation Center (NOC) monitora e gestisce le prestazioni e la disponibilità di una rete di telecomunicazioni, mentre il Security Operation Center (SOC) raccoglie, analizza e risponde alle allerte in materia di sicu-

[1] Per migliorare l'interoperabilità, è stata creata la Open RAN Alliance (O-RAN Alliance), il cui scopo è quello di garantire la futura interoperabilità dei vari componenti di una rete di telecomunicazione. Con la standardizzazione delle caratteristiche dei componenti hardware e software, lo standard Open RAN dovrebbe consentire di integrare in una rete mobile i componenti hardware e software di diversi produttori, senza che sia necessario effettuare delle modifiche.

rezza e agli incidenti informatici. Quest'ultimo utilizza strumenti avanzati di rilevamento delle minacce e di gestione degli eventi relativi alla sicurezza per identificare attività sospette, vulnerabilità e tentativi di intrusione o attacco.

2.2 Rischi tecnici con una componente geopolitica

A seguito della digitalizzazione, sempre più processi economici, sociali e politici sensibili per uno Stato sono gestiti da reti e sistemi digitali che possono essere vulnerabili agli attacchi informatici. Questi attacchi vengono eseguiti a livello professionale da attori statali, semi-statali o non statali che sfruttano le vulnerabilità e le lacune di sicurezza nei sistemi informatici e di telecomunicazione, oppure utilizzano software maligni (trojan, spyware e altri malware) o backdoor preinstallate per controllare o perturbare i sistemi colpiti.

Gli attacchi informatici comportano rischi geopolitici che possono avere conseguenze di vasta portata per un Paese come la Svizzera. In particolare, il collegamento in rete e la crescente complessità delle infrastrutture e dei sistemi digitali offrono agli autori di attacchi informatici la possibilità di piratare e sabotare il funzionamento delle infrastrutture sensibili o critiche come le reti energetiche, i servizi finanziari e le reti di approvvigionamento idrico, causando ripercussioni sia economiche che politiche sullo Stato, le imprese e i cittadini. Inoltre, molte risorse informatiche sono impiegate in tutto il mondo a fini di spionaggio. La Svizzera non viene risparmiata: il suo potenziale economico e scientifico, la presenza sul suo territorio di una grande quantità di organizzazioni internazionali e le numerose conferenze internazionali che ospita la rendono un territorio interessante per i servizi d'informazione stranieri[2].

La Svizzera ha già subito attacchi informatici contro le sue infrastrutture digitali, alcuni dei quali probabilmente condotti da Paesi stranieri, anche se la loro origine è rimasta incerta, in particolare contro l'azienda RUAG (2014-2016), il Dipartimento federale degli affari esteri DFAE (2017), il Laboratorio Spiez che tratta le minacce atomiche, biologiche e chimiche (2018), le Nazioni Unite (ONU) a Ginevra (2020) e, più recentemente, contro la rete aziendale delle FFS, l'Università di Zurigo e l'Amministrazione federale attraverso la società svizzera *Xplain* (2023). Nel giugno 2023, un attacco DDoS generale da parte del gruppo filorusso *NoName* in reazione al discorso del Presidente ucraino alle Camere federali ha colpito anche i siti web del Parlamento, dell'Amministrazione federale, della Posta, dell'Aeroporto di Ginevra, dell'Esercito svizzero, dei Cantoni e delle città svizzere.

Seguendo l'esempio del *Cloud Act* statunitense, una legge cinese approvata nel 2017 impone alle aziende cinesi di collaborare e condividere con i servizi d'informazione del proprio Paese l'accesso ai dati raccolti, anche per le loro operazioni all'estero. L'impresa *Huawei*, fondata nel 1987 da un ex ufficiale di alto rango dell'esercito cinese che ha beneficiato di un considerevole sostegno finanziario da parte dello Stato, è stata accusata dagli Stati Uniti di spionaggio per conto delle autorità cinesi. Sebbene non si abbiano prove concrete di attività di spionaggio o dell'installazione di bac-

[2] Rapporto del Consiglio federale del 12 maggio 2023 alle Camere federali e al pubblico: Valutazione annuale dello stato della minaccia, pag. 8.

kdoor da parte di *Huawei* nelle infrastrutture 5G, alcuni attacchi o backdoor rimangono difficili, se non impossibili da rilevare. È anche immaginabile che un fornitore installi in un secondo tempo aggiornamenti software deliberatamente modificati[3].

2.3 Rischi geopolitici veri e propri

Le crisi attuali (in particolare la pandemia COVID-19, la guerra in Ucraina, il cambiamento climatico, la crisi energetica, l'insicurezza economica e le tensioni in merito a Taiwan) evidenziano il crescente divario geopolitico a livello globale[4]. Questi divari hanno un impatto sullo sviluppo tecnologico e sull'innovazione e potrebbero ridurre la disponibilità di beni ad alta tecnologia. Le crescenti tensioni tra Cina e Stati Uniti nel campo della sicurezza nazionale e della tecnologia potrebbero causare interruzioni nelle catene di fornitura di beni strategici come le apparecchiature per le telecomunicazioni, minacciare l'interconnessione dei mercati e persino portare al loro disaccoppiamento. Con l'intensificarsi della competizione internazionale quanto all'influenza nel cyberspazio, è aumentato il rischio di ingerenze statali esercitate direttamente sui fornitori di apparecchiature[5].

La frattura con l'Occidente si riflette nel desiderio dichiarato da Paesi come la Cina, la Russia e da un numero crescente di Paesi del Sud globale di avere un maggiore influsso su un ordine mondiale percepito in modo troppo "occidentale", il che per la Svizzera rappresenta una sfida in termini di posizionamento politico ed economico. Ciò rischia di mettere a repentaglio i fattori di successo del nostro Paese, ovvero l'apertura al mondo del libero scambio e la capacità di innovazione, che dipende dall'accesso delle imprese svizzere a tutti i prodotti e servizi tecnologici d'avanguardia del mondo. L'approccio pragmatico della Svizzera in materia di politica estera deve aiutare a conciliare queste tensioni e a mantenere un approccio generale e non discriminatorio della Svizzera ai rischi di sicurezza associati alle infrastrutture digitali.

Se necessario, tuttavia, la Svizzera dovrebbe essere pronta a integrarsi maggiormente a livello internazionale, dato il suo sistema di valori basato sulla libertà e sullo Stato di diritto, e a rimanere parte integrante del sistema di innovazione dell'emisfero occidentale. Bisognerebbe evitare che in fatto di sicurezza, il nostro Paese sia considerato un anello debole al centro dell'Europa [6], che venga discriminato economicamente in caso utilizzasse determinate infrastrutture di rete provenienti dalla Cina o che quest'ultima possa sfruttare la potenziale dipendenza dalle sue infrastrutture

---

[3] Occorre rilevare che, *Huawei* implementa standard di sicurezza riconosciuti come il NESAS (Network Equipment Security Assurance Scheme), contribuisce al lavoro di sicurezza della GSMA (Global System for Mobile Communications Association) e offre a tutti i suoi clienti la possibilità di consultare il codice sorgente dei programmi, del sistema operativo o delle applicazioni presenti nei suoi componenti di rete.

[4] Sulla tendenza verso un mondo sempre più bipolare, cfr. Servizio delle attività informative della Confederazione SIC, La sicurezza della Svizzera 2023 del 26 giugno 2023, pag. 27 e segg.

[5] Rapporto del Consiglio federale del 24 novembre 2021 concernente la "Sicurezza dei prodotti e il supply chain risk management nei settori della cibersicurezza e della ciberdifesa", in risposta ai postulati Dobler 19.3135 e 19.3136, pag. 8.

[6] Nel suo rapporto del 9 giugno 2023 sullo stato attuale delle relazioni Svizzera-UE (pag. 11), il Consiglio federale sottolinea che l'UE è preoccupata per la crescente influenza tecnologica della Cina. Per evitare, o almeno ridurre, le dipendenze future, intende promuovere le capacità di sviluppo e di produzione nel mercato interno (sovranità tecnologica). Questo non ha ripercussioni sulle imprese e sui consumatori in Svizzera.

digitali per esercitare pressioni politiche sulla Svizzera. In definitiva, la Svizzera potrebbe essere costretta, in casi specifici, a scegliere se sostenere gli Stati Uniti o mantenere una posizione indipendente[7].

3 L'attuale regime giuridico e politico

3.1 Obblighi internazionali

L'Accordo generale sul commercio dei servizi (GATS)[8] disciplina il commercio internazionale dei servizi, compresi quelli di telecomunicazione. Il GATS è completato da regole vincolanti contenute nell'allegato sulle telecomunicazioni e il Quarto Protocollo relativo all'allegato concernente i negoziati sulle telecomunicazioni, che contiene gli impegni specifici di ciascuno Stato membro (cfr. artt. XVI e XXIX del GATS). Oltre al fatto che la Svizzera, sulla base di questi diversi accordi, si sia impegnata a liberalizzare il proprio mercato delle telecomunicazioni, essa è tenuta a garantire ai fornitori di servizi e ai servizi di qualsiasi membro dell'OMC un trattamento non discriminatorio (clausola della nazione più favorita).

L'Accordo generale sulle tariffe doganali e il commercio (GATT)[9] liberalizza il commercio delle merci sulla base di liste di concessioni di ogni membro e si applica, se del caso, agli impianti e alle apparecchiature di telecomunicazione. Il GATT è completato dall'Accordo sugli ostacoli tecnici agli scambi (OTC)[10] che definisce un quadro multilaterale teso a garantire che le prescrizioni tecniche, gli standard e le procedure di valutazione della conformità non siano discriminatori e non ostacolino inutilmente il commercio. L'accordo OTC riconosce il diritto di emanare prescrizioni tecniche volte a definire un livello adeguato di protezione degli obiettivi legittimi, come la sicurezza nazionale, nel rispetto dei principi di non discriminazione, proporzionalità e trasparenza.

Le restrizioni o le esclusioni di accesso al mercato svizzero per i produttori di apparecchiature ritenuti problematici per la sicurezza del nostro Paese o di proprietà, sotto il controllo o l'influenza di uno Stato straniero che rappresenta un rischio per la sicurezza, possono violare gli obblighi GATS, GATT e OTC della Svizzera. Il GATS e il GATT contengono clausole d'eccezione che in determinate condizioni consentono di giustificare le misure necessarie per proteggere l'ordine pubblico (art. XIV lett. a GATS) o della sicurezza (artt. XIV lett. c iii e XIVbis GATS, art. XXI GATT)[11]. Queste eccezioni sono interpretate in modo severo dagli organi decisionali dell'OMC. L'Accordo OTC ammette anche considerazioni relative alla sicurezza nazionale (articoli 2.10, 5.4 e 5.7 OTC). Molti Paesi occidentali e dell'UE hanno già adottato misure di

[7] Cancelleria federale, Svizzera 2035: 20 domande per rispondere alle sfide del futuro - analisi della situazione e del contesto 2022, pagg. 69 e 72.
[8] Il GATS fa parte dell'Accordo del 15 aprile 1994 che istituisce l'Organizzazione mondiale del commercio (OMC) (allegato 1.B; RS 0.632.20).
[9] Il GATT (General Agreement on Tariffs and Trade) fa parte dell'Accordo del 15 aprile 1994 che istituisce l'OMC (allegato 1.B; RS 0.632.20).
[10] L'OTC fa parte dell'Accordo del 15 aprile 1994 che istituisce l'OMC (allegato 1A.6; RS 0.632.20).
[11] L'art. 5 lett. e dell'allegato sulle telecomunicazioni completa queste garanzie prevedendo che l'accesso e l'uso delle reti e dei servizi pubblici di trasporto dell'informazione possano essere soggetti alle condizioni necessarie per proteggere l'integrità tecnica di tali servizi e reti.

questo tipo nei confronti di fornitori ritenuti problematici (cfr. sezione 3.6), presumibilmente in conformità con gli accordi GATS, GATT e OTC che hanno sottoscritto.

Poiché il diritto della neutralità definisce i diritti e gli obblighi di uno Stato neutrale in caso di conflitto armato internazionale[12], esso non si applica alle eventuali misure vincolanti che la Svizzera potrebbe adottare in relazione all'acquisizione e allo sviluppo di infrastrutture digitali e di telecomunicazione come il 5G.

3.2 Diritto delle telecomunicazioni e sicurezza delle reti

Il diritto delle telecomunicazioni organizza la fornitura di servizi e impianti di telecomunicazione sottoponendola alla concorrenza in conformità con gli impegni internazionali assunti dalla Svizzera nell'ambito dell'Organizzazione mondiale del commercio (OMC; cfr. sezione 3.1). Questo diritto non conferisce attualmente alla Confederazione alcuna influenza sull'acquisto di apparecchiature di rete da parte degli operatori, che sono liberi di fare le proprie scelte.

In conformità al segreto delle telecomunicazioni (art. 13 cpv. 2 Cost. e art. 43 LTC), gli operatori devono garantire la riservatezza e l'integrità delle informazioni affidate loro dagli utenti per la trasmissione tramite telecomunicazioni. Ciò obbliga gli operatori a proteggere le proprie infrastrutture da accessi non autorizzati e altri attacchi informatici. I dettagli di questo obbligo non sono specificati nel diritto delle telecomunicazioni in quanto gli operatori devono adottare misure tecnicamente fattibili in condizioni ragionevoli tenendo conto dei rischi per la sicurezza.

Sulla base del nuovo articolo 48*a* LTC adottato nel 2021, il Consiglio federale ha ripreso nell'ordinanza sui servizi di telecomunicazione (OST) una serie di misure tese a rafforzare la sicurezza delle reti di telecomunicazione. Il sistema di notifica delle interruzioni delle operazioni di telecomunicazione è stato consolidato e i fornitori di servizi Internet devono combattere gli attacchi DDoS (Distributed Denial of Service) e possono bloccare o limitare l'accesso a Internet o gli elementi di indirizzo che minacciano di compromettere il corretto funzionamento degli impianti di telecomunicazione. Devono inoltre gestire un servizio specializzato che raccolga le segnalazioni di tali manipolazioni.

Per quanto riguarda la sicurezza delle reti 5G, gli operatori sono tenuti ad allestire un sistema di gestione della sicurezza delle informazioni (SGSI) in conformità agli standard riconosciuti e ai requisiti dell'UFCOM. Devono inoltre gestire i loro centri operativi di rete (NOC) e i centri di gestione della sicurezza (SOC) esclusivamente in Paesi la cui legislazione garantisca un'adeguata protezione dei dati. Le attuali basi legali non consentono tuttavia di imporre una gestione unicamente sul suolo svizzero.

Gli operatori delle reti 5G devono infine assicurare che gli impianti di telecomunicazione critici sul piano della sicurezza da loro esercitati corrispondano all'attuale stato della tecnica. L'UFCOM può definire gli impianti critici per la sicurezza, se necessario,

[12] La neutralità permanente è uno strumento della politica estera svizzera (art. 173 cpv. 1 lett. a e 185 cpv. 1 Cost.; RS 101). Il diritto della neutralità è codificato nelle Convenzioni dell'Aia del 18 ottobre 1907 (RS 0.515.21 e 0.515.22) e fa parte del diritto internazionale consuetudinario.

in collaborazione con il settore. Questo obbligo implica l'allestimento di una procedura di certificazione o di valutazione della conformità per le apparecchiature critiche delle reti mobili (cfr. sezione 4.3). Date le dimensioni del mercato europeo e gli accordi di reciproco riconoscimento con l'UE sulle apparecchiature di telecomunicazione, sarebbe opportuno armonizzare le normative svizzere con quelle dell'UE. L'agenzia per la sicurezza informatica dell'UE (ENISA) sta preparando uno schema di certificazione della sicurezza informatica 5G in seguito all'adozione del toolbox 5G. Bisognerebbe esaminare la possibilità per la Svizzera di utilizzare questo schema di certificazione, che andrebbe basato su standard riconosciuti, e di formalizzare la cooperazione con questa agenzia.

3.3 Resilienza delle infrastrutture critiche

La legge federale sulla sicurezza delle informazioni in seno alla Confederazione (LSIn; RS 128) mira a garantire la sicurezza del trattamento delle informazioni di competenza della Confederazione e la sicurezza delle sue risorse informatiche. In particolare, prevede una valutazione del rischio per le aziende che eseguono mandati pubblici sensibili per la sicurezza della Confederazione[13]. Questa legge, che non è ancora entrata in vigore, deve essere modificata per rafforzare la resilienza della Svizzera a fronte dei ciber-rischi. I compiti e le competenze del futuro Ufficio federale per la cibersicurezza (UFCS) saranno sanciti per legge e sarà introdotto l'obbligo di segnalare gli attacchi informatici alle infrastrutture critiche come processi e sistemi essenziali per il funzionamento dell'economia e il benessere della popolazione.

Sebbene l'Ufficio federale per l'approvvigionamento economico del Paese (UFAE) abbia pubblicato uno standard minimo per la protezione delle TIC dai rischi informatici, la futura LSIn non richiede che le infrastrutture critiche siano conformi a questo standard. L'Amministrazione federale ne tiene invece conto poiché deve provvedere affinché i suoi organi e i suoi sistemi presentino un'adeguata resilienza ai ciber-rischi (art. 6 LSIn). L'UFCS dovrà fornire anche un supporto sussidiario ai gestori di infrastrutture critiche (art. 74 LSIn). Se reti e sistemi informatici ubicati all'estero sono utilizzati per attacchi a infrastrutture critiche in Svizzera, il Servizio delle attività informative della Confederazione (SIC) può cercare di infiltrarvisi per perturbare, impedire o rallentare l'accesso alle informazioni (art. 37 cpv. 1 della legge federale sulle attività informative; RS 121).

Il progetto LSIn e la nuova Strategia nazionale per la protezione delle infrastrutture critiche adottata dal Consiglio federale il 16 giugno 2023[14] concretizzano la Ciberstrategia nazionale (CSN) dettando misure tese a rafforzare la resilienza delle infrastrutture critiche digitali. Per il resto, spetta al Consiglio federale verificare quali settori debbano essere regolamentati e proporre al Parlamento, se necessario e se di competenza della Confederazione, modelli di direttive vincolanti per l'applicazione degli standard nelle infrastrutture critiche.

---

[13] Lo scopo di questa valutazione è di escludere le aziende che danno luogo a un alto grado di probabilità di eseguire i contratti in modo inadeguato o in violazione delle norme di sicurezza. Ciò può avvenire se l'azienda è controllata o influenzata da Stati esteri in modo incompatibile con gli interessi svizzeri (art. 57 cpv. 2 lett. b LSIn).

[14] FF **2023** 1659

Il protocollo SCION (Scalability, Control, and Isolation on Next-Generation Networks), sviluppato dal Politecnico federale di Zurigo (ETHZ), è un ottimo esempio di ciò che si può prevedere per proteggere le infrastrutture critiche. Consente di creare una nuova architettura Internet che offre le proprietà delle reti chiuse e private sull'infrastruttura Internet pubblica. SCION aumenta la sicurezza di Internet consentendo al mittente di selezionare i percorsi di trasmissione e quindi di controllare il flusso delle informazioni. Dal giugno 2022, la Banca nazionale svizzera (BNS) utilizza SCION nell'ambito della Secure Swiss Finance Network (SSFN), come pure il gestore della borsa svizzera SIX Group, gli operatori Swisscom e Sunrise oltre a SWITCH, che gestisce il dominio Internet ".ch".

3.4 Protezione degli impianti di telecomunicazione e di altri prodotti TIC

Per minimizzare i ciber-rischi occorre mettere in sicurezza apparecchiature, impianti di telecomunicazione e altri prodotti TIC, che presentano ancora molte lacune in termini di riservatezza, integrità, disponibilità e tracciabilità dei dati. A questo proposito, l'adozione e l'applicazione di standard di sicurezza per le apparecchiature, gli impianti e i prodotti TIC, e la loro certificazione o valutazione di conformità da parte di organismi riconosciuti, contribuiscono a migliorarne la sicurezza e a integrarli correttamente nelle infrastrutture digitali.

Le disposizioni introdotte nel 2022 nell'ordinanza dell'UFCOM sugli impianti di telecomunicazione (OOIT; RS 784.101.21) rafforzano la sicurezza in rete di alcuni dispositivi senza filo (smartphone, orologi connessi, tracker di attività e giocattoli senza filo) acquistabili sul mercato svizzero. Questi ultimi devono avere funzionalità che impediscano loro di danneggiare le reti di comunicazione contribuendo quindi a renderle più resilienti. Le disposizioni dell'OOIT riguardano anche le installazioni di reti 5G. Hanno consentito alla Svizzera di allineare la propria legislazione a quella dell'UE (cfr. sezione 3.6). Per facilitare la valutazione della conformità dei prodotti e la loro immissione sul mercato, gli organismi di standardizzazione europei stanno attualmente sviluppando norme armonizzate che dovrebbero essere disponibili per l'industria europea e svizzera.

Sarebbe auspicabile che la legislazione svizzera prendesse in considerazione, ad esempio nella legge federale sugli ostacoli tecnici al commercio (LOTC; RS 946.51) o nella LSIn (cfr. sezione 3.3), le questioni di cibersicurezza dei prodotti con componenti digitali critici, stabilendo requisiti per i loro produttori sulla scia del progetto UE sulla ciber-resilienza (sezione 3.6).

3.5 Strategia nazionale per la protezione della Svizzera contro i ciber-rischi

Conformemente all'orientamento strategico per la legislatura 2023-2027, la Confederazione anticipa i ciber-rischi, sostiene e adotta misure efficaci per proteggere la popolazione, l'economia e le infrastrutture critiche[15]. Questa direzione strategica è stata

[15] Consiglio federale, Indirizzi politici e obiettivi per il programma di legislatura 2023-2027, 11 gennaio 2023, obiettivo 18.

concretizzata nella CSN dell'aprile 2023[16], che mira a proteggere la Svizzera contro le minacce informatiche.

La CSN descrive in dettaglio le principali minacce informatiche che sono fonte di rischi geopolitici, come lo spionaggio informatico, il sabotaggio informatico, la sovversione informatica volta a minare il sistema politico di uno Stato e le operazioni informatiche nel contesto di un conflitto armato (cfr. sezione 2.2). Sottolinea che l'evoluzione della minaccia informatica dipende in larga misura dai cambiamenti geopolitici e dalle innovazioni tecnologiche e che possiamo aspettarci crescenti tensioni tra i principali Paesi produttori di hardware e software per computer. La CSN si fonda su un approccio globale basato sul rischio e volto a migliorare la resilienza della Svizzera alle minacce informatiche. Secondo la CSN, è importante verificare in quali settori sia necessaria una legislazione che stabilisce standard o regolamenti da rispettare, questione trattata nel presente rapporto.

3.6 Misure adottate all'estero

Nel maggio 2019, gli Stati Uniti hanno bandito dai propri sistemi di telecomunicazione i prodotti e i servizi delle aziende cinesi *Huawei* e *ZTE*. Il divieto è stato esteso nel 2022 a tutti i prodotti cinesi per le telecomunicazioni e la videosorveglianza. Non è dovuto solo al sospetto di spionaggio ma anche a considerazioni legate al dominio del mercato della tecnologia 5G esercitato dalle aziende cinesi e al ritardo accumulato dalle aziende americane in questo settore. Altri Paesi del mondo, in particolare Canada, Regno Unito, Giappone e Australia, hanno imboccato la stessa via.

Dal canto loro, gli Stati membri dell'UE hanno definito un approccio globale ai rischi associati alle reti 5G sotto forma di un toolbox adottato nel gennaio 2020[17]. Le misure proposte mirano a rafforzare i requisiti di sicurezza, a valutare i profili di rischio dei fornitori di apparecchiature, ad applicare restrizioni efficaci ai fornitori considerati ad alto rischio, compresa la loro esclusione, e a mettere in atto strategie per garantire la diversificazione dei fornitori di apparecchiature. Mentre la maggior parte degli Stati membri dell'UE ha adottato una legislazione che limita e/o proibisce di ricorrere a fornitori ad alto rischio per l'allestimento dell'infrastruttura 5G nazionale o delle relative parti critiche, come le funzioni della rete centrale, solo alcuni di essi hanno effettivamente attuato queste prerogative per limitare o escludere i fornitori ad alto rischio. La Commissione europea ritiene che *Huawei* e *ZTE* presentino rischi significativamente più elevati rispetto ad altri fornitori 5G e considera che le restrizioni e le esclusioni applicate nei loro confronti da 10 Stati membri siano giustificate in base al toolbox 5G. Incoraggia dunque vivamente gli altri Stati membri e gli operatori di telecomunicazioni ad adottare tali misure in considerazione del rischio per la sicurezza collettiva dell'Unione[18].

---

[16] https://www.admin.ch/gov/it/pagina-iniziale/documentazione/comunicati-stampa.msg-id-94237.html

[17] 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).

[18] Comunicazione del 15 giugno 2023 (https://digital-strategy.ec.europa.eu/en/library/communication-commission-implementation-5g-cybersecurity-toolbox).

La Direttiva 2014/53/UE sulle apparecchiature radio (RED), alla quale la Svizzera si è allineata (cfr. sezione 3.4), stabilisce un quadro normativo per l'immissione sul mercato di apparecchiature radio che comprende requisiti tecnici per la protezione della sfera privata, dei dati personali e contro le frodi. L'UE ha inoltre presentato una proposta di regolamento sulla resilienza informatica[19], che stabilisce degli obblighi per i fabbricanti di prodotti con componenti digitali. Questi obblighi riguardano in particolare la progettazione, lo sviluppo e la produzione di detti prodotti, la gestione del loro ciclo di vita e la segnalazione delle vulnerabilità. Gli Stati Uniti impongono ai fornitori la trasparenza sui componenti software venduti al governo (Software Bill of Materials) sulla base di un "executive order" del maggio 2021 teso a migliorare la sicurezza informatica.

3.7 Sintesi dell'attuale regime giuridico e politico

Sebbene la Svizzera stia già adottando alcune misure per proteggere la propria infrastruttura digitale, permangono rischi per la sicurezza in relazione all'infrastruttura di telecomunicazione, tramite cui è possibile attaccare o sabotare le infrastrutture critiche e ricattare il nostro Paese sul piano economico e politico (cfr. cap. 2.2). Visti i rischi geopolitici che ciò comporta per la Svizzera, è opportuno rafforzare i mezzi di lotta contro i rischi tecnici in un approccio generale e non discriminatorio.

Nell'attuale contesto geopolitico diviso, vi è il rischio che il nostro Paese sia visto come una falla di sicurezza nel cuore dell'Europa e che venga discriminato economicamente se utilizza determinate infrastrutture digitali o di rete, o che sia addirittura soggetto a pressioni politiche se è potenzialmente dipendente da uno o più fornitori di apparecchiature particolari (cfr. sezione 2.3). In tali circostanze, è essenziale che la LTC tenga conto di questi rischi geopolitici.

4 Potenziali misure da considerare

4.1 Rafforzare la lotta contro i rischi tecnici

In considerazione dei rischi tecnici con una componente geopolitica (cfr. sezione 2.2 e 3.7), occorre precisare e ampliare nella LTC le competenze del Consiglio federale che consentono di definire nuovi strumenti e le esigenze necessarie a rafforzare la sicurezza delle infrastrutture di telecomunicazione, in analogia a quanto previsto dall'UE nel toolbox 5G e in altri progetti di regolamentazione, in particolare sulla resilienza informatica, ossia:

- Obbligare gli operatori di telecomunicazione ad acquistare e utilizzare apparecchiature, strutture e software che necessitano per fornire servizi di telecomunicazione, provenienti da diversi fornitori (strategia multi-vendor);
- Estendere i requisiti di sicurezza previsti dall'OST alle reti 5G (cfr. sezione 3.2) e a tutte le reti di telecomunicazione, in particolare l'obbligo di garantire che le apparecchiature, gli impianti e i software critici per la sicurezza corrispondano

[19] Proposta di regolamento del Parlamento europeo e del Consiglio relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali e che modifica il regolamento (UE) 2019/1020 [COM(2022) 454 final — 2022/0272(COD)]

allo stato della tecnica e siano soggetti ad adeguate procedure di certificazione in materia di cibersicurezza;
- Prevedere vincoli aggiuntivi per queste apparecchiature, questi impianti e software ritenuti a rischio;
- Stabilire requisiti di sicurezza più severi per l'acquisizione e l'esercizio di apparecchiature, impianti e software in vista del prossimo bando per le frequenze di radiocomunicazione (concessioni) nel 2028;
- Analizzare la possibilità di imporre, a condizione che gli obblighi internazionali della Svizzera lo consentano, ai NOC e ai SOC l'obbligo di stabilirsi in Svizzera, i quali dovrebbero essere gestiti dall'operatore stesso o da un mandatario indipendente dai fornitori di apparecchiature.

L'attuazione di questi nuovi requisiti, che in ultima analisi miglioreranno la sicurezza delle nostre infrastrutture di telecomunicazione, richiede la creazione di capacità di certificazione e di controllo tecnico in Svizzera (cfr. sezione 4.3) e l'introduzione di una vigilanza rafforzata da parte dell'UFCOM.

Visti i costi tecnologici e il livello di innovazione richiesti per lo sviluppo di infrastrutture digitali, sarebbe irrealistico prevedere una politica industriale che ci consentirebbe di ridurre la dipendenza tecnologica del nostro Paese dai fornitori stranieri di apparecchiature. D'altra parte, non si può escludere che in Svizzera possano nascere soluzioni di sicurezza specifiche in relazione a impianti, software o prestazioni legate ai servizi di telecomunicazione. In questo contesto, sarebbe opportuno che la ricerca e lo sviluppo di soluzioni di sicurezza svizzere, sulla scia del protocollo SCION sviluppato dall'PFZ (cfr. sezione 3.3), possano essere sostenuti dagli appositi strumenti di finanziamento esistenti (Fondo nazionale svizzero, Innosuisse).

4.2 Anticipare i rischi geopolitici

Considerati i potenziali rischi geopolitici cui la Svizzera è esposta (cfr. sezione 2.3 e 3.7), essa dovrebbe disporre, se necessario, degli strumenti legali per affrontarli prontamente, sebbene si debba continuare a privilegiare, per quanto possibile, un approccio generale e non discriminatorio ai rischi per la sicurezza (cfr. cap. 4.1). La LTC deve quindi includere una nuova disposizione che conferisce al Consiglio federale la possibilità di adottare, conformemente agli obblighi internazionali della Svizzera, le misure necessarie quando si concretizza un potenziale rischio geopolitico. In definitiva, si tratta di mettere il nostro Paese in condizione di agire rapidamente, se necessario attraverso il Consiglio federale, per salvaguardare i suoi interessi e preservare la sua sicurezza interna ed esterna e la sua indipendenza.

Il Consiglio federale dovrebbe pertanto avere la facoltà, nell'ambito della LTC, di adottare per via di ordinanza le seguenti potenziali misure di salvaguardia volte a rafforzare la sicurezza delle infrastrutture digitali e di telecomunicazione, in linea con quanto previsto dall'UE nel toolbox 5G e dai Paesi membri nelle loro legislazioni:

- Obbligare gli operatori di telecomunicazioni ad acquistare, installare e gestire apparecchiature, impianti e software tesi a fornire servizi di telecomunicazione, solo presso specifici fornitori o categorie di fornitori di apparecchiature;
- Limitare, sospendere o vietare l'acquisto, l'installazione e l'esercizio di apparecchiature, impianti e software tesi a fornire servizi di telecomunicazione,

da parte di fornitori di apparecchiature ritenuti problematici per la sicurezza del nostro Paese o che sono di proprietà, sotto il controllo o l'influenza di uno Stato estero che presenta un rischio geopolitico per la Svizzera;
- Obbligare gli operatori a rimuovere dalle loro infrastrutture le apparecchiature, le installazioni e i software legati all'offerta di servizi di telecomunicazione, provenienti da fornitori di apparecchiature ritenuti problematici per la sicurezza del nostro Paese o che sono di proprietà, sotto il controllo o l'influenza di uno Stato straniero che rappresenta un rischio geopolitico per la Svizzera.

L'adozione delle misure previste potrebbe avere notevoli conseguenze economiche per gli operatori interessati, nonché importanti ripercussioni operative sulle loro reti e sui loro servizi di telecomunicazione. Dovrebbe quindi essere attuata con prudenza, rispettando i diritti fondamentali delle imprese interessate, e soggetta a periodi di attuazione sufficientemente lunghi.

4.3 Sviluppare le capacità di audit e certificazione tecniche

La messa in sicurezza delle infrastrutture digitali, delle apparecchiature e degli impianti di telecomunicazione e dei prodotti TIC avviene tramite la loro certificazione o la valutazione della loro conformità in termini di sicurezza (cfr. cap. 3.2, e 3.4). Ciò richiede capacità, attrezzature e competenze di cui la Svizzera dispone ampiamente nelle sue università, nel suo settore pubblico e nelle sue imprese.

In Svizzera si stanno sviluppando capacità di audit e certificazione, come dimostrano da un lato la recente creazione dell'NCSC, che dispone di competenze all'avanguardia nel campo della cibersicurezza, e dall'altro la crescita esponenziale dell'offerta privata di servizi di analisi delle vulnerabilità e di test d'intrusione[20]. Il Cyber-Defence Campus (CYD Campus) di armasuisse lavora inoltre a stretto contatto con le università e gli ambienti economici per creare un monitoraggio tecnologico incentrato sulla cibersicurezza, mentre le Accademie svizzere delle scienze sono incaricate di valutare le opportunità e i rischi delle nuove tecnologie.

Questo ecosistema svizzero della sicurezza in rete dovrebbe essere in grado di fornire alla Svizzera gli organismi di controllo e certificazione nazionali indipendenti di cui ha bisogno per valutare la sicurezza a livello di software e hardware delle sue infrastrutture digitali, delle apparecchiature di telecomunicazione e dei prodotti TIC. Allo stesso tempo, la Svizzera dovrebbe creare accordi internazionali volti a riconoscere le certificazioni tecniche, in particolare nell'ambito dell'accordo tra la Svizzera e l'UE sul reciproco riconoscimento (ARR CH-UE; RS 0.946.526.81.

[20] Un esempio è il National Test Institute for Cybersecurity (NTC) con sede a Zugo, che verifica l'affidabilità e la sicurezza dei prodotti connessi e delle applicazioni digitali. I test sono stati avviati in collaborazione con il settore, le aziende di sicurezza informatica e le università e si basano sugli attuali standard internazionali. L'NTC ha verificato il certificato COVID-19 nel giugno 2021 e l'applicazione cinese "TikTok" nell'aprile 2023 per conto dell'NCSC.

4.4 Rafforzare la cooperazione internazionale

La collaborazione internazionale è essenziale per garantire la sicurezza delle reti e delle infrastrutture digitali, data la loro interconnessione globale. In linea con la Strategia di politica estera digitale 2021-2024[21], la Svizzera intende rafforzare la sicurezza informatica promuovendo l'attuazione pratica di norme di diritto internazionale[22]. È coinvolta nei negoziati per la stesura di una convenzione delle Nazioni Unite (ONU) sulla criminalità informatica, sta negoziando un aggiornamento dell'agenda globale sulla sicurezza informatica dell'Unione internazionale delle telecomunicazioni (UIT), partecipa attivamente all'attuazione delle misure dell'Organizzazione per la sicurezza e la cooperazione in Europa (OCSE) tese a rafforzare la fiducia nel campo della sicurezza informatica, sostiene inoltre una serie di iniziative internazionali volte a mantenere un ciberspazio aperto, libero e sicuro[23]. Il contributo della Svizzera nella regolamentazione internazionale coinvolge anche la "Ginevra internazionale", che è una piattaforma essenziale per i dibattiti sulla cibersicurezza a livello globale.

I governi non possono garantire da soli la sicurezza dello spazio digitale, gli attori del settore privato svolgono infatti un ruolo decisivo con i loro standard, prodotti e servizi globali. Per questo motivo la Svizzera sostiene un approccio multi-stakeholder e incoraggia il dialogo con le imprese. Molto importanti sono anche la collaborazione con iniziative private internazionali e i centri di competenza tecnica sulla cibersicurezza (in particolare FIRST, TF-CSIRT, NatCSIRT), così come la partecipazione alla standardizzazione delle reti di telecomunicazione all'interno di varie organizzazioni (UIT, ETSI, 3GPP, ecc.) in collaborazione con i fornitori di apparecchiature.

5 Conclusione

In linea con l'orientamento strategico per la legislatura 2023-2027, la Confederazione deve anticipare i ciber-rischi e adottare misure efficaci per proteggere la popolazione, l'economia e le infrastrutture critiche. La Strategia nazionale 2023 per la protezione delle infrastrutture critiche e la Strategia nazionale per la protezione della Svizzera contro i ciber-rischi 2023 riprendono questo approccio preventivo, incaricando al contempo il Consiglio federale di analizzare i rischi e le vulnerabilità informatiche e di proporre le norme necessarie in considerazione delle necessità e delle lacune legali.

Considerati i rischi tecnici con una componente geopolitica che la Svizzera deve affrontare in relazione alle sue infrastrutture di telecomunicazione e digitali, il Consiglio federale è convinto che sia necessario rafforzare i mezzi per combattere questi rischi e propone pertanto misure basate sulla LTC (strategia multi-vendor, vincoli per gli impianti considerati a rischio, requisiti di sicurezza più severi per la prossima asta delle frequenze). Per il resto, l'ecosistema svizzero relativo alla cibersicurezza dovrebbe

---

[21] Rapporto del Consiglio federale del 4 novembre 2020, Strategia di politica estera digitale 2021-2024, in risposta al postulato 17.3789.
[22] A questo proposito va menzionato il coinvolgimento attivo della Svizzera nell'"Open-Ended Working Group on Developments in the Field of ICTs in the Context of International Security" (UN OEWG) su mandato dell'Assemblea generale dell'ONU.
[23] In particolare, la Svizzera sponsorizza un programma delle Nazioni Unite per incoraggiare un comportamento responsabile degli Stati nel ciberspazio e partecipa alla *Counter Ransomware Initiative*.

essere in grado di fornire gli organismi nazionali di controllo e certificazione di cui il nostro Paese ha bisogno.

Seguendo l'esempio di quanto previsto dall'UE nel suo toolbox 5G e in altri progetti normativi, in particolare sulla ciber-resilienza, il Consiglio federale ritiene necessario inserire nella LTC una nuova disposizione che gli dia la possibilità di adottare, conformemente agli obblighi internazionali della Svizzera, le misure necessarie quando si concretizza un tale rischio geopolitico. Si tratterebbe in particolare di vietare, se necessario, l'acquisto, l'installazione e l'esercizio di apparecchiature di fornitori ritenuti problematici per la sicurezza della Svizzera o che sono di proprietà, sotto il controllo o l'influenza di uno Stato estero che rappresenta un rischio geopolitico per la Svizzera. A tale proposito, la libertà economica e il corretto funzionamento della concorrenza devono essere garantiti nella misura del possibile.

Infine, la Svizzera deve continuare a impegnarsi nella collaborazione internazionale, essenziale per garantire la sicurezza delle reti e delle infrastrutture digitali, data la loro interconnessione su scala mondiale.