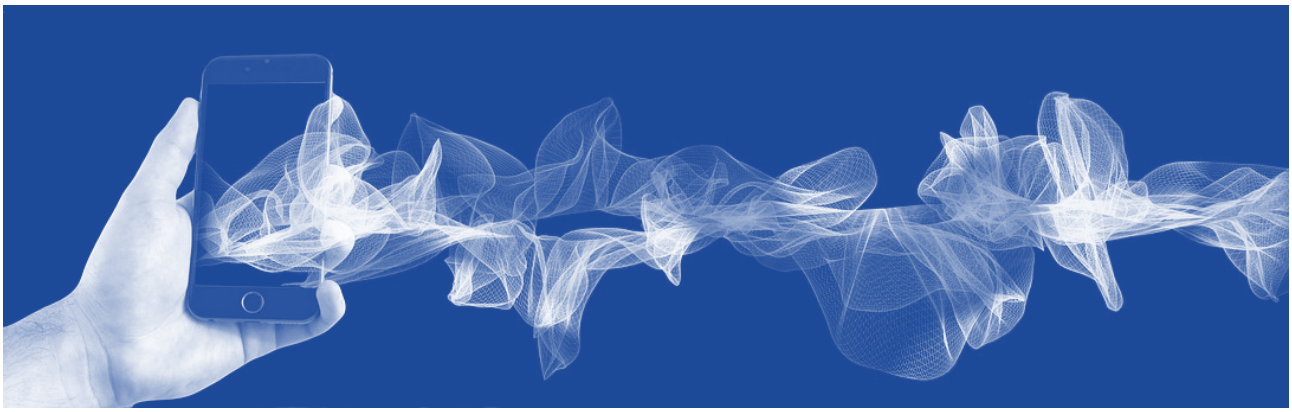
UNIVERSITÀ DEGLI STUDI DI ROMA TOR VERGATA
Centro Studi in Intelligence Economica e Security Management
Dipartimento di Ingegneria dell'Impresa

IL 5G:
TRA INTELLIGENCE ECONOMICA E SECURITY



A cura di

Francesco Farina[1], Massimo Giannini[2], Bruno Pellero[3]

[1] **Direttore esecutivo CeSIntES**
[2] **Coordinatore scientifico CeSIntES**
[3] **Comitato tecnico CeSIntES**

CeSIntES - Università degli Studi di Roma Tor Vergata
CASALE 6 - Viale Guido Carli snc - 00133 Roma
C.F. 80213750583 - Partita I.V.A. 02133971008

IL 5G: TRA INTELLIGENCE ECONOMICA E SECURITY

Sempre più alla ribalta della cronaca le discussioni attorno alla tecnologia 5G, la rivoluzione nella velocità di trasferimento dei dati via etere che sta impegnando studiosi, strateghi e politici delle maggiori potenze mondiali. In breve far circolare e scambiare in tempi velocissimi enormi quantità di informazioni in formato digitale (compresi audio, video e immagini) a distanza.
Una discussione che rischia di essere quasi obsoleta se si pensa che la Cina starebbe lavorando già dal 2018 al 6G, per dargli implementazione a partire dal 2020, ed è già in fase di studio sul 7G, per evolvere, come sostiene Neil McRae (Chief Architect di rete della Soc. British Telecom (BT)) ad un potenziamento o convergenza del 5G con le reti satellitari.

Ad oggi il mercato potenziale dice che se si vuole realizzare il 5G, gran parte della tecnologia dovrà passare dalla Cina. Aziende cinesi partecipano a tutte le sperimentazioni italiane e non solo, e sul fronte del business confidano, giustamente, di rientrare degli investimenti fatti in ricerca e sviluppo producendo e vendendo tecnologia 5G alle aziende e alle PA di tutto il mondo, e contribuendo a costruire le architetture di rete mondiali.
La reputazione cinese però, di "attitudine allo spionaggio" economico ed industriale, rappresenta un forte disincentivo alla partnership con le sue aziende, e certo non contribuisce a far diminuire le perplessità il fatto che le aziende cinesi o che operano in Cina vengono obbligate ad una stretta "collaborazione" con i loro Servizi.
Perplessità che per tutti gli altri Paesi, Italia in primis, rischiano alla lunga di diventare un alibi se non si è in grado di proporsi come alternativa, o di dimostrare concretamente eventuali sospetti e rischi collegati alle tecnologie prodotte dai cinesi.
Il problema reputazionale è difficile da superare, ma nel contesto politico ed economico attuale non si possono nemmeno trascurare gli accordi economici con la CINA che tutti i paesi hanno stipulato o stanno stipulando, vedi "Via della Seta", piuttosto che gli importanti investimenti in titoli di Stato di altri paesi che il governo cinese ha sostenuto e "mantiene" in questi anni.
Mentre Stati Uniti, Australia, Nuova Zelanda, Giappone e Repubblica Ceca, tra gli altri, hanno imposto restrizioni all'uso di soluzioni 5G della più importante e conosciuta delle cinesi, Huawei, a tutela della sicurezza nazionale, l'Europa è in fase di riflessione.

Ci troviamo quindi e senza ombra di dubbio a cavallo tra intelligence economica e Security, ma l'impressione è che il ritardo si sia accumulato su tutti i fronti: nella ricerca sul 5G, nei servizi e processi avanzati che le aziende potrebbero realizzare, ed infine sulla sicurezza nell'utilizzo della tecnologia.
Un gap tecnico, quantitativo e temporale che stacca tutti gli altri Paesi dalla Cina, in termini di investimenti e soprattutto di opportunità temporale nel quale questi sono stati fatti e danno frutti.
Di certo oggi c'è solo il protocollo che identifica o meglio delinea le caratteristiche tecniche che il 5G o quinta generazione della telefonia mobile deve possedere per essere considerato tale.

L'ITU (International Telecommunication Union), ovvero l'Organizzazione internazionale che si occupa di definire gli standard nelle telecomunicazioni e nell'uso delle onde radio, ha stabilito che per parlare di 5G:

- ogni cella dovrà sostenere una banda di picco di almeno 20 Gbps in downstream e 10 Gbps in upstream, rispetto ad 1 Gbps attuale
- deve consentire la connessione di 1 milione di dispositivi per km quadrato
- gli operatori di telecomunicazioni dovranno disporre di almeno 100 MHz in frequenza, con la possibilità di scalare fino a 1 GHz
- la latenza, in condizioni ideali, non dovrà superare i 4 ms e con le connessioni URLLC (ultra-reliable low latency communications non dovrà superare 1 ms. Allo stato attuale le reti 4G consentono una latenza solitamente pari a 70-100 ms

Quello che non è stato ancora protocollato sono i requisiti di base o standard di sicurezza che le tecnologie 5G devono avere ma si può contare che saranno non inferiori a quelli del 4G.

L'aggiornamento della "Golden Power" con i "Poteri speciali inerenti le reti di telecomunicazione elettronica a banda larga con tecnologia 5G", ha esteso il raggio d'azione dalla partecipazione azionaria alla «stipula di contratti o accordi aventi ad oggetto l'acquisto di beni o servizi relativi alla progettazione, alla realizzazione, alla manutenzione e alla gestione» delle reti 5G, «ovvero l'acquisizione di componenti ad alta intensità tecnologica» funzionali alla rete stessa, se «posti in essere con soggetti esterni all'Unione europea», sono soggetti agli obblighi di notifica. Di fatto tutti gli operatori di telecomunicazioni che intendono acquisire beni e servizi relativi al 5G da Paesi extra UE lo devono comunicare alla Presidenza del Consiglio che potrà valutare se esercitare il veto sull'operazione oppure vincolarla con particolari prescrizioni o condizioni.

In termini di Intelligence Economica parliamo di una misura per tutelare la sicurezza di un Paese, intervenendo in quei settori o, in questo caso, tecnologie che hanno maggiore valenza strategica in termini di complessità e correlazione sistemica.
Ma in termini di Security la "Golden Power", è certamente inquadrabile come "misura passiva di opposizione", perché rallenta l'azione della eventuale minaccia, in attesa che la collaborazione con altre misure la neutralizzino ovvero impediscano che si concretizzi il rischio.

Ma quali sono le altre misure? Non affrontare il rischio è plausibile soltanto con il non effettuare l'innovazione di prodotto o di processo che la genera, eliminandone però anche i benefici che la stessa porta con se. Chiudere alla tecnologia "extra UE" sul 5G rischia di tradursi in rinunciare ai benefici offerti dal 5G proprio per mancanza di competizione credibile.

L'Intelligence Economica deve lavorare alla sicurezza coniugandola con la competitività economica di un Paese; ciò significa che può e deve supportare la ricerca e sviluppo nazionale, a patto che questa abbia parità di benefici.
Ci troviamo in queste condizioni?

In Italia non esistono realtà o competitor attualmente all'altezza, mentre a livello europeo, Eriksson e NOKIA, soprattutto in seguito al freno a mano "Trumpiano", iniziano ad acquisire il "fisico" del competitor globale ma riusciranno a competere sul piano dei tempi e dei costi di implementazione?
Intelligence Economica significa sedersi al tavolo e porsi nelle condizioni di trattare o meglio di competere; non si possono chiudere gli occhi davanti all'innovazione di altri paesi ne ci si può alzare o non partecipare ai tavoli di concertazione e di confronto perché non si possiedono mai le informazioni conoscenze e competenze per potersi confrontare.
In assenza di eccellenza "industriale" italiana occorre lavorare per l'eccellenza dei processi da parte delle aziende e dalla PA italiana favoriti dal 5G; Rispondiamo ad un evidente gap sulla parte "industriale" e di innovazione almeno sulla architettura di sicurezza.
Ogni innovazione tecnologica porta sempre conseguenze nei sistemi collegati o paralleli, benefici o condizionamenti o interferenze positivi e negativi a seconda dei casi.
L'approccio all'innovazione dovrebbe sempre essere preceduto da una ponderata ed equilibrata analisi di scenario per le opportunità ed i rischi generabili, non tanto e non solo in ottica di ritorno degli investimenti, ma anche relativamente alle conseguenze sulle organizzazioni e sulla società.
Nel contesto che stiamo analizzando, dubbi, incertezze e paure relativamente ai rischi cui ci si sta esponendo sono state abbastanza puntuali, meno puntuali sono le risposte nell'assessment ovvero nella valutazione di questi rischi generati e generabili.
E data la premessa al di là della strategia di intelligence economica che un paese può adottare, proviamo almeno a capire come utilizzare in sicurezza le tecnologie esistenti, ovvero proviamo a definire un protocollo di regole e criteri oggettivi che tali tecnologie devono superare per poter essere utilizzate dalle compagnie di telecomunicazioni di un Paese.

Ma essendo proprio la "velocità" il miglior beneficio ma potenzialmente anche il maggior rischio del 5G, altrettanto rapidamente occorre trovare delle risposte oggettive.
Occorrono risposte concrete ai ragionevoli timori su eventuali effetti dannosi sulla salute umana dalle caratteristiche delle onde elettromagnetiche che caratterizzano il 5G e risposte sulle ripercussioni che l'uso di questo sistema di trasferimento dati e questa tecnologia da un punto di vista di sicurezza aziendale, personale e di sicurezza paese.

ANALISI DEL RISCHIO "5G"

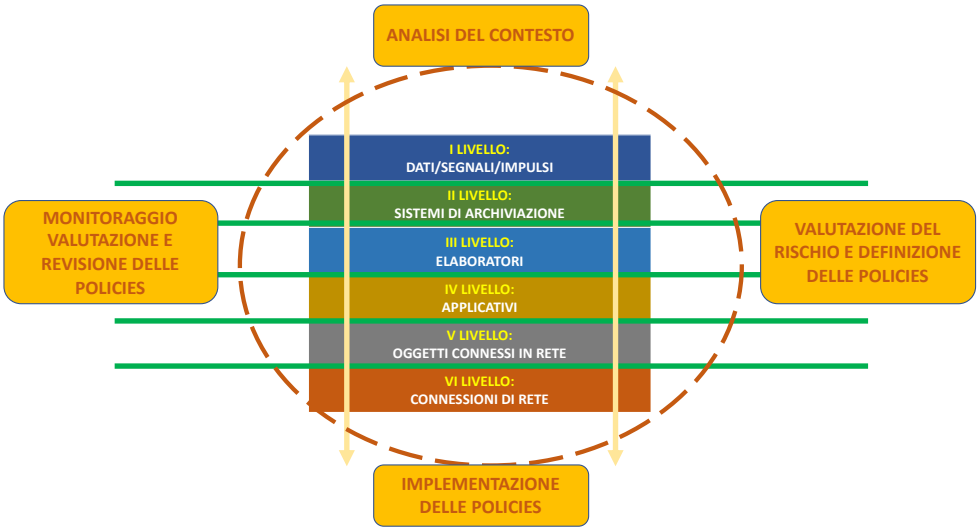
Per parlare di sicurezza dobbiamo necessariamente entrare nell'ottica di analisi del rischio, a partire da una analisi del contesto, fino alla valutazione della policy proposta per il trattamento del rischio; la scelta sarà se affrontarlo oppure evitarlo non effettuando un determinato processo o non implementando quella determinata innovazione che lo può generare. In estrema sintesi, e considerate anche le opportunità, arriveremo a:

- Accettare il rischio perché lo possiamo gestire
- Non accettare il rischio perché non siamo in grado di strutturare una policy per poterlo gestire

Nel caso del 5G accettare il rischio significa adottare la quinta evoluzione dei sistemi di trasferimento di dati e segnali, andando ad affrontare eventuali vulnerabilità sulla sicurezza come effettuato progressivamente su 2G a 3G, e poi a 4G, tutti con falle più o meno importanti di sicurezza via via scoperte e quasi sempre risolte.
Non accettare il rischio potrebbe significare rinunciare in tutto o in parte al potenziale dell'intelligenza artificiale, della realtà virtuale della realtà aumentata, della robotica, di tutti gli oggetti connessi dell'Internet of Things e della sensoristica o di quella che abbiamo definito "Intelligence of Everything" [4].
Accettare il rischio significa affrontare cospicui investimenti ed importanti sforzi economici, per costruire una nuova "dorsale" della comunicazione mobile, dalla quale non si può recedere a cuor leggero.
Certamente, come nella composizione di quei pacchetti di investimento finanziari a rendimento garantito, occorrerebbe trovare una giusta composizione che permetta di coglierne le opportunità, tenendone però il rischio sotto controllo.

Come facilmente riscontrabile dalle cronache, hackerare un dispositivo mobile significa violare privacy delle comunicazioni (vedi messaggi), posizione geografica del consumatore, oltre che i dati contenuti sul dispositivo e, magari, riuscire ad attivare il microfono e/o la telecamera dell'apparecchio.
Gestire il rischio generato dal 5G significa individuarne le vulnerabilità di tutte le componenti della struttura o architettura di funzionamento e definire delle policies per cautelarsi dalle minacce che di queste potrebbero approfittare.

[4] Francesco Farina a "Gli Stati Generali dell'Intelligence Economica" – Internet of Everything: governance dei rischi e delle opportunità. Roma 02 marzo 2017. "attività di ricerca e analisi di dati e informazioni provenienti dalle "cose", e dall'insieme di relazioni e processi da queste alimentati, finalizzata a sfruttare i benefici generati o a contrastare le minacce implicite per la competitività e sicurezza economica di stati e aziende.



La nostra impostazione ci porta a ragionare su una security "multistrato" con valutazioni asimmetriche di obbiettivi da osservare prima come esposizioni e poi come minacce a seconda del livello e del mandato di "tutela" del "risk manager" di turno.

Il primo passo abbiamo detto essere l'analisi di contesto, che in questo caso deve identificare tutte le esposizioni che in esso si manifestano; quindi tutto ciò che deve essere tutelato dalle minacce che possono arrivare dall'uso del 5G o delle tecnologie ad esso correlate.

1. L'esposizione primaria, ovvero l'oggetto del desiderio di chi cerca di violare i sistemi informatici nei più svariati modi possibili, sono certamente i dati, per un beneficio economico piuttosto che per arrecare un danno ad un qualsiasi competitor, piuttosto che per atti criminali o terroristici. Dati che possono essere di qualsiasi tipo, personali, riservati, immagini, audio, video, etc. ma anche segnali o stimoli che azionano o comandano apparecchiature e sistemi di vario tipo connessi in rete.

   Il dato è l'esposizione primaria, ma allo stesso tempo è portatore di minaccia per l'Organizzazione che, per il fatto stesso di possederlo deve tutelarsi da azioni malevole volte ad impossessarsene, modificarlo o cancellarlo.
2. Il secondo livello di esposizione è il luogo fisico o virtuale in cui il dato viene conservato, server fisici e virtuali. I server raccolgono dagli elaboratori che pertanto nell'ambito del processo di scambio dei dati devono essere osservati come elemento di minaccia rispetto alla difesa dei server.
3. Il terzo livello sono gli elaboratori, i telefonini, i tablet, che lavorano e riclassificano i dati per poi salvarli su memoria interna o passarli ai server di raccolta. Gli elaboratori devono a loro volta tutelarsi dagli applicativi che trattano i dati ricevuti e trasmessi da ai dispositivi.
4. Il quarto livello sono gli applicativi che trattano i dati all'interno degli elaboratori ricevuti dai dispositivi in rete e dal web.
5. Il quinto livello sono tutti i dispositivi che ricevono e trasmettono dati in rete, il mondo IOT.
6. Sesto ed ultimo livello la tipologia di connessione e la tecnologia ad esso correlata.

Una security "multistrato" che alzerebbe certamente il grado sistemico di difesa, e ci fa riflettere sul fatto che il 5G più che portare nuove minacce amplifica lo spazio d'azione di minacce esistenti e certamente agisce sull'impatto dei rischi che possono concretizzarsi perché si diversificano i processi e le attività che tramite 5G possono essere gestiti.

Aumenta chiaramente la rapidità di circolazione dei dati e pertanto il numero dei dati che possono essere violati rubati e modificati a parità di tempo.

Se il 5G può permettere però a mezzi pubblici e automobili di essere guidati da remoto senza nessuno alla guida, o di effettuare operazioni chirurgiche tramite robot guidati a distanza, o di pilotare una intera catena di montaggio, o di controllare un intero sistema di distribuzione di gas o energia, quello che sta aumentando nella canonica formula per la determinazione della magnitudo dei rischi è innanzitutto l' "impatto", la dimensione economica dell'esposizione, dei triliardi di dati sensibili movimentati o custoditi.

Viene da sé che un hacker o attaccante che dovesse prendere il controllo di uno di questi processi potrebbe creare un danno potenzialmente enorme.

La probabilità rimarrà sostanzialmente collegata alle solite variabili, frequenza (gli attacchi non subiranno modifiche sostanziali ma aumentando le esposizioni cresceranno indubbiamente in termini numerici complessivi) e la vulnerabilità, inversamente proporzionale all'efficacia delle misure di opposizione messe in atto (aumenta l'impatto, aumenta il rischio e deve aumentare l'efficacia delle misure messe in atto per ridurre le vulnerabilità fisiche, logiche ed organizzative delle Organizzazioni).

Tante le minacce o strumenti di minaccia che agiscono tra i livelli, attacchi Ddos, Sniffing, Spoofing, Botnet, Malware, Ransomware, Back Doors, attacchi Man In The middle.

Ed è soprattutto sulle back doors che si muovono i sospetti ed i timori sulla sicurezza delle tecnologie Cinesi 5G, mentre per i sistemi precedenti le eccezioni sono state sollevate non per vizi volontari ma per vulnerabilità rilevate segnalate all'Azienda di turno.

I problemi di vulnerabilità riscontrati nel 4G furono rilevati essenzialmente nei tre protocolli per associare i dispositivi alla rete, per ricavarne le informazioni, e per disconnettere il dispositivo.

Rispetto al timore di back doors non esiste ad oggi riscontro ufficiale di tecnologie americane, svedesi, finlandesi o cinesi che nascano con il peccato originale di possedere cavalli di troia pronti a raccogliere comunicazioni e dati che viaggiano con il 5G.

Rispetto alla principale azienda cinese non le hanno rilevate ad oggi in 5 anni di verifiche dell' Oversight Board al **HUAWEI CYBER SECURITY EVALUATION CENTRE** (Centro creato da Huawei nel Regno Unito per le valutazioni di sicurezza nell'utilizzo delle tecnologie fornite da Huawei)[5]; non le

[5] Controllato da un "Oversight board" istituito nel 2014, che è presieduto dal direttore generale dell'NCSC, comprende un alto dirigente di Huawei in qualità di vicepresidente, nonché rappresentanti di alto livello del governo e del settore delle telecomunicazioni nel Regno Unito. Attraverso la HCSEC, il governo britannico raccoglie informazioni sulle strategie e sulle tecnologie di Huawei commercializzate nel Regno Unito, supportato dal National Cyber Security Centre (NCSC), e in precedenza Government Communications Headquarters (GCHQ)), in qualità di autorità tecnica nazionale per la sicurezza informatica e principale agenzia operativa governativa per la sicurezza informatica.

rileva ad oggi il **CCDCOE**[6] (The NATO Cooperative Cyber Defence Centre of Excellence), che pur sollevando i dovuti alert non può produrre ad oggi prove oggettive a supporto.

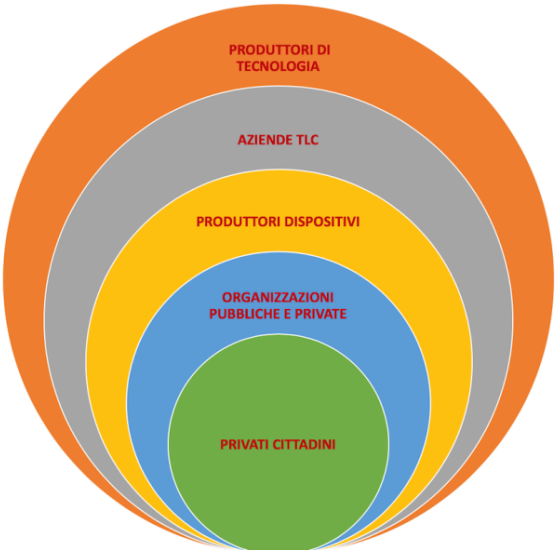
I rischi ovvero la diretta conseguenza del concretizzarsi delle minacce che sfruttano le vulnerabilità del contesto, a livello generale possono essere:

- **esfiltrazione di dati**
- **modifiche non autorizzate di dati**
- **trasmissione non autorizzata di segnali**
- **perdita di dati**
- **intercettazione Comunicazioni**
- **furto di identità / frodi**
- **blocco delle comunicazioni a livello periferico**
- **blocco delle comunicazioni a livello centrale**

Le vulnerabilità si riducono con l'adozione di misure di opposizione, una "cassetta degli attrezzi" da cui attingere, con all'interno misure attive passive e organizzative o di sicurezza fisica, logica o cyber ed organizzativa cui attingere per ridurre le vulnerabilità del contesto.
Misure che devono necessariamente operare in combinazione perché le misure passive rallentano gli attacchi ma non li fermano e hanno necessità di misure attive che segnalino l'eventuale attacco, ed organizzative che attraverso formazione, procedure ricerca, test, ecc. completino la policy difensiva mettendo le persone preposte nelle condizioni di operare in modo corretto con gli strumenti più adatti per fermare o limitare i danni dell'attacco.
Firewall, antivirus, antimalware, penetration test, formazione dedicate, procedure operative, aggiornamenti software, sono alcune delle misure utilizzabili in ambito informatico, ma anche misure di sicurezza fisica quali sistemi antintrusione, strong authentication, sistemi di videosorveglianza etc.

Ma volendosi focalizzare sul contesto sesto livello, quello della tipologia di connessione, proviamo a sintetizzare quali effettivamente possono essere le vulnerabilità collegate alla futura modalità di connessione, in particolare a nuove vulnerabilità rispetto al 4G, o a evoluzioni di vulnerabilità già previste nel 4G e non ancora risolte, o soggette a mutazione.
Ogni componente del sistema coinvolta deve fare la propria analisi e determinare le proprie policies di sicurezza, trattando i rischi che lo coinvolgono direttamente e contribuendo alla gestione del rischio residuo che per il suo operato potrebbe trasferire agli altri anelli della catena.
Una security stratificata che dato l'alto livello di complessità e correlazione non può non prevedere misure di security di sistema che interessino tutte le componenti fino a misure dedicate, per i produttori piuttosto che per organizzazioni pubbliche e private o cittadini che utilizzano la tecnologia e la rete.

[6] Huawei, 5G and China as a Security Threat – di Kadri Kaska, Henrik Beckvard and Tomáš Minárik



Misure minime obbligatorie per chiunque voglia produrre o fare uso di determinate tecnologie o applicativi che possono in qualche modo avere vulnerabilità che aprano a conseguenze di rilevanza sistemica, misure tecnologiche come organizzative.
Tra le misure di organizzative andrebbe colmato quel "buco nero" che ancora esiste in termini di educazione e formazione a chi utilizza la rete a qualsiasi livello.
Tra le misure di maggiore efficacia va certamente considerata quella di rendere inutilizzabili o immodificabili i dati, di modo che anche nel caso in cui l'attaccante riesca ad accedervi illecitamente non li possa utilizzare perché non ne possiede le chiavi per poterli decodificare. Parliamo di cifratura, che può servire sia per conservare i dati sia per scambiarli in modo totalmente protetto, purché il dispositivo che trasmette non sia corrotto e permetta all'attaccante la lettura prima che avvenga la cifratura.

DALLA TEORIA ALLA PRATICA: QUALE RISPOSTA DI ANALISI DEL RISCHIO SU UNA RETE DI COMUNICAZIONI ELETTRONICHE 5G.

Questa analisi non si prefigge di essere estremamente dettagliata né esaustiva ma solo di aprire la strada per future più dettagliate analisi che possano essere partecipate dall'industria e dalle istituzioni e concorrere alla definizione delle policies di sicurezza da adottare.

Non è possibile parlare genericamente di "*rischi potenziali alla sicurezza dovuti al 5G*" senza individuare e ragionare sugli asset che si intende proteggere, ovvero come sopra descritto:

- i "dati" (cioè il contenuto informativo scambiato tra sistemi informatici)
- le "comunicazioni" (la corrispondenza tra uomini o macchine)
- la "continuità del servizio pubblico"

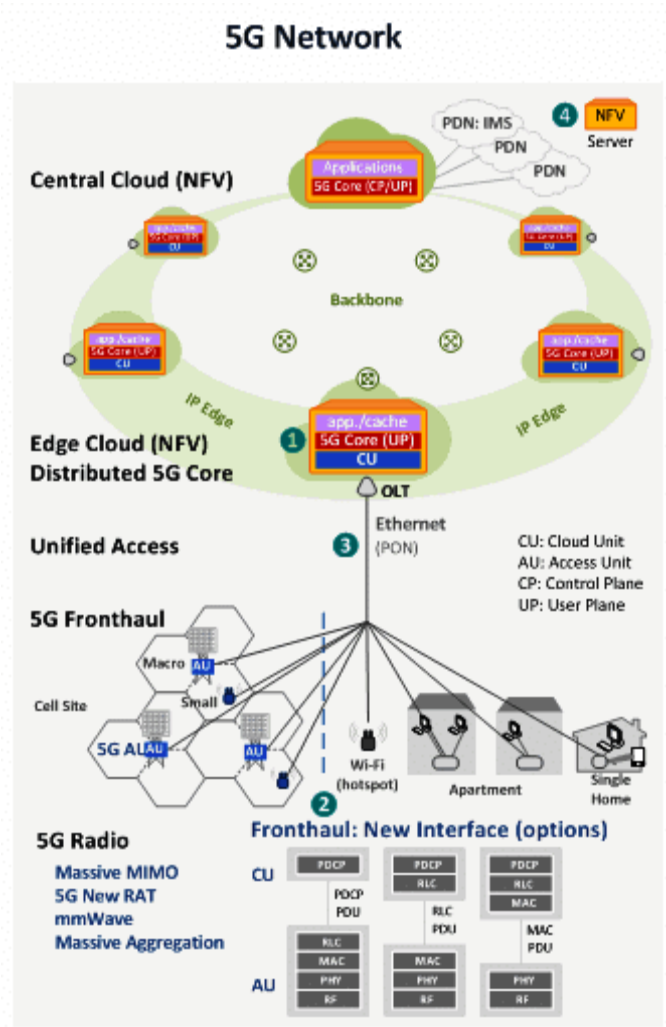
Per ciascun asset sarà quindi possibile individuare le minacce, verificarne la concretezza, l'impatto e le misure di protezione da adottare.

Si potrebbero cosi individuare, in estrema sintesi, i rischi connessi agli assets:

- di "esfiltrazione di dati sensibili"
- di intercettazione non autorizzata di comunicazioni
- di modifica delle condizioni di funzionamento / spegnimento di una o più BTS
- di modifica dei piani di routing, dei piani di numerazione, dell'identità (elettronica) delle utenze, ecc.
- di modifica delle condizioni di funzionamento / spegnimento dell'intera rete

Un'analisi puntuale di tali rischi, ad oggi mancante nei documenti a sostegno delle eccezionali misure estensive della Golden Power, ma di cui non si può fare a meno, che necessita di partire dalla suddivisione della rete in aree di omogenea criticità.

Ma ragioniamo su architettura e priorità da considerare.



Prendendo ad esempio la descrizione schematica di una rete 5G[7]:
un esame sommario delle funzioni e delle caratteristiche degli elementi di rete consente di evidenziare quattro macroblocchi quale bersaglio di potenziali minacce omogenee:

1. La **Core Network**, il cuore della rete
2. La **RAN**, Rete di Accesso Radio
3. La **Rete Trasmissiva**
4. L'**Ambiente di Virtualizzazione (NFV)**

La Core Network (CN) è indubbiamente il macroblocco chiave di tutta la rete. E' ragionevole impegnarsi con misure di protezione di massima efficacia perché qualunque attacco o incidente possa coinvolgere la CN avrebbe gravi conseguenze.

La RAN è polverizzata in decine di migliaia di impianti indipendenti (o al più collegati in cascata in serie di max 8 impianti) che trasportano comunicazioni cifrate end-to-end tra ciascun terminale d'utente e la Core Network. Però l'eventuale accesso logico o fisico ad uno o più degli impianti della RAN non consentirebbe quindi di ottenere accesso in chiaro ad alcun dato o comunicazione. Inoltre, l'eventuale perdita di uno o più impianti (BTS) è comunque tollerabile per via delle ridondanze insite

[7] Immagine tratta da "*New Developments and Research Challenges for 5G*" di Frank Kataka Banaseka and Stephen Dotse, Dept. of Information Communication Technology, Radford University College, Accra – Ghana, pubblicato su International Journal of Current Research, Vo.9, Issue 02, pp.46626-46631, Feb. 2017, ISSN: 0975-833X

nell'architettura della rete cellulare, così come, la perdita di un numero significativo di impianti di uno stesso fornitore (in considerazione di un eventuale rischio connesso ad uno specifico fornitore), sarebbe comunque tollerabile; si potrebbe infatti pianificare a priori di servire i siti sensibili con impianti di fornitori diversi. Infine, l'accesso remoto per finalità di esercizio e manutenzione potrà essere protetto mediante strong authentication e cifratura delel comunicazioni di O&M in transito (avendo cura di rimuovere i certificati/chiavi di cifratura di fabbrica ed installare esclusivamente certificati/chiavi di cifratura affidabili).

La **rete trasmissiva** è certamente importante in quanto su di essa transitano i dati e le comunicazioni provenienti da ampie porzioni di rete. Tuttavia tali dati e comunicazioni transitano con comunicazioni cifrate end-to-end tra ciascun terminale d'utente e la Core Network. L'eventuale accesso logico o fisico ad un flusso della rete trasmissiva non consentirebbe quindi di ottenere accesso in chiaro ad alcun dato o comunicazione. Anche l'eventuale perdita di una direttrice della rete trasmissiva è comunque tollerabile per via delle ridondanze insite nell'architettura della rete. Si evidenzia in tal senso, che nella tecnologia 5G la bassa latenza del traffico è anche dovuta ad una peculiare dote della rete di individuare e modificare i percorsi trasmissivi in tempi ridottissimi.

L'**Ambiente di Virtualizzazione** è con la CN l'altro macroblocco chiave di tutta la rete. E' ragionevole anche in questo caso adottare misura di protezione della massima efficacia per opporsi a qualunque attacco o incidente che lo possa coinvolgere inducendo gravi conseguenze.

Da questa sintetica ma non superficiale "antifona" di analisi dei rischi di una qualunque rete 5G si può pertanto preliminarmente concludere che:

- in relazione alla Core Network ed all'Ambiente di Virtualizzazione emergono rischi da ritenersi significativi rispetto alle potenziali conseguenze legate al concretizzarsi di una minaccia o attacco. Sarebbe pertanto ragionevole **imporre l'adozione di robuste ed efficaci misure cautelative, fino all'esercizio del potere di veto di cui all'estensione della Golden Power**;
- in relazione alla RAN ed alla rete trasmissiva, le conseguenze del concretizzarsi di una minaccia o di un attacco sono ridotte, stante che dati e comunicazioni in transito non corrono rischi significativi, e il rischio per la continuità del servizio può essere trattato con l'adozione di misure organizzative semplici da specificare e porre in essere. Al fine di minimizzare il rischio conseguente ad attacco / incidente che coinvolga uno o più impianti della RAN, le misure da adottare devono essere efficaci e non trascurabili, ma non si ritiene necessario arrivare a drastiche misure restrittive fino a quelle previste dal "Golden Power" o particolari restrizioni all'origine delle tecnologie adottate.

Trattasi di ragionamenti che anche altri paesi europei stanno portando avanti, puntando a verifiche ed accertamenti che gli permettano di giungere a posizioni pragmatiche basate su riscontri oggettivi, basate su analisi dei rischi e proporzionalità delle misure adottate.

Il Regno Unito[8] come osservato per il **HUAWEI CYBER SECURITY EVALUATION CENTRE,** collabora di fatto con l'industria nell'individuare comunemente le vulnerabilità e le misure correttive; tramite l'"Oversight Board", pur non potendo raggiungere livelli di garanzia assoluta, ha modo di analizzare e segnalare eventuali vulnerabilità, anche potenziali rispetto alla loro possibile correlazione con la sicurezza delle reti inglesi, chiedendo all'Azienda di intervenire, come riscontrabile negli ultimi rapporti pubblicati per aspetti legati allo sviluppo software.

In Germania BNetzA[9], l'equivalente del nostro MiSE, non limita l'impiego di tecnologie cinesi nel 5G ma indica ed esige requisiti di sicurezza per tutti i fornitori, fornendo linee guida per il contenimento dei rischi, come ad es. la diversificazione dei fornitori degli elementi di rete. Tutte le componenti e le attrezzature che devono entrare a far parte dell'architettura di rete tedesca dovranno essere certificate a prescindere dal luogo di produzione o residenza dell'azienda. I requisiti di sicurezza che in sintesi sono di tipo:

- **Regulatory**: le regole sulla sicurezza sono da applicarsi a TUTTI i vendors, non solo cinesi
- **Procurement**: i componenti critici (da cui la necessità di distinguere quali siano critici da quelli che critici non sono) possono essere utilizzati solo se certificati dall'Ufficio Federale per la Sicurezza delle Informazioni (BSI)
- **Operations**: il personale che installa o gestisce i componenti critici dovrà anche essere anch'esso certificato dalle autorità tedesche
- **Cyber Security**: monitoraggio e gestione del rischio, il traffico di rete deve essere monitorato continuamente per rilevare eventuali anomalie e i componenti di rete e di sistema rilevanti per la sicurezza devono essere sottoposti a controlli di sicurezza regolari e continui.

La Svizzera[10] ha affidato a Huawei la fornitura delle tecnologie per il 5G.

Viene spontaneo pensare che tali paesi i ragionamenti fatti vadano oltre l'analisi del rischio prettamente tecnologico, ed abbiamo soppesato anche il rischio di "rimanere indietro", nello

[8] https://www.bbc.com/news/uk-48032286

[9] Dal sito web ufficiale di BNetzA, il Regolatore Tedesco per le comunicazioni elettroniche:
Bundesnetzagentur publishes key elements of additional security requirements for telecommunications networks
https://www.bundesnetzagentur.de/SharedDocs/Pressemitteilungen/EN/2019/20190307_SL.html?nn=404530

Information on the current BNetzA security requirements:
https://www.bundesnetzagentur.de/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/OeffentlicheSicherheit/KatalogSicherheitsanforderungen/Sicherheitsanforderungen-node.html;jsessionid=D487D3639B7F4809AC0385ADAB6E172E

BNetzA key elements of additional security requirements for telecommunications networks:
https://www.bundesnetzagentur.de/SharedDocs/Downloads/EN/BNetzA/PressSection/PressReleases/2019/20190307_SL.pdf;jsessionid=D487D3639B7F4809AC0385ADAB6E172E?__blob=publicationFile&v=2

[10] Sunrise and Huawei Jointly Announce 5G FWA Pioneer Users in Switzerland
https://www.huawei.com/en/press-events/news/2019/4/huawei-sunrise-5g-fwa-pioneer-users-switzerland

Sunrise 5G network is live in more than 150 cities across Switzerland
https://5gobservatory.eu/sunrise-launches-5g-in-switzerland-swisscom-announces-its-plan/

sviluppo del 5G e della sicurezza ad esso correlata, tema che andrebbe seriamente valutato in Italia, anche in termini e con le prerogative dell' Intelligence Economica.

L'approccio tedesco e l'esperienza anglosassone in particolare ci portano a pensare ad un eventuale **Centro nazionale o europeo**, per la valutazione dei rischi e la certificazione dei requisiti di sicurezza che devono avere i prodotti utilizzati nella rete nazionale o europea; per la definizione degli standard di sicurezza, e delle strategie anche in termini di ridondanza nelle reti. Non solo per le aziende cinesi ma per tutti i vendors di tecnologia 5G, Huawei come Eriksson, Nokia come ZTE etc.. La collaborazione da parte dei produttori e la concessione spontanea dell'accesso ed ispezione dei "sorgenti" anche in modo riservato e isolato sarebbe certamente ben visto in termini di fiducia e reputazione.

Un Centro che non potrebbe prescindere, o avrebbe efficacia limitata, senza un approccio normativo volontario e cogente, che incentivi e/o obblighi a implementare misure di sicurezza minime obbligatorie chiunque voglia produrre o fare uso di determinate tecnologie o applicativi che in qualche modo aprano a conseguenze di rilevanza sistemica.

Egualmente importante per quanto riguarda le Operations con personale "sicuro" anche la selezione e coinvolgimento del personale dedicato, con alta competenza qualificata e certificata, nulla osta di sicurezza e preferibilmente alle dipendenze dell'operatore limitando l'ousourcing.

Il Centro per ogni componente hardware / software potrebbe inoltre:

1. analizzare la struttura dell'hardware rispetto alla progettazione logica stabilendo l'equivalenza mediante test sistematici
2. per il firmware così come per gli agli componenti software, avere la disponibilità dei sorgenti (incluse le componenti fornite da subfornitori e/o terze parti), procedendo quindi all'ispezione dei sorgenti mediante tool di analisi statica e mediante analisi anche manuale di vulnerabilità; in alcuni casi (analisi dei protocolli ad esempio) si possono anche usare i cosiddetti "metodi formali" sempre al fine di analisi di vulnerabilità
3. stabilire l'equivalenza fra i binari forniti dall'operatore e i binari risultanti dalla compilazione dei sorgenti

In questo modo si potrebbe ottenere anche un notevole controllo sul processo di realizzazione degli apparati e del software relativo, in termini di gestione delle versioni e configurazioni uso di componenti commerciali (cots) oppure open source ecc.