SIOI
UNA Italy
OSSERVATORIO
sulle attività delle organizzazioni internazionali e sovranazionali, universali e regionali, sui temi di interesse della politica estera italiana

Le nuove sfide della tecnologia 5G per la sicurezza cibernetica: l'approccio dell'Unione europea

Lorenzo Grossio
Studente senior, Università degli Studi di Torino

Lo sviluppo della c.d. "quinta generazione" delle reti di telecomunicazione, più comunemente nota come "5G", costituisce da alcuni anni uno dei temi di massima attenzione della politica estera ed economica delle maggiori potenze mondiali. Tale nuova tecnologia è destinata a costituire l'infrastruttura privilegiata per numerosi servizi essenziali, divenendo lo strumento principale per la transizione digitale di numerosi settori, tra cui l'industria, i media, la sanità ed i trasporti.

In questo contesto, l'Unione europea si è posta obiettivi ambiziosi: nel piano di attuazione del 2016 – COM(2016) 588 final, Il 5G per l'Europa: un piano d'azione – è stato previsto il raggiungimento di una copertura totale nelle aree urbane e lungo i principali assi di trasporto entro il 2025. Ad oggi, secondo i dati dell'European 5G Observatory – programma di monitoraggio della Commissione europea sullo sviluppo del 5G (http://www.5GObservatory.eu) – circa il 16% delle nuove frequenze risultano essere assegnate nei vari Stati membri. Nello scenario delineato, il nostro Paese si pone in posizione piuttosto avanzata, con due operatori telefonici che hanno già effettuato il lancio commerciale dei propri servizi 5G.

L'evidente rilevanza strategica del 5G pone molteplici sfide a livello internazionale, riconducibili principalmente a due macroaree. La prima è sicuramente costituita dall'aspetto economico, caratterizzato da una vera e propria concorrenza tra i principali fornitori di servizi *hi-tech* a livello globale, con particolare riferimento alle imprese statunitensi e cinesi. L'altro ambito, non meno importante, è costituito dalle istanze relative alla sicurezza delle reti 5G, uno degli aspetti più attuali e problematici della c.d. "sicurezza cibernetica".

L'Unione europea è stata particolarmente solerte nel comprendere l'importanza di un approccio comune tra gli Stati membri rispetto alle sfide della sicurezza informatica. L'allora Presidente della Commissione europea Juncker, nel corso del discorso sullo stato dell'Unione del 2017 dichiarava: «per la stabilità delle democrazie e delle economie i cyberattacchi possono essere più pericolosi delle armi e dei carri armati». Tale affermazione è stata accompagnata dall'adozione di una serie di atti legislativi, tra cui vanno ricordati la direttiva NIS, direttiva (UE) 2016/1148, ed il più recente Regolamento relativo all'ENISA, Regolamento (UE) 2019/881.

Nell'ambito più ristretto in esame, il 26 marzo 2019 la Commissione europea ha adottato la Raccomandazione n. 2019/534, delineando una strategia europea per la sicurezza delle reti 5G. Quest'ultima si compone innanzitutto di una valutazione dei rischi per la sicurezza informatica connessi al dispiegamento di tale nuova tecnologia, da effettuarsi prima a livello nazionale e successivamente a livello europeo. Nel corso di

questa attività, la Raccomandazione suggerisce al punto 4 l'adozione di alcune specifiche misure, tra cui l'aggiornamento dei requisiti di sicurezza e degli obblighi imposti alle imprese fornitrici di comunicazione elettronica.

Sulla base dei risultati delle analisi nazionali, la Commissione ha proposto l'individuazione di una «serie comune di misure da adottare per attenuare i rischi di cyber-sicurezza relativi alle infrastrutture alla base dell'ecosistema digitale», da effettuarsi in seno all'ENISA (European Network Information Security Agency). Scopo di tale fase è la creazione di «un inventario dei tipi di rischi di sicurezza» che possono incidere sulle reti 5G, nonché una serie di «misure di attenuazione» di questi ultimi (punto 15). Tra queste, la Commissione mette in particolare risalto la creazione di un sistema di certificazione e controllo per gli *hardware* e i *software* coinvolti, che dovrebbero essere attuati mediante l'adozione di regolamentazioni tecniche a livello nazionale (punto 16). L'approccio delineato dovrebbe inoltre favorire, nelle intenzioni della Commissione, la condivisione tra Stati membri delle buone pratiche nazionali per il contrasto alle minacce alle reti 5G, creando una sorta di *know-how* a livello europeo.

A seguito del completamento delle operazioni prospettate dalla Raccomandazione poc'anzi esaminata, il 29 gennaio 2020 la Commissione ha pubblicato una comunicazione – COM(2020) 50 final – sull'attuazione del pacchetto di strumenti UE per il dispiegamento del 5G sicuro. In questo documento la Commissione enuclea efficacemente le principali risultanze della valutazione dei rischi effettuata in sede europea, le cui risultanze specifiche sono state pubblicate ad ottobre scorso. Essa, inoltre, ha il merito di descrivere in modo compiuto lo "stato dell'arte" e le prospettive future della strategia europea per la sicurezza del 5G.

L'analisi condotta ha evidenziato alcuni aspetti nodali per la sicurezza delle infrastrutture informatiche coinvolte. È stato infatti notato come, a differenza delle precedenti reti di comunicazione, il 5G veda un ruolo sempre più predominante dei *software*, sviluppati e distribuiti da fornitori terzi. Pertanto, assumono un ruolo cruciale sia il controllo del profilo di rischio del terzo fornitore, sia la necessità di assicurare una catena di approvvigionamento opportunamente diversificata. A questo ultimo riguardo, la relazione ha evidenziato come una eventuale situazione di dipendenza significativa da un unico fornitore comporterebbe un notevole aumento dei rischi per la sicurezza, in un contesto in cui «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».

Muovendo da queste ultime considerazioni, è stato elaborato un pacchetto di strumenti UE volto a far fronte alle criticità evidenziate. Le misure in questione, come sottolineato nella comunicazione, sono ascrivibili a due diverse tipologie. Troviamo innanzitutto le misure strategiche, consistenti principalmente nell'attribuzione di maggiori poteri di controllo alle autorità nazionali volte al controllo del dispiegamento delle reti. Accanto a questo primo gruppo si trovano le misure tecniche, le quali prevedono essenzialmente l'elaborazione di standard tecnici al fine di assicurare la sicurezza delle reti.

Tra le varie misure proposte, assumono primaria importanza quelle destinate a garantire una effettiva diversificazione dei fornitori terzi, ivi compresi quelli prestanti servizi di manutenzione e aggiornamento dei *software*. Sul piano strategico il pacchetto di misure suggerisce la possibilità a livello nazionale di applicare restrizioni a fornitori considerati «ad alto rischio» nonché, se necessario, adottare delle «esclusioni volte ad attenuare efficacemente i rischi». La Commissione potrebbe a sua volta contribuire a tale finalità sia attraverso il controllo degli investimenti esteri diretti, sia mediante il potenziamento di pertinenti programmi di finanziamento e sviluppo tecnologico all'interno dell'Unione.

Il *focus* sul controllo dei fornitori non può destare particolare sorpresa. Infatti, il contesto internazionale è attualmente caratterizzato da forti pressioni statunitensi affinché gli Stati europei escludano dai propri fornitori nel campo del 5G le imprese cinesi, in virtù dei loro legami con l'autorità statale. A tale proposito, l'ENISA invita gli Stati membri ad adottare un «approccio basato sul rischio», valutando con attenzione la possibilità di escludere determinate imprese dalla catena di approvvigionamento. Allo stesso tempo, la Commissione riconosce come la competenza per tale decisione rimanga comunque in capo agli Stati membri, circostanza già ribadita da parte dell'allora Alto rappresentante UE Federica Mogherini nel corso del *Summit* UE-Cina tenutosi il 18 marzo 2019.

Nel contesto della strategia delineata, il ruolo della Commissione assume una particolare rilevanza, poiché essa assume l'impegno di coordinare e sostenere l'attuazione delle misure previste, promuovendo un'azione collettiva che coinvolga sia gli Stati membri che il settore privato. A tale scopo, la Commissione pone in rilievo la necessità di un sostegno agli Stati membri per il completamento del sistema di certificazione di cyber-sicurezza UE (già introdotto dalla Direttiva NIS), nonché di un severo controllo sui profili di sicurezza dei soggetti partecipanti ai bandi di finanziamento UE in campo tecnologico. Inoltre, si sottolinea l'importanza di sfruttare appieno le potenzialità garantite dal programma europeo per una risposta coordinata agli incidenti di cyber-sicurezza su vasta scala, introdotto dalla Raccomandazione (UE) 2017/1584. Infine, con un occhio puntato verso gli sviluppi futuri, la Commissione puntualizza come le misure elaborate vadano necessariamente accompagnate da massicci finanziamenti in campo tecnologico. Per questo scopo, la comunicazione in esame ricorda come sia intenzione della Commissione aumentare i finanziamenti in tale ambito fino a tre miliardi di euro nelle more del bilancio UE 2021-2027.

In conclusione, dagli elementi esaminati si può notare come l'Unione europea abbia individuato una strategia piuttosto elaborata e avanzata per fronteggiare le sfide della sicurezza cibernetica relative al 5G. Uno dei suoi punti di forza è sicuramente l'ampia consapevolezza dei possibili rischi e delle relative contromisure, grazie soprattutto alle approfondite analisi effettuate sia a livello nazionale che a livello europeo. Tuttavia, va notato che la maggior responsabilità per l'attuazione pratica della strategia ricade sugli Stati membri, dalla cui diligenza e grado di cooperazione dipenderà buona parte dell'efficacia concreta degli strumenti elaborati. Ed è proprio in mancanza di azioni coordinate che le pressioni statunitensi avverso gli operatori cinesi potrebbero trovare terreno fertile, rischiando di favorire approcci diversificati tra gli

Stati membri. Pertanto, è importante che ogni decisione in tale ambito venga assunta in coerenza con la strategia dell'Unione, senza influenze di natura meramente economica ed agendo in piena armonia con gli altri Stati membri e la Commissione. A quest'ultimo aspetto andrà riservata una particolare attenzione in futuro in quanto, come sottolineato dalla Commissione stessa, «un approccio coordinato e coerente alla cyber-sicurezza nell'UE per le tecnologie e le reti critiche è fondamentale affinché l'Unione possa garantire la sua sovranità tecnologica», permettendo un concreto avanzamento del progetto europeo anche in questo settore.