COMMISSIONE
EUROPEA

Bruxelles, 29.1.2020
COM(2020) 50 final

COMUNICAZIONE DELLA COMMISSIONE AL PARLAMENTO EUROPEO, AL CONSIGLIO, AL COMITATO ECONOMICO E SOCIALE EUROPEO E AL COMITATO DELLE REGIONI

Dispiegamento del 5G sicuro - Attuazione del pacchetto di strumenti dell'UE

1. *Introduzione*

La quinta generazione (5G) delle reti di telecomunicazione è destinata a svolgere un ruolo essenziale nello sviluppo della società e dell'economia europee e si prevede che offrirà ampie opportunità economiche e costituirà una base importante per le trasformazioni digitale e verde in settori quali i trasporti, l'energia, l'industria manifatturiera, la sanità, l'agricoltura e i media.

Il 5G potrebbe pertanto avere un impatto su quasi tutti gli aspetti della vita dei cittadini dell'UE. La cibersicurezza delle reti 5G è quindi essenziale non solo per proteggere le nostre economie, società e processi democratici, ma anche per garantire la fiducia in una trasformazione digitale che vada a vantaggio di tutti i cittadini dell'UE.

Poiché molti servizi essenziali dipenderanno dalle reti 5G, le conseguenze di perturbazioni sistemiche e generalizzate di tali reti potrebbero essere particolarmente gravi e, data la natura interconnessa degli ecosistemi digitali, avere un impatto significativo anche al di là dei confini nazionali. Di conseguenza, garantire la cibersicurezza delle reti 5G è una questione di importanza strategica per l'Unione, in un momento in cui gli attacchi informatici sono in aumento, più sofisticati che mai e ad opera di un'ampia gamma di soggetti, in particolare attori statali o soggetti sostenuti da governi di paesi terzi. Per quanto riguarda la sicurezza delle infrastrutture critiche come il 5G, si è scelto di definire, per la prima volta, un approccio comune europeo. Tale approccio rispetta pienamente l'apertura del mercato interno dell'UE, a condizione che siano rispettati i requisiti di sicurezza dell'UE basati sul rischio.

Il 22 marzo 2019 il Consiglio europeo ha chiesto un approccio concertato alla sicurezza delle reti 5G. Il 26 marzo 2019 la Commissione ha adottato la raccomandazione (UE) 2019/534 sulla cibersicurezza delle reti 5G[1]. In tale raccomandazione gli Stati membri sono stati invitati a completare le valutazioni nazionali dei rischi e a rivedere le misure nazionali, per collaborare a una valutazione coordinata dei rischi a livello dell'UE e a un pacchetto di strumenti comprendente possibili misure di attenuazione comuni. La presente comunicazione costituisce parte integrante della strategia digitale europea globale della Commissione, come richiesto dal Consiglio europeo.

2. *Lancio del 5G nell'UE*

Il dispiegamento in Europa dell'infrastruttura di rete 5G è fondamentale per la strategia e per la competitività dell'industria europea. La Commissione ha riconosciuto che il dispiegamento delle tecnologie di rete 5G costituisce un fattore abilitante fondamentale per i futuri servizi digitali. Nel 2016 la Commissione ha adottato il piano d'azione per il 5G volto a garantire che l'Unione disponga delle infrastrutture di connettività necessarie per la sua trasformazione digitale a partire dal 2020 e per il dispiegamento completo nelle aree urbane e lungo i principali assi di trasporto entro il 2025[2]. La comunicazione relativa alla società dei Gigabit fissa l'obiettivo ambizioso di garantire che sia possibile accedere ovunque alla connettività mobile dei dati[3], anche nelle zone rurali e periferiche.

[1] Raccomandazione (UE) 2019/534 - Cibersicurezza delle reti 5G (GU L 88 del 29.3.2019, pag. 42).
[2] COM(2016) 588 final - Il 5G per l'Europa: un piano d'azione.
[3] COM(2016) 587 final - Connettività per un mercato unico digitale competitivo: verso una società dei Gigabit europea.

Per quanto riguarda l'assegnazione delle frequenze, gli Stati membri hanno assegnato il 16 % delle bande pioniere 5G[4]. Nei prossimi mesi sono previste consultazioni per una serie di procedure di assegnazione, in vista dell'obbligo giuridico di consentire l'uso di tutte le bande pioniere 5G entro la fine dell'anno.

L'Europa è una delle regioni più avanzate del mondo per quanto riguarda il lancio commerciale dei servizi 5G[5]. Attualmente si prevede che i primi servizi 5G saranno disponibili in 138 città europee entro la fine del 2020. Le prime reti 5G sono basate sull'attuale 4ª generazione (4G) di tecnologie di rete e i servizi 5G sono destinati principalmente al grande pubblico, sia come miglioramento rispetto al 4G in termini di capacità e velocità sia come alternativa, senza fili ed efficiente sotto il profilo dei costi, alle reti fisse[6].

Per quanto riguarda le opportunità dei nuovi servizi destinati alle imprese (*business-to-business*), ad esempio nei settori dell'energia, dell'alimentazione e dell'agricoltura, dell'assistenza sanitaria, dell'industria manifatturiera o dei trasporti, l'Europa si trova già in una posizione avanzata con un investimento dell'ordine di 1 miliardo di EUR, di cui 300 milioni di EUR di finanziamenti dell'UE nel contesto del partenariato pubblico-privato per il 5G nell'ambito di Orizzonte 2020. Tale investimento comprende oltre 160 sperimentazioni del 5G su larga scala individuate in Europa, di cui dieci corridoi autostradali transfrontalieri per la sperimentazione su larga scala di servizi di mobilità connessa e automatizzata basati sul 5G. Le sperimentazioni comprendono le applicazioni abilitate al 5G in settori che vanno da assistenza sanitaria sostenibile, mobilità automatizzata e agricoltura efficiente sotto il profilo delle risorse a reti elettriche intelligenti e industria 4.0. Oltre a ciò la BEI, con il sostegno del Fondo europeo per gli investimenti strategici, ha erogato prestiti per accelerare la ricerca e lo sviluppo della tecnologia 5G.

Il codice europeo delle comunicazioni elettroniche ("il codice")[7], che si applicherà dal 21 dicembre 2020, rappresenta una base importante per creare un ambiente favorevole agli investimenti per le reti 5G e non solo. Inoltre i programmi di finanziamento pubblico, quali il meccanismo per collegare l'Europa - settore digitale[8] o i fondi strutturali e di investimento europei saranno altresì essenziali per sostenere il futuro dispiegamento delle reti 5G, in particolare collegando le comunità ai servizi abilitati al 5G, quali scuole, ospedali, città e amministrazioni locali.

Considerando le opportunità strategiche dell'Europa nell'applicazione di servizi 5G in vari settori industriali, sarà di fondamentale importanza che gli operatori e i fornitori di servizi investano nelle soluzioni di rete e di servizi 5G avanzate. Queste ultime richiederanno non solo nuove reti radio 5G, ma anche le nuove reti centrali 5G cosiddette "*stand-alone*", al fine

[4] http://www.5GObservatory.eu

[5] http://www.5GObservatory.eu

[6] Alcune delle nuove funzionalità del 5G saranno introdotte secondo un approccio graduale. In una prima fase (breve o brevissimo termine) il dispiegamento del 5G consisterà principalmente in reti "non autonome" ("*non stand-alone*"), in cui solo la rete di accesso radio è aggiornata alla tecnologia 5G, mentre per il resto ci si affiderà ancora alle reti centrali 4G esistenti, che forniranno agli utenti finali prestazioni potenziate della banda larga mobile. Durante le fasi successive (da breve/medio termine a lungo termine) il dispiegamento delle reti 5G "autonome" ("*stand-alone*"), comprese le funzioni della rete centrale 5G, richiederà e si tradurrà nel tempo in un cambiamento molto più radicale dell'architettura di rete.

[7] Direttiva (UE) 2018/1972 del Parlamento europeo e del Consiglio che istituisce il codice europeo delle comunicazioni elettroniche (rifusione).

[8] Proposta di regolamento del Parlamento europeo e del Consiglio che istituisce il meccanismo per collegare l'Europa e abroga i regolamenti (UE) n. 1316/2013 e (UE) n. 283/2014 [COM(2018) 438 final].

di fornire funzionalità 5G avanzate come il *network slicing*[9] (segmentazione della rete) e l'*edge computing*[10] (elaborazione dati ai margini della rete).

La Commissione continuerà a sostenere pienamente il lancio efficace del 5G nell'UE, anche impegnandosi con gli Stati membri e le parti interessate a cogliere le opportunità del 5G. Gli aspetti pertinenti relativi alla salute saranno tenuti in debita considerazione in base al principio di precauzione[11], in collaborazione con le organizzazioni internazionali competenti e la comunità scientifica.

3. La valutazione dei rischi coordinata a livello dell'UE sulla cibersicurezza delle reti 5G

Lavorando insieme nell'ambito del gruppo di cooperazione NIS[12], ciascuno Stato membro ha completato la valutazione dei rischi a livello nazionale delle sue infrastrutture di rete 5G e ha trasmesso i risultati alla Commissione e all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, entro l'inizio di luglio 2019.

Sulla base di tali valutazioni nazionali dei rischi, il 9 ottobre 2019 il gruppo di cooperazione NIS, composto da rappresentanti degli Stati membri, della Commissione e dell'ENISA, ha pubblicato una relazione sulla valutazione dei rischi coordinata a livello dell'UE sulla cibersicurezza delle reti 5G[13]. In tale relazione si individuano le minacce più rilevanti e i principali autori di tali minacce, le risorse più sensibili e le principali vulnerabilità (di natura tecnica e di altro tipo) che interessano le reti 5G. In base a ciò, nella relazione sono inoltre individuate una serie di categorie di rischio di importanza strategica per l'UE, illustrate da scenari di rischio concreti, che riflettono combinazioni pertinenti dei diversi parametri (vulnerabilità, minacce e autori di tali minacce) con riferimento ai diversi asset (cfr. appendice).

A complemento di tale relazione e come ulteriore contributo al pacchetto di strumenti, l'ENISA ha effettuato un'apposita mappatura del panorama delle minacce[14], che consiste in un'analisi dettagliata di determinati aspetti tecnici, in particolare l'individuazione degli asset di rete e delle minacce da cui sono interessati.

La relazione di valutazione dei rischi coordinata a livello dell'UE evidenzia una serie di aspetti importanti per le reti 5G, in particolare:

a) i cambiamenti tecnologici introdotti dal 5G offriranno ai responsabili di attacchi informatici una più ampia superficie complessiva di attacco e un numero maggiore di potenziali punti di ingresso:

[9] Il *network slicing* 5G consente un elevato grado di separazione tra diversi livelli di servizio sulla stessa rete fisica, aumentando così le possibilità di offrire servizi differenziati su tutta la rete.

[10] L'*edge computing* è un paradigma di calcolo distribuito che consente di elaborare e immagazzinare i dati più vicino a dove servono, per migliorare i tempi di risposta e risparmiare larghezza di banda.

[11] Raccomandazione 1999/519/CE del Consiglio, del 12 luglio 1999, relativa alla limitazione dell'esposizione della popolazione ai campi elettromagnetici da 0 Hz a 300 GHz.

[12] Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (direttiva NIS). Il gruppo di cooperazione NIS è stato istituito dalla direttiva NIS per garantire la cooperazione strategica e lo scambio di informazioni in materia di cibersicurezza tra gli Stati membri dell'UE.

[13] https://ec.europa.eu/digital-single-market/en/news/eu-wide-coordinated-risk-assessment-5g-networks-security

[14] Panorama delle minacce per le reti 5G dell'ENISA: https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks.

- poiché le funzionalità ai margini della rete sono migliorate e l'architettura è meno centralizzata rispetto alle precedenti generazioni di reti mobili, alcune funzioni delle reti centrali possono essere integrate in altre parti della rete, rendendo le apparecchiature corrispondenti più sensibili (ad esempio stazioni radio base o funzioni MANO);

- l'aumento dell'importanza del software utilizzato nelle apparecchiature 5G comporta maggiori rischi legati allo sviluppo di software e ai processi di aggiornamento, crea nuovi rischi di errori di configurazione e attribuisce un ruolo più importante nell'analisi della sicurezza alle scelte effettuate da ciascun operatore di rete mobile nella fase di dispiegamento della rete.

b) Queste nuove caratteristiche tecnologiche attribuiranno maggiore importanza alla dipendenza degli operatori di rete mobile dai fornitori terzi e al loro ruolo nella catena di approvvigionamento del 5G.

Ciò, a sua volta, aumenterà il numero dei percorsi di attacco che potrebbero essere utilizzati dagli autori delle minacce, in particolare gli attori statali o i soggetti sostenuti da governi di paesi terzi, a causa delle loro capacità (intenzione e risorse) di compiere attacchi contro le reti di telecomunicazione degli Stati membri dell'UE, nonché la potenziale gravità dell'impatto di tali attacchi.

In questo contesto di maggiore esposizione agli attacchi facilitati da fornitori terzi, il profilo di rischio individuale dei fornitori diventerà particolarmente importante, in particolare qualora un fornitore abbia una presenza significativa all'interno di reti o aree.

c) Una dipendenza significativa da un unico fornitore aumenta l'esposizione a un potenziale fallimento di tale fornitore e alle conseguenze che ne derivano. Ciò amplifica inoltre le potenziali conseguenze di debolezze o vulnerabilità, nonché la possibilità che queste vengano sfruttate dagli autori di minacce, in particolare qualora tale dipendenza riguardi un fornitore che presenta un elevato grado di rischio.

d) Se alcuni dei nuovi casi d'uso previsti per il 5G si concretizzeranno, le reti 5G finiranno per essere una parte importante della catena di approvvigionamento di molte applicazioni informatiche critiche e, in quanto tali, non solo avranno un impatto sulla riservatezza e sui requisiti di tutela della vita privata, ma l'integrità e la disponibilità di tali reti diventeranno importanti questioni di sicurezza nazionale e una sfida di primo piano per la sicurezza a livello di UE.

Fonte: valutazione dei rischi coordinata a livello dell'UE

La relazione di valutazione dei rischi coordinata a livello dell'UE conclude inoltre che tali sfide creano un nuovo paradigma di sicurezza, il che rende necessario riesaminare l'attuale quadro strategico e di sicurezza applicabile al settore 5G e al suo ecosistema, rendendo inoltre essenziale che gli Stati membri adottino le necessarie misure di attenuazione.

Al fine di affrontare efficacemente i rischi individuati e rafforzare la sicurezza e la resilienza delle reti 5G è necessario un approccio globale, che implichi l'attuazione di una serie di misure chiave e di azioni di sostegno correlate che possano, allo stesso tempo, affrontare i

rischi. La valutazione dei rischi coordinata a livello dell'UE ha fornito la base per individuare le misure di attenuazione che possono essere applicate a livello nazionale ed europeo.

Le conclusioni del Consiglio del 3 dicembre 2019 hanno appoggiato i risultati della valutazione coordinata dei rischi e hanno sottolineato "l'importanza di un approccio coordinato e di un'efficace attuazione della raccomandazione al fine di evitare la frammentazione del mercato unico"[15]. A tal fine, il Consiglio ha invitato gli Stati membri, la Commissione e l'ENISA "ad adottare tutte le misure necessarie nell'ambito delle rispettive competenze per garantire la sicurezza e l'integrità delle reti di comunicazione elettronica, in particolare le reti 5G, e a continuare a consolidare un approccio coordinato per affrontare le sfide per la sicurezza relative alle tecnologie 5G".

4. Pacchetto di strumenti dell'UE sulla cibersicurezza del 5G

Il 29 gennaio 2020 il gruppo di cooperazione NIS ha pubblicato il pacchetto di strumenti dell'UE comprendente misure di attenuazione dei rischi[16], che affronta tutti i rischi individuati nella relazione coordinata sulla valutazione dei rischi.

Il pacchetto di strumenti dell'UE individua e descrive una serie di misure strategiche e tecniche, nonché di corrispondenti azioni di sostegno volte a rafforzare la loro efficacia, che possono essere attuate per attenuare i rischi individuati. Le **misure strategiche** comprendono misure riguardanti il conferimento di maggiori poteri di regolamentazione alle autorità per controllare gli appalti e il dispiegamento delle reti, misure specifiche per affrontare i rischi relativi alle vulnerabilità di tipo non tecnico, nonché possibili iniziative volte a promuovere catene di approvvigionamento e del valore del 5G sostenibili e diversificate, al fine di evitare rischi di dipendenza sistemici e a lungo termine. Le **misure tecniche** comprendono misure volte a rafforzare la sicurezza delle reti e delle apparecchiature 5G, affrontando i rischi derivanti dalle tecnologie, dai processi e dai fattori umani e fisici. Inoltre, per ciascuna delle aree di rischio individuate nell'ambito della valutazione dei rischi coordinata a livello dell'UE, il pacchetto di strumenti prevede **piani di attenuazione dei rischi** basati sulle misure più efficaci.

Tra queste, nelle conclusioni del pacchetto di strumenti dell'UE concordate dal gruppo di cooperazione NIS, si raccomandano una serie di **misure chiave** che devono essere attuate da tutti gli Stati membri e dalla Commissione, come segue.

Conclusioni del pacchetto di strumenti dell'UE

Il pacchetto di strumenti dell'UE stabilisce una serie di misure e azioni che, se adeguatamente combinate e attuate in modo efficace, costituiscono la base per un approccio coordinato in questo settore. Infatti data l'ampia gamma di aree a rischio individuate nell'ambito della valutazione dei rischi coordinata a livello dell'UE e la loro diversa natura, un singolo tipo di misure non è sufficiente, ma è invece necessaria una serie di misure utilizzate in una combinazione adeguata, al fine di affrontare tutte le principali aree di rischio.

In base alla valutazione dei possibili piani di attenuazione e all'individuazione delle misure più efficaci, il pacchetto di strumenti comprende le seguenti raccomandazioni.

[15] Conclusioni del Consiglio del 3 dicembre 2019 sull'importanza del 5G per l'economia europea e sulla necessità di attenuare i relativi rischi per la sicurezza, 14517/19, https://data.consilium.europa.eu/doc/document/ST-14517-2019-INIT/it/pdf.

[16] *Cybersecurity of 5G networks - EU Toolbox of risk mitigating measures* (Cibersicurezza delle reti 5G - Pacchetto di strumenti dell'UE comprendente misure di attenuazione), 29 gennaio 2020, https://ec.europa.eu/digital-single-market/en/nis-cooperation-group.

1. Tutti gli Stati membri dovrebbero garantire l'attuazione di misure (compreso il conferimento di poteri alle autorità nazionali) volte a rispondere in modo adeguato e proporzionato ai rischi già individuati e ai rischi futuri e in particolare garantire di essere in grado di limitare, vietare e/o imporre requisiti o condizioni specifici per quanto riguarda la fornitura, il dispiegamento e il funzionamento delle apparecchiature di rete 5G, adottando un approccio basato sul rischio e basandosi su una serie di motivi legati alla sicurezza.

In particolare dovrebbero:

- *rafforzare i **requisiti di sicurezza** per gli operatori di rete mobile (ad esempio controlli rigorosi degli accessi, norme relative al funzionamento sicuro e al monitoraggio, restrizioni all'esternalizzazione di funzioni specifiche ecc.);*

- *valutare il profilo di rischio dei fornitori; di conseguenza, **applicare le pertinenti restrizioni (comprese le necessarie esclusioni volte ad attenuare efficacemente i rischi) ai fornitori ritenuti ad alto rischio per gli asset chiave**, definiti critici e sensibili nella valutazione dei rischi coordinata a livello dell'UE (ad esempio funzioni della rete centrale, funzioni di gestione e orchestrazione della rete e funzioni di accesso alla rete);*

- *garantire che ogni operatore disponga di un'adeguata strategia multifornitore per **evitare o limitare l'eventuale forte dipendenza** da un unico fornitore (o da fornitori con un profilo di rischio simile), garantire un adeguato equilibrio tra i fornitori a livello nazionale ed **evitare la dipendenza da fornitori considerati ad alto rischio**. A tal fine sarà inoltre necessario evitare situazioni di lock-in con un unico fornitore, anche promuovendo una maggiore interoperabilità delle apparecchiature.*

2. La Commissione europea, di concerto con gli Stati membri, dovrebbe contribuire a:

- *mantenere **una catena di approvvigionamento del 5G diversificata e sostenibile** al fine di evitare dipendenze a lungo termine, anche:*

  *o utilizzando appieno gli strumenti dell'UE esistenti, in particolare mediante il controllo dei possibili **investimenti esteri diretti** (IED) che incidono sugli asset chiave del 5G ed evitando **distorsioni** del mercato della fornitura del 5G derivanti da possibili pratiche di dumping o sovvenzioni; e*

  *o rafforzando ulteriormente le **capacità dell'UE nelle tecnologie 5G e post 5G** facendo ricorso ai pertinenti programmi e finanziamenti dell'UE;*

- *facilitare il coordinamento tra gli Stati membri in materia di **normazione** per conseguire specifici obiettivi di sicurezza e **sviluppare pertinenti sistemi di certificazione dell'UE** al fine di promuovere prodotti e processi più sicuri.*

3. Per garantire che tale approccio coordinato resista alla prova del tempo, il mandato del gruppo di cooperazione NIS dovrebbe essere ampliato, come pure la cooperazione con altri organismi ed entità pertinenti, in particolare al fine di:

- *rivedere periodicamente, con il sostegno della Commissione e dell'ENISA, le **valutazioni dei rischi a livello nazionale e dell'UE** in materia di sicurezza delle reti 5G e post-5G, sviluppando ulteriormente e allineando la metodologia di valutazione seguita e adeguandosi all'evoluzione della tecnologia 5G;*

- *effettuare **un monitoraggio e una valutazione** dettagliati e periodici **dell'attuazione** del pacchetto di strumenti sulla base di relazioni strutturate degli Stati membri;*

- *coordinare e sostenere l'attuazione delle **azioni di sostegno**, che richiedono una cooperazione a livello dell'UE, in particolare per quanto riguarda l'elaborazione di orientamenti e lo scambio delle migliori pratiche sulle varie misure;*

- *sostenere, ove opportuno, un ulteriore eventuale coordinamento a livello dell'UE, in particolare per promuovere una maggiore convergenza per quanto riguarda **i requisiti di sicurezza tecnici e organizzativi per gli operatori di rete**.*

Fonte: pacchetto di strumenti dell'UE.

Le conclusioni del pacchetto di strumenti dimostrano la forte determinazione degli Stati membri a rispondere congiuntamente alle sfide per la sicurezza delle reti 5G. Ciò è di fondamentale importanza per la sicurezza all'interno degli Stati membri e a livello dell'UE, per le economie nazionali, per il mercato interno dell'UE e per la sovranità tecnologica dell'Europa. Sia la valutazione dei rischi coordinata a livello dell'UE sia il pacchetto di strumenti dell'UE mostrano l'elevato valore del lavoro collettivo svolto nell'ambito del gruppo di cooperazione NIS, con un'intensa collaborazione tra i rappresentanti di tutti gli Stati membri, della Commissione e dell'ENISA.

Il pacchetto di strumenti consente un approccio comune dell'UE alla cibersicurezza del 5G, sostenendo la coerenza in tutto il mercato interno mediante le politiche e il coordinamento dell'UE, nonché l'esercizio delle competenze degli Stati membri, in particolare per quanto riguarda la sicurezza nazionale. Le misure e i piani di attenuazione in esso contenuti consentono all'UE di rispondere in modo adeguato, efficace e proporzionato alle sfide comuni per la cibersicurezza del 5G.

La Commissione accoglie con favore la pubblicazione del pacchetto di strumenti dell'UE sulla cibersicurezza del 5G e sostiene pienamente tutte le sue conclusioni di cui sopra.

La Commissione invita gli Stati membri e le pertinenti istituzioni, agenzie e altri organismi dell'Unione a:

i) garantire la rapida attuazione di strategie efficaci e appropriate di attenuazione dei rischi in tutta l'UE, in linea con il pacchetto di strumenti dell'UE, e

ii) adottare tutte le ulteriori misure necessarie per garantire il coordinamento a livello dell'Unione, anche mediante un lavoro costante nell'ambito del gruppo di cooperazione NIS e l'istituzione di un solido meccanismo per monitorare l'attuazione del pacchetto di strumenti dell'UE, al fine di garantire l'efficacia delle misure e il funzionamento senza intoppi del mercato interno.

5. Attuazione del pacchetto di strumenti

La determinazione degli Stati membri nell'utilizzare appieno il pacchetto di strumenti è essenziale per un approccio europeo efficace e credibile alla sicurezza del 5G. Saranno gli Stati membri a decidere, in base alle circostanze nazionali, se una particolare misura è adeguata, ma è assolutamente essenziale che, **come raccomandato dal gruppo di cooperazione NIS (cfr. le conclusioni del pacchetto di strumenti di cui sopra), una serie di misure chiave siano attuate in ogni Stato membro, , e alcune di esse siano attuate a livello dell'UE**, al fine di affrontare i rischi individuati.

La Commissione è pronta a continuare a fornire pieno sostegno durante le prossime fasi e invita gli Stati membri:

- **entro il 30 aprile 2020**, a intraprendere azioni concrete e misurabili per attuare la serie di misure chiave raccomandate nelle conclusioni del pacchetto di strumenti dell'UE;

- **entro il 30 giugno 2020**, a preparare una relazione del gruppo di cooperazione NIS sullo stato di attuazione in ciascuno Stato membro di tali misure chiave, in base alle relazioni presentate e al monitoraggio effettuato periodicamente, in particolare nell'ambito del gruppo di cooperazione NIS, con il sostegno della Commissione e dell'ENISA.

5.1. Un approccio concertato e basato sul rischio ai fornitori del 5G

Dato l'obiettivo ultimo di garantire la sicurezza, la resilienza e la sostenibilità delle reti 5G, gli Stati membri hanno convenuto sulla necessità di valutare il profilo di rischio dei singoli fornitori e di applicare di conseguenza, per gli asset principali, le relative misure restrittive nei confronti dei fornitori considerati ad alto rischio, comprese le esclusioni necessarie per attenuare efficacemente i rischi, come indicato nel pacchetto di strumenti. La Commissione è pronta a sostenere gli Stati membri nell'attuazione di tali misure.

Per sostenere tale attuazione in tutta l'UE, la valutazione dei rischi coordinata a livello dell'UE e il pacchetto di strumenti dell'UE forniscono orientamenti per quanto riguarda 1) la valutazione del profilo di rischio dei fornitori[17] e 2) la sensibilità degli elementi e delle funzioni di rete[18], come pure di altri asset. Sia la valutazione dei rischi coordinata a livello dell'UE sia le misure del pacchetto di strumenti contemplano i rischi relativi ai fornitori di apparecchiature e servizi di rete 5G, ma non coprono gli altri prodotti o servizi che possono essere offerti da tali o da altri fornitori.

Come definito al punto 2.37 della valutazione dei rischi coordinata a livello dell'UE, i profili di rischio dei singoli fornitori possono essere valutati sulla base di diversi fattori.

La valutazione dei profili di rischio dei fornitori dovrebbe essere condotta unicamente per motivi di sicurezza e sulla base di criteri oggettivi. Per facilitare un approccio coordinato all'attuazione di tali misure, il pacchetto di strumenti raccomanda agli Stati membri di scambiarsi informazioni in merito agli approcci e alle migliori pratiche a livello nazionale. La Commissione ritiene inoltre che tale azione debba costituire una delle principali priorità della prossima fase di lavoro in seno al gruppo di cooperazione NIS, in collaborazione con la Commissione e l'ENISA.

È importante che le misure restrittive nei confronti dei fornitori considerati ad alto rischio, comprese le esclusioni necessarie per mitigare efficacemente i rischi, e le misure volte a evitare la dipendenza da tali fornitori, siano attuate tempestivamente. Un'attuazione già nelle primissime fasi, se possibile anche in relazione alle procedure di concessione delle licenze per le frequenze 5G, aumenterà anche la prevedibilità per gli operatori del mercato, contribuendo

[17] Punto 2.37 della valutazione dei rischi coordinata a livello dell'UE.

[18] Al punto 2.21 della valutazione dei rischi coordinata a livello dell'UE sono illustrati le principali categorie di elementi e funzioni e il loro livello complessivo di sensibilità, e sono elencati una serie di elementi chiave individuati dagli Stati membri per ciascuna categoria. Ai punti 2.28 e 2.29 sono individuati diversi altri tipi di asset o ambiti sensibili (ad esempio entità o aree geografiche specifiche).

quindi a un rapido lancio delle reti 5G, garantendone la sicurezza a lungo termine e assicurando la resilienza della catena di approvvigionamento del 5G.

Nel contempo, l'attuazione di tali misure a livello nazionale può prevedere scadenze diverse, se necessario e giustificato, in particolare nel caso in cui sussista un elevato grado di dipendenza da apparecchiature o servizi offerti da fornitori giudicati ad alto rischio (ad esempio tenendo conto dei cicli di aggiornamento delle apparecchiature, in particolare della migrazione da reti 5G *non stand-alone* a reti 5G *stand-alone*). Gli Stati membri potrebbero prendere in considerazione la definizione di piani di attuazione che includano gli opportuni periodi di transizione per gli operatori di rete interessati. In tale contesto i periodi di transizione dovrebbero essere definiti in modo tale da preservare o addirittura rafforzare gli incentivi agli investimenti in apparecchiature di rete moderne, anche accelerando il dispiegamento di reti centrali 5G vere e proprie (*stand-alone*) e sostituendo le attuali apparecchiature 4G in altre parti delle reti (ad esempio nella rete di accesso radio), in linea con gli obiettivi del piano d'azione per il 5G[19].

Inoltre, a causa della complessità delle reti 5G basate su software, è possibile che gli operatori di telecomunicazioni si affidino sempre più a terzi per svolgere determinate attività, quali la manutenzione e l'aggiornamento delle reti e dei software 5G, nonché altri servizi gestiti esternalizzati, oltre che per la fornitura di apparecchiature di rete. Come descritto nella valutazione dei rischi coordinata a livello dell'UE, ciò costituisce una fonte di grave rischio per la sicurezza ed è quindi necessario prestarvi particolare attenzione. È fondamentale effettuare anche una valutazione approfondita della sicurezza del profilo di rischio dei fornitori che si occupano di tali servizi, in particolare quando le attività non sono svolte nell'UE. È opportuno adottare le misure adeguate, anche applicando restrizioni, in particolare in parti sensibili delle reti 5G, o la necessaria esclusione dei soggetti ad alto rischio, in linea con le misure di attenuazione del pacchetto di strumenti, al fine di preservare l'integrità a lungo termine dell'infrastruttura 5G.

5.2. Il ruolo della Commissione nel sostegno all'attuazione del pacchetto di strumenti

La Commissione continuerà a sostenere l'attuazione dell'approccio dell'UE alla cibersicurezza del 5G nel suo complesso, nonché a intraprendere iniziative specifiche in relazione alle misure e agli obiettivi del pacchetto di strumenti ove ciò possa apportare un valore aggiunto. La Commissione utilizzerà appieno le sue competenze e gli strumenti pertinenti nella misura necessaria per affrontare le considerazioni in materia di sicurezza che sono state sollevate. In questo modo, e mediante un'azione collettiva con gli Stati membri e il settore privato, la Commissione intende sostenere misure strategiche che contribuiranno a garantire la sovranità e la leadership tecnologica dell'UE nello sviluppo futuro delle tecnologie di rete, nelle tecnologie di cibersicurezza e in tutti i pertinenti elementi costitutivi da cui dipendono la nostra intera economia e la nostra sicurezza.

Più precisamente, per garantire l'attuazione delle corrispondenti misure di attenuazione del pacchetto di strumenti nei settori di sua competenza la Commissione intraprenderà le azioni seguenti.

Salvaguardia della cibersicurezza delle reti 5G e di una catena del valore del 5G diversificata

[19] Comunicazione della Commissione del 14 settembre 2016 - Il 5G per l'Europa: un piano d'azione [COM(2016) 588 final].

- **Cooperazione in materia di cibersicurezza**: proseguimento del sostegno agli Stati membri per l'attuazione efficace, coordinata e tempestiva di misure nazionali attraverso il gruppo di cooperazione NIS.

- **Norme in materia di telecomunicazioni e cibersicurezza**: sostegno all'attuazione delle misure del pacchetto di strumenti relative ai requisiti di sicurezza, in particolare per quanto riguarda le pertinenti disposizioni della normativa europea sulle comunicazioni elettroniche, e presa in esame del valore aggiunto di eventuali atti di esecuzione che specifichino misure di sicurezza tecniche e organizzative al fine di integrare le norme nazionali e rafforzare l'efficacia e la coerenza delle misure di sicurezza imposte agli operatori.

- **Normazione**: interventi per contribuire a mantenere e, se necessario, ad aumentare la partecipazione europea in seno ai rispettivi organismi di normazione al fine di conseguire gli obiettivi europei di sicurezza e interoperabilità. In particolare la Commissione, insieme agli Stati membri, valuterà e promuoverà le specifiche e le norme tecniche che consentono l'interoperabilità tra i fornitori di apparecchiature 5G in diverse parti della rete, comprese le reti legacy, al fine di garantire un ambiente propriamente multifornitore, ad esempio attraverso interfacce aperte e interoperabili.

- **Certificazione**: sostegno all'elaborazione di sistemi di certificazione del 5G volti a rispondere alle esigenze delle reti 5G nell'ambito del quadro di certificazione della cibersicurezza dell'UE.

- **Controllo degli investimenti esteri diretti (IED)**: sostegno all'attuazione del quadro di controllo dell'UE attraverso la mappatura della catena del valore del 5G, compresi gli asset di rete sensibili, e il controllo periodico degli IED lungo la catena del valore. In linea con il calendario per il controllo degli IED (ottobre 2020), la Commissione esaminerà gli investimenti esteri nel settore del 5G conformemente agli orientamenti di cui al regolamento (UE) 2019/452, tenendo conto della valutazione dei rischi coordinata a livello dell'UE e del pacchetto di strumenti dell'UE.

- **Strumenti di difesa commerciale**: monitoraggio di tutti i pertinenti sviluppi del mercato nell'UE e nei paesi terzi e tutela degli attori dell'UE sul mercato europeo del 5G mediante misure di difesa commerciale volte a far fronte a potenziali pratiche di distorsione degli scambi (dumping o sovvenzioni), anche attraverso l'avvio di indagini preliminari laddove opportuno.

- **Regole di concorrenza:** monitoraggio del funzionamento dei mercati per la fornitura di hardware e software per il 5G al fine di garantire che producano risultati concorrenziali, anche in relazione a possibili situazioni di lock-in contrattuale o tecnico.

- **Programmi di finanziamento dell'UE**: garanzia che la partecipazione ai programmi di finanziamento dell'UE nei pertinenti settori tecnologici sia subordinata al rispetto dei requisiti di sicurezza, facendo pieno ricorso alle condizioni di sicurezza e attuandole ulteriormente nei programmi di ricerca e innovazione, in particolare Orizzonte Europa, il programma Europa digitale e il Meccanismo per collegare l'Europa (*Connecting Europe Facility*, CEF) 2.0, nei fondi strutturali e di investimento europei e in altri programmi pertinenti. Un approccio analogo dovrebbe essere adottato anche nell'ambito dei programmi di finanziamento e degli strumenti finanziari esterni dell'UE, anche per quanto riguarda i finanziamenti erogati mediante le istituzioni finanziarie internazionali.

- Appalti pubblici: sfruttamento degli appalti pubblici nel settore delle reti 5G per sostenere gli obiettivi individuati relativi alla sicurezza, alla diversificazione dei fornitori e alla sostenibilità a lungo termine delle reti 5G. In particolare, la Commissione cercherà di garantire che nell'aggiudicazione degli appalti pubblici relativi al settore delle reti 5G si tengano in debita considerazione gli aspetti di sicurezza, in linea con le norme dell'UE in materia di appalti pubblici.

- **Risposta agli incidenti e gestione delle crisi (programma) e esercitazioni di cibersicurezza**: pieno sfruttamento dello sviluppo del programma dell'UE[20] per una risposta coordinata agli incidenti di cibersicurezza su vasta scala. Inoltre, in collaborazione con l'ENISA, la Commissione esaminerà la possibilità di condurre un'esercitazione di cibersicurezza del 5G non appena la maturità del mercato lo consentirà.

E, sotto la responsabilità dell'alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza e vicepresidente della Commissione, e del Consiglio:

- **quadro relativo a una risposta diplomatica comune dell'UE alle attività informatiche dolose (pacchetto di strumenti della diplomazia informatica)[21]**: in caso di attività informatiche dolose che minacciano l'integrità e la sicurezza dell'UE, gli Stati membri sono incoraggiati ad avvalersi delle pertinenti misure in materia di politica estera e di sicurezza comune che fanno parte del pacchetto di strumenti della diplomazia informatica (comprese, se necessario, misure restrittive) al fine di incoraggiare la cooperazione, facilitare l'attenuazione delle minacce e influenzare il comportamento di potenziali aggressori.

Una serie di programmi contribuirà inoltre al raggiungimento dell'obiettivo di evitare o limitare il rischio di dipendenza a lungo termine mediante la promozione di un mercato diversificato e sostenibile per il 5G, anche mantenendo le capacità dell'UE nella catena del valore del 5G e investendo nell'innovazione, in linea con gli obblighi internazionali dell'UE.

Promozione dell'innovazione e investimenti nella cibersicurezza e nelle tecnologie di infrastruttura di rete

- **Programmi** di finanziamento dell'UE: aumento degli investimenti in ricerca, innovazione e dispiegamento delle tecnologie di rete e dei pertinenti elementi costitutivi. Nel quadro del prossimo bilancio dell'UE per il periodo 2021-2027, la Commissione ha proposto quasi 3 miliardi di EUR di investimenti nelle tecnologie di cibersicurezza, compresi la ricerca e l'innovazione nel quadro di Orizzonte Europa e il sostegno alle capacità di cibersicurezza nel quadro del programma Europa digitale. Anche InvestEU può fornire sostegno finanziario alla ricerca e allo sviluppo nel settore del 5G, nonché sostegno al suo dispiegamento.

Nel quadro del prossimo programma Orizzonte Europa[22], la Commissione ha inoltre proposto l'istituzione di un partenariato istituzionalizzato dell'UE in materia di Internet di prossima generazione (*Next Generation Internet*, NGI)/6G ("Reti e servizi intelligenti"), in collaborazione con l'industria e coordinandosi con gli Stati membri, al fine di ultimare il dispiegamento del 5G e soprattutto **prepararsi al 6G**, la prossima generazione di tecnologie

[20] Raccomandazione (UE) 2017/1584 della Commissione relativa alla risposta coordinata agli incidenti e alle crisi di cibersicurezza su vasta scala.
[21] Conclusioni del Consiglio del 20 novembre 2017 (9916/17).
[22] I finanziamenti possono essere erogati anche attraverso il CEF 2.0 e il programma Europa digitale.

mobili. Per questa iniziativa sono stati proposti oltre 2,5 miliardi di EUR di investimenti dell'UE a titolo del bilancio dell'Unione 2021-2027, cui si dovranno aggiungere almeno 7,5 miliardi di EUR di investimenti privati.

- **Sviluppo industriale e dispiegamento**: valutazione di potenziali fallimenti o lacune di mercato lungo la catena del valore del 5G, tali da giustificare interventi mirati nel quadro del prossimo bilancio a lungo termine o un possibile IPCEI (importante progetto di comune interesse europeo) sulla cibersicurezza, in linea con i suggerimenti del forum ad alto livello IPCEI. La decisione in merito alla definizione e alla preparazione degli IPCEI spetta agli Stati membri e alle imprese. Le norme dell'UE offrono un quadro favorevole e la Commissione è pronta a facilitare i contatti necessari e a fornire orientamenti.

6. Conclusioni

Le reti 5G offriranno una serie di opportunità ai cittadini, alla società e all'economia europei. È quindi essenziale garantirne la sicurezza e la resilienza. Al tempo stesso le minacce alla cibersicurezza (compreso il rischio di interferenza da parte di attori statali o soggetti sostenuti da governi di paesi terzi) rappresentano una sfida in continua evoluzione, la cui rilevanza aumenta parallelamente all'aumento della dipendenza dalla tecnologia e dai dati. Trascurare la cibersicurezza comprometterebbe la fiducia nello sviluppo dell'economia e della società digitali e impedirebbe all'UE di trarne pienamente vantaggio. Per questo motivo è necessaria una risposta che sia ugualmente in evoluzione e rafforzata.

Un approccio coordinato e coerente alla cibersicurezza nell'UE per le tecnologie e le reti critiche è fondamentale affinché l'Unione possa garantire la sua sovranità tecnologica, mantenendo e sviluppando capacità industriali. La Commissione sosterrà pienamente l'attuazione dell'approccio dell'UE alla cibersicurezza delle reti 5G, garantendo nel contempo che i mercati dell'Unione restino aperti a prodotti e servizi che rispettano i requisiti in evoluzione in materia di cibersicurezza e fiducia.

A tal fine è importante che tutte le parti interessate mantengano un elevato livello di impegno in materia di sicurezza del 5G, e sarà necessaria una collaborazione continua tra gli Stati membri, la Commissione e l'ENISA.

Quale passo immediatamente successivo, come illustrato in precedenza, la Commissione invita gli Stati membri ad agire rapidamente per attuare in maniera efficace e obiettiva le misure concordate nell'ambito del pacchetto di strumenti e a continuare a collaborare, con il sostegno della Commissione e dell'ENISA, per garantire il coordinamento a livello dell'UE. Parallelamente, la Commissione intraprenderà tutte le azioni pertinenti nell'ambito delle sue competenze al fine di sostenere l'attuazione del pacchetto di strumenti da parte degli Stati membri e di rafforzarne l'impatto.

Appendice: categorie di rischio (fonte: valutazione dei rischi coordinata a livello dell'UE)

	Categorie di rischio
Scenari di rischio relativi a insufficienti misure di sicurezza	*R1: configurazione errata delle reti*
	R2: mancanza di controlli degli accessi
Scenari di rischio relativi alla catena di approvvigionamento del 5G	*R3: scarsa qualità dei prodotti*
	R4: dipendenza da singoli fornitori all'interno di singole reti o mancanza di diversificazione su base nazionale
Scenari di rischio relativi al modus operandi dei principali autori delle minacce	*R5: interferenza statale attraverso la catena di approvvigionamento del 5G*
	R6: sfruttamento delle reti 5G da parte della criminalità organizzata o di gruppi criminali organizzati che mirano a colpire gli utenti finali
Scenari di rischio relativi alle interdipendenze tra le reti 5G e altri sistemi critici	*R7: perturbazione significativa di infrastrutture o servizi critici*
	R8: guasto di rete grave e generalizzato causato dall'interruzione della fornitura di energia elettrica o di altri sistemi di supporto
Scenari di rischio relativi ai dispositivi degli utenti finali	*R9: sfruttamento dell'Internet delle cose (Internet of Things, IoT)*