5G e sicurezza. Perché l'occidente non crede all'indipendenza di Huawei

Edoardo Sarti

UNIVERSITÀ
DEGLI STUDI
FIRENZE

Research Analysis

Novembre 2019

Center for Cyber Security and International Relations Studies (CCSIRS)

Centro Interdipartimentale di Studi Strategici, Internazionali e Imprenditoriali (CCSSII)

Università degli Studi di Firenze

Via delle Pandette 2, 50127, Firenze

https://www.cssii.unifi.it/ls-6-cyber-security.html

Center for Cyber Security and International Relations Studies

5G e sicurezza. Perché l'occidente non crede all'indipendenza di Huawei

Edoardo Sarti

UNIVERSITÀ DEGLI STUDI FIRENZE

Research Analysis

Novembre 2019

Riguardo all'autore

Edoardo Sarti collabora col Center for Cyber Security and International Studies dal giugno 2019. Ha conseguito la Laurea Magistrale in "Relazioni Internazionali e Studi Europei" presso la Scuola di Scienze Politiche "Cesare Alfieri" dell'Università degli Studi di Firenze con la tesi dal titolo "Il ruolo delle organizzazioni internazionali per la cooperazione nel cyberspazio un approccio costruttivista". Nel 2019 ha conseguito il corso di perfezionamento in "Intelligence e sicurezza nazionale" presso l'Università di Firenze. La sua attività di ricerca per il CCSIRS include le Relazioni Internazionali nel cyberspazio, la cyber-diplomacy e l'analisi delle politiche nazionali ed internazionali relative al cyberspazio e alle tecnologie emergenti.

5G e sicurezza. Perché l'occidente non crede all'indipendenza di Huawei[1]

Il gigante cinese Huawei ha recentemente pubblicato un documento intitolato "Huawei's Position Paper on Cyber Security"[2], in cui indica la filosofia dell'azienda, attraverso un vero e proprio manifesto col quale suggerisce a governi, aziende e a tutti gli stakeholder le politiche necessarie per risolvere le problematiche inerenti alla cybersecurity. Tuttavia, visti sia i tempi che le modalità, il documento sembra essere più un tentativo da parte del colosso cinese di convincere i Paesi occidentali a diffidare dalle accuse di spionaggio e a non abbracciare l'invito proveniente da Washington di escludere la tecnologia cinese dai bandi per la realizzazione delle reti 5G, perché frutto di una guerra commerciale che va al di là delle questioni tecnologiche.

La difesa di Huawei

Huawei è stata duramente colpita dagli attacchi sferrati dall'amministrazione Trump. In particolare, la telco di Shenzhen, ha sofferto gli effetti delle misure adottate da Washington sia dal punto di vista tecnologico (dal momento che sui suoi dispositivi non possono essere più utilizzati servizi offerti da compagnie americane come Google) sia da un punto di vista politico-commerciale, poiché i Paesi vicini agli Usa sono sempre più diffidenti nei confronti di Huawei e

[1] La seguente analisi è apparsa su Formiche.net il giorno 19 novembre 2019 ed è reperibile al seguente link: https://formiche.net/2019/11/huawei-cyber-security-5g-usa/.

[2] Huawei, "Huawei's Position Paper on Cyber Security", novembre 2019, reperibile al seguente link: https://www-file.huawei.com/-/media/corp/facts/pdf/2019/huaweis-position-paper-on-cyber-security.pdf?la=en.

decisi a rivolgersi altrove per affidare la realizzazione e la gestione delle proprie reti 5G.

A tal proposito, Huawei ha deciso di pubblicare un nuovo documento interamente dedicato alla cybersecurity in cui vengono riportate la filosofia dell'azienda che crede che i potenziali rischi presenti nei prodotti o nei sistemi, secondo quanto si legge nel *position paper*, dovrebbero essere valutati sulla base di fattori che hanno un effetto materiale sulla sicurezza invece che su fattori geopolitici, come il paese d'origine dove viene prodotta la tecnologia. La seconda parte del white paper si concentra invece "sull'apologia" degli sforzi realizzati dalla telco di Shenzhen per fornire prodotti sicuri e affidabili, mettendo in risalto la presunta trasparenza dell'azienda, sulla cui attività non interferirebbe in alcun modo il governo cinese.

Perché è rischioso affidarsi a Huawei?

Ma allora perché, nonostante questi tentativi di dimostrare la propria trasparenza, Stati Uniti e alleati continuano a considerare la tecnologia di Huawei pericolosa?

Il primo motivo è che Pechino ha sempre considerato Huawei un "campione nazionale" al centro del progetto per la realizzazione del 5G. Nonostante l'affermazione di essere un'azienda privata, questa ha una lunga storia di supporto statale e di collegamenti con l'intelligence militare cinese. Questo aspetto non può non essere considerato rilevante se si considerano la valenza strategica di una tecnologia come il 5G e della sua importanza per lo sviluppo delle tecnologie su cui si baserà la società futura, ovvero l'Internet of Things e l'Intelligenza Artificiale. Basti pensare che, come emerso da

un'inchiesta condotta da *Bloomberg*[3], numerosi dipendenti di Huawei hanno collaborato (e collaborano ancora) a progetti di ricerca a stretto contatto con il personale delle forze armate cinesi. In particolare è emerso come, nell'ultimo decennio, i lavoratori di Huawei hanno collaborato con membri di vari organi dell'Esercito di liberazione popolare (PLA) in almeno 10 progetti di ricerca che vanno dall'intelligenza artificiale alle comunicazioni radio. Tali progetti includono anche uno sforzo congiunto con il ramo investigativo della Commissione militare centrale – l'organo supremo delle forze armate cinesi – per estrarre e classificare le emozioni nei commenti video online e un'iniziativa con l'élite della National University of Defense Technology per esplorare le modalità di raccolta e analizzare immagini satellitari e coordinate geografiche.

La posizione dell'UE

A proposito delle minacce e i rischi relativi al 5G, il report del *NIS Cooperation Group* "EU coordinated risk assessment of the cybersecurity of the 5G networks" individua quattro maggiori minacce: interruzione dei servizi 5G a livello locale o globale, spionaggio, modifica o reindirizzo di dati e distruzione delle infrastrutture digitali o dei sistemi informatici. La giustificazione dell'allarme lanciata dagli analisti europei si basa sulla consapevolezza che, nonostante questi attacchi siano già ampiamente condotti attraverso gli strumenti cyber, un attacco contro una rete 5G potrebbe causare danni dirompenti in grado di minacciare la sicurezza nazionale, la sicurezza pubblica e avere effetti deleteri sui settori critici, in particolare quelli che compongono le future. Il rischio che le vulnerabilità delle reti, inserite

[3] Bloomberg, "Huawei Personnel Worked with China Military on Research Projects", 27 giugno 2019, reperibile al seguente link: https://www.bloomberg.com/news/articles/2019-06-27/huawei-personnel-worked-with-china-military-on-research-projects.

intenzionalmente o meno, possano essere armate e usate contro gli Stati in uno scenario di crisi o di guerra non è solo fantasia. Per questo lo stesso report del *NIS Cooperation Group* avverte che i fornitori stessi in certe circostanze possono essere considerati attori pericolosi, specialmente se utilizzati da uno Stato per accedere alle infrastrutture critiche avversarie.

Il 5G: da minaccia a opportunità

Queste minacce e questi avvertimenti spiegano perché il 5G debba essere realizzato attraverso un approccio che sin dall'inizio escluda fornitori pericolosi, richieda il rispetto di determinati standard di sicurezza e test scrupolosi. Per questo, in un momento di difficoltà come quello che sta affrontando Huawei, il Position Paper rappresenta un vero e proprio tentativo dell'azienda stessa di convincere i Paesi e i governi che ancora dubitano della trasparenza della telco di Shenzhen, al fine di evitare la messa al bando di prodotti cinesi. Tuttavia, al di là del caso specifico, il dibattito sul 5G e Huawei, potrebbe rappresentare un'opportunità più unica che rara per l'Europa e l'Italia in particolare: ripensare l'indotto industriale nel settore dell'alta tecnologia, favorendo i campioni nazionali, non attraverso mere scelte autarchiche (che per certi versi vengono portate avanti sia in Cina che in altri Paesi, anche occidentali) ma tramite la volontà politica di perseguire la scelta strategica di creare strumenti sicuri, o quanto meno controllabili e certificabili sin dalla progettazione.

Center for Cyber Security and International Relations Studies (CCSIRS)

Centro Interdipartimentale di Studi Strategici, Internazionali e Imprenditoriali (CCSSII)

Università degli Studi di Firenze

Via delle Pandette 2, 50127, Firenze

https://www.cssii.unifi.it/ls-6-cyber-security.html