Geopolitica.info

CINA

I rischi del 5G cinese

A cura di *Mattia Patriarca*
Coordinamento di *Lorenzo Termine*

1 AGOSTO 2020

Il tema del 5G, le tecnologie informatiche di quinta generazione, ha sicuramente un indiscusso valore economico correlato allo sviluppo dell'industria 4.0, che rende i processi produttivi sempre più legati alle infrastrutture digitali. Il 5G ha però anche un peso politico e diplomatico molto rilevante, in grado di influenzare le relazioni tra i paesi. Esso si inserisce nelle complesse dinamiche della rivalità tra Stati Uniti e Cina, la quale è al momento in vantaggio nello sviluppo del 5G e dei dispositivi ad esso correlati. L'Italia, insieme ad altri paesi europei, si trova a dover valutare rischi e opportunità di una ipotetica collaborazione con la Cina in tale ambito.

DOMINO – Geopolitical Brief n. 3/agosto 2020 | Aut. Trib. Roma n. 88 - 6 marzo 2008
Centro Studi Geopolitica.info | www.geopolitica.info | centrostudi@geopolitica.info
Direttore responsabile: Lorenzo Termine

Il 5G rappresenta un fattore decisivo nell'economia dell'immediato futuro: con lo scoppio della pandemia di COVID19, l'Italia dovrà presto far fronte ad una fase socio-economica complessa, nella quale sarà necessario fare affidamento su infrastrutture più efficienti possibile. La pandemia e le restrizioni messe in atto per contenerla hanno dimostrato che la connettività informatica è vitale per l'economia e la società. Questo significa da un lato cercare le opportunità di innovazione necessarie ad efficientare le telecomunicazioni del Paese, dall'altro prevenire rischi e minacce cibernetiche, operando un controllo dei vari fornitori di servizi del settore in questione.

In occasione di un incontro bilaterale del 4 settembre 2019, il premier Giuseppe Conte ha smentito il presidente americano Donald Trump che aveva precedentemente affermato di "aver parlato con l'Italia" e di aver saputo che questa avrebbe chiuso a Huawei ed al 5G cinese. Il presidente Conte ha negato di aver parlato di 5G con il presidente americano, aggiungendo che l'Italia gode di una delle legislazioni più avanzate in Europa in materia di sicurezza, in grado di difendere gli "asset strategici" e di far fronte a qualsiasi minaccia informatica. La versione statunitense è che il 5G cinese rappresenti una minaccia per l'Europa e che i servizi delle compagnie cinesi delle telecomunicazioni potrebbero veicolare attacchi informatici e fungere da basi per lo spionaggio. Dal canto suo l'Italia ha negli ultimi anni intensificato le relazioni con la Cina, come verrà illustrato nel prossimo paragrafo, e sta tutt'ora valutando la cooperazione con Pechino anche in questo settore. Dopo aver ripercorso gli sviluppi recenti delle relazioni sino-italiane, il report procede effettuando un'analisi generale dei vantaggi e dei rischi delle tecnologie 5G, per poi enucleare i punti critici del 5G cinese, citando, tra le varie fonti, i rapporti redatti dal COPASIR e dal CNAS.

La cooperazione tra Italia e Cina

L'Italia e le Nuove vie della seta

L'avvio del progetto cinese delle Nuove vie della seta nel 2013 ha gradualmente messo gli stati europei di fronte alla riflessione sulle possibilità e le complessità derivanti dall'iniziativa, oltre che suscitato preoccupazioni circa gli obiettivi strategici di lungo periodo di Pechino. L'Italia sembra aver effettuato una notevole apertu-

ra alla Belt and Road Initiative, la cosiddetta “Nuova via della seta”, con il Governo Conte I (1° giugno 2018 - 5 settembre 2019) sotto il quale è arrivata la firma del noto Memorandum d’intesa con la Cina. Tuttavia, è bene ricordare che già nel febbraio del 2017, in una visita a Pechino, il Presidente Mattarella presentava l’Italia come un partner solido, affidabile e ideale per gli investimenti stranieri, spiegando come “il sistema di porti e logistica italiano offra alla Cina la possibilità di completare, nel modo più efficiente e conveniente possibile, l'ultimo, prezioso tratto di questa "Nuova Via della Seta fino al cuore dell'Europa”. Lungi dall’avere esclusivamente un carattere politico quindi, il sostegno ad un coinvolgimento dell’Italia nel progetto Belt and Road Initiative è arrivato anche dalla sfera istituzionale. La cooperazione italo-cinese ha visto in seguito l’intensificarsi delle relazioni, come testimoniano le visite susseguitesi in Cina, tra agosto e settembre del 2018, del ministro dell’Economia del governo Conte I, Giovanni Tria, e del Sottosegretario allo Sviluppo Economico Michele Geraci. Il primo ha incontrato il ministro delle Finanze cinese Liu Kun e il Governatore della Banca Popolare Cinese Yi Gang, con l’obiettivo di rafforzare le relazioni in materia economico-finanziaria, mentre il secondo mirava ad intensificare la cooperazione in ambito commerciale e ad attrarre nuovi investimenti cinesi. Il sottosegretario Geraci ha incontrato esponenti della finanza, del governo e rappresentanti delle aziende cinesi, con l’obiettivo dichiarato di valutare i benefici del ruolo dell’Italia nei progetti Belt and Road Initiative e China 2025, quest’ultimo volto a diminuire il gap di industria manifatturiera tecnologica tra Cina e paesi occidentali.

Il Memorandum Italia-Cina

Culmine di questa convergenza tra Roma e Pechino è stato appunto il Memorandum d’Intesa del marzo del 2019, firmato in occasione della visita di Xi Jinping a Roma. Tale documento, pur non prevedendo clausole vincolanti per i due paesi, ha aperto alla cooperazione in vari ambiti come logistica e infrastrutture, commercio, investimenti, ambiente, connettività, start-up e e-commerce, collegando potenzialmente numerose imprese strategiche italiane con quelle cinesi, coinvolgendole nei progetti infrastrutturali della Belt and Road Initiative. L’Italia è stato il primo paese europeo, tra quelli del G7, a firmare un documento di tale rilevanza politica con la Cina, andando in controtendenza ad una tradizione diplo-

matica più cauta riguardo simili aperture. Elemento poco chiaro è il ruolo svolto nel Memorandum d'intesa dal 5G. Il 5G, ovvero le tecnologie informatiche di quinta generazione, costituendo un'innovazione tecnologica di importanza strategica, hanno risvolti decisivi anche sulla rete nazionale e sulle infrastrutture critiche. In questo settore la Cina ha compiuto importanti passi avanti, guadagnando un vantaggio anche rispetto agli Stati Uniti, da sempre leader in campo informatico. Ad oggi Pechino si appresta ad offrire al mondo servizi 5G a prezzi molto convenienti, determinati dalle politiche interne al mercato cinese che sostengono gli operatori nazionali, Huawei e Zte, che, pertanto, si ritrovano più avanti rispetto agli altri competitor, principalmente Nokia ed Ericsson. All'interno del Memorandum non si cita il 5G, ma si parla di cooperazione nell'ambito delle telecomunicazioni, elemento fondamentale se si intende sviluppare una cooperazione a livello infrastrutturale e commerciale. Tramite il ramo delle telecomunicazioni quindi, il tema del 5G è presente indirettamente nel Memorandum e quindi nelle intenzioni, se pur non vincolanti, di cooperazione tra Italia e Cina. Di conseguenza, il 5G cinese è finito sotto lo scrutinio delle istituzioni italiane ed europee.

Il COPASIR e l'Unione Europea

L' 11 settembre 2019, il Comitato Parlamentare per la Sicurezza delle Repubblica (COPASIR) approva una relazione "sulle politiche e gli strumenti per la protezione cibernetica e la sicurezza informatica, a tutela dei cittadini, delle istituzioni, delle infrastrutture critiche e delle imprese di interesse strategico nazionale", nel quale emergono diverse criticità riguardo l'usufruire dei servizi 5G di Huawei. In precedenza, l'Unione Europea, con la direttiva (UE) 2016/1148 (direttiva NIS – Network and Information Security), aveva stabilito misure di sicurezza comuni in ambito informatico, costituendo un Gruppo di cooperazione tra i paesi membri in materia di sicurezza cibernetica. Secondo la direttiva, i paesi membri sono tenuti, al fine di una cooperazione strategica europea in materia di sicurezza, a dotarsi di sistemi efficaci di sicurezza informatica, a notificare eventuali incidenti e/o minacce informatiche agli altri paesi membri e ad imporre determinati obblighi di sicurezza "agli operatori di servizi essenziali e ai fornitori di servizi digitali".

I rischi del 5G cinese

Le reti 5G garantiranno maggiore efficienza su molti fronti: una velocità di 20 volte superiore al 4G, una maggior velocità di download e la possibilità di sostenere una connessione estesa su tutto il territorio a bassissima latenza. In sostanza, il 5G aumenta la connettività di utenti e dispositivi in generale, costituendo una tecnologia strategica per il presente e l'immediato futuro, essendo ormai la connettività la chiave della maggior parte dei processi produttivi e di comunicazione. Come sottolineato dal report Securing our 5G Future del Center for a New American Security (CNAS), Il 5G non procurerà semplicemente una connessione più veloce, ma costituirà una componente vitale per le infrastrutture critiche nazionali. Pertanto, la letteratura suggerisce un atteggiamento di estrema cautela nei confronti degli operatori che si propongono di fornire i servizi 5G.

I rischi insiti nelle tecnologie 5G

Innanzitutto, va detto che il 5G presenta delle criticità in tema di sicurezza a prescindere dall'operatore che fornisca i servizi correlati: una maggiore connessione costituisce una maggiore esposizione a minacce cibernetiche dal momento che più alto è il livello di connessione, maggiore è il numero dei punti di accesso utilizzabili, con conseguente aumento delle possibilità di attacchi informatici. Considerazioni condivise dalla Relazione sulla valutazione coordinata a livello di UE dei rischi per la cybersicurezza delle reti di quinta generazione (5G) secondo cui l'aumento della dimensione software nelle tecnologie 5G porterà ad una crescente vulnerabilità complessiva, anche a causa dei maggiori rischi derivanti dal processo di sviluppo dei software, che potrebbero essere volontariamente compromessi dal principio.

Per quanto riguarda le preoccupazioni concernenti il 5G cinese nello specifico, esse sono essenzialmente due:

- il rischio connesso alle eventuali attività di spionaggio che la Cina potrebbe mettere in atto tramite i servizi forniti da suoi operatori come Huawei e ZTE;
- i dubbi circa la qualità dei prodotti Huawei e la presenza in essi di vulnerabilità e difetti di sicurezza.

Il principale fornitore: Huawei

Nel caso particolare degli operatori cinesi, si dubita, legittimamente, dell'indipendenza di questi dal governo cinese. Il quadro normativo interno della Repubblica Popolare Cinese prevede leggi

apposite (la Chinese National Intelligence Law del 2016 e la Counter-intelligence Law del 2014) che stabiliscono l'obbligo delle aziende cinesi a supportare l'intelligence nazionale e a cooperare con essa (anche fornendo informazioni). In particolare, Huawei è stata già al centro di accuse di spionaggio, come quella mossa dall'intelligence australiana nel 2018, o ancora prima da Cisco (Cisco Systems Inc, multinazionale americana nel settore informatico) nel 2003. Si accusa, ad esempio, la compagnia cinese di aver introdotto backdoors nei propri prodotti, creando così delle vie d'accesso ai network di altri paesi. L'altra criticità che l'introduzione di tecnologie Huawei comporta, come detto in precedenza, riguarda la qualità delle stesse, con particolare riferimento alla vulnerabilità del suo sistema di sicurezza, come testimonierebbe il report annuale del Huawei Cyber Security Evaluation Centre, datato 2019. Questo non implicherebbe tanto una maggiore esposizione delle infrastrutture IT allo spionaggio cinese, ma, più in generale, renderebbe i dispositivi connessi più vulnerabili a cyber attacchi di hacker indipendenti o di organizzazioni criminali.

Nel presentare rischi ed opportunità riguardanti un particolare fornitore di servizi 5G, va considerato inoltre che una volta che tali servizi vengano integrati all'interno di un'infrastruttura "critica" è pressocché impossibile separarsi totalmente da questi in un secondo momento per ripristinare la situazione ex ante. Si aggiunga, inoltre, che effettuare un monitoraggio efficace su questi servizi è assai complesso, essendo solo i fornitori, in questo caso, ad essere in possesso delle conoscenze tecnologiche per implementarli e aggiornarli. È quindi di vitale importanza valutare e filtrare i vari operatori al fine di non compromettere la sicurezza delle infrastrutture operando un controllo preventivo. In quest'ottica, il Comitato Parlamentare per la Sicurezza della Repubblica (COPASIR), notando l'aumento delle minacce cibernetiche sia a livello quantitativo che qualitativo e viste le considerazioni precedenti, valuta, nella relazione dell'11 settembre 2019, l'esclusione delle aziende cinesi per le forniture 5G.

Il rapporto del CNAS

Opportunità e rischi

Il già citato rapporto del CNAS, (2019), conferma le medesime preoccupazioni. Huawei viene presentata come un'azienda con forti

legami con l'apparato militare cinese e sostenuta dallo Stato, il quale ha sin da subito foraggiato la ricerca nel campo del 5G, in cui Huawei, secondo il rapporto, godrebbe di vantaggi al momento indiscutibili. Per molti paesi, rinunciare ai servizi di Huawei potrebbe voler dire aumentare i costi del 5G e ritardarne l'applicazione. Prospettive confermate anche in un rapporto del 2019 redatto dal GSMA, gruppo che racchiude 750 operatori telefonici da tutto il mondo, e le cui stime prevedono, in caso di totale esclusione di Huawei, un aumento dei costi delle tecnologie 5G di più di 50 miliardi di euro per l'Europa, oltre che un ritardo di 18 mesi nella loro implementazione. Tuttavia, il CNAS ribadisce i timori derivanti dai forti legami tra Huawei e il governo cinese, sottolineando come le minacce non riguardino solamente possibili attività di spionaggio. Nella società 5G i cyber attacchi andranno ben oltre il furto di dati, potendo invece recare gravi danni a strutture più complesse, compromettendo la sicurezza pubblica e i processi produttivi, laddove questi sono particolarmente digitalizzati. Si aggiunga che attraverso l'infrastruttura del 5G viaggeranno informazioni chiave per la sicurezza nazionale, concernenti l'intelligence, l'apparato militare e l'industria, prospettiva che va tenuta presente nel momento in cui occorre pensare, come accennato in precedenza, ad una cooperazione in materia di sicurezza tra i paesi europei, basata sul coordinamento e la condivisione di informazioni.

Conclusioni

La tecnologia 5G sarà presto parte integrante delle telecomunicazioni e dei processi produttivi di molti paesi. Essa costituirà l'elemento vitale che permetterà non solo la connettività, ma la competitività della stessa. Come spiegato in precedenza però, tale tecnologia porta con sé i rischi di una maggiore connettività, quindi l'aumento delle minacce possibili di attacchi informatici, motivo per il quale l'adozione di tecnologie 5G richiede anche un sistema di sicurezza informatica efficiente. Estrema cautela inoltre va operata nei confronti dei fornitori di servizi 5G a livello preventivo. Lo scrutinio dei vari operatori delle telecomunicazioni è fondamentale per evitare situazioni critiche per la sicurezza informatica nazionale. I documenti citati in precedenza, come quello del

COPASIR e del CNAS, esprimono preoccupazioni specialmente nei confronti degli operatori cinesi. I dubbi riguardo Huawei e ZTE sono legittimi, essendo la legislazione cinese poco rassicurante riguardo i legami tra il governo e le aziende cinesi. Quest'ultime sono tenute infatti a collaborare con il governo, in modi più o meno definiti, rendendo dubbio in prospettiva il rispetto di queste aziende delle normative di altri paesi in materia di privacy e sicurezza. La Cina ha guadagnato indiscutibili vantaggi nello sviluppo delle tecnologie 5G, potendo offrire anche costi relativamente bassi, costituendo per molti paesi una opportunità da cogliere. Tuttavia, la criticità del fattore 5G e la posta in gioco rendono necessaria una considerazione totale del 5G cinese, che vada oltre i potenziali vantaggi economici e che prenda in considerazione tutte le possibili minacce alla sicurezza. Infine, è da sottolineare che data la rilevanza delle infrastrutture connesse tramite il 5G, un controllo capillare andrebbe effettuato a prescindere dal possibile fornitore, poiché una gestione non adatta della tecnologia potrebbe seriamente compromettere la sicurezza del Paese.

Mattia Patriarca

Laureato in Scienze Politiche e Relazioni internazionali. Studente del corso di Laurea Magistrale in Scienze della Politica a Sapienza Università di Roma. Le sue tematiche di interesse includono la geoeconomia e la geopolitica, con un focus particolare sulla regione dell'Indo-Pacifico.

Lorenzo Termine

Dottorando presso il Dipartimento di Scienze Politiche di Sapienza Università di Roma e Research Fellow del Centro Studi Geopolitica.info per cui coordina l'attività redazionale e la ricerca in materia di Cina e Indo-Pacifico. I suoi ambiti di ricerca sono la teoria delle Relazioni Internazionali e gli Studi Strategici con particolare riferimento alla politica di difesa, alla strategia e alla dottrina militare cinesi e alla relazione strategica USA-Cina.

Il Centro Studi

l Centro Studi Geopolitica.info nasce nel 2004 con l'obiettivo di offrire un contributo al dibattito sulla politica estera, la geopolitica e le relazioni internazionali dalla prospettiva dell'Italia. Le attività del Centro Studi si articolano in tre filoni principali: la pubblicazione della Rivista online *Geopolitica.info* e la ricerca in materia di politica internazionale e geopolitica; la formazione attraverso i corsi in presenza e i corsi online sulla piattaforma www.onlineeducation.it; l'organizzazione di momenti di dibattito pubblico sui temi dell'agenda politica italiana relativi alle relazioni internazionali. Tutte le attività sono consultabili sul sito web www.geopolitica.info.

Centro Studi Geopolitica.info
www.geopolitica.info | centrostudi@geopolitica.info