Documento di audizione TIM sul

DL “perimetro di sicurezza nazionale cibernetica”

Avv. Stefano Grassi

Responsabile Funzione Security TIM

Presidente,
nel porgere il mio personale saluto, a Lei e agli Onorevoli componenti la Commissione, desidero, anche a nome del mio Amministratore Delegato, dott. Luigi Gubitosi, ringraziarLa per questo invito che costituisce una importante occasione di confronto tra Aziende e Istituzioni.

L’introduzione del nuovo DL 105/2019 è da accogliere come un ulteriore passo sulla strada che il Governo sta percorrendo e che vede attribuire un ruolo di sempre più elevata importanza all’interlocutore privato, rispetto agli interessi strategici del Paese.

In linea con tale indirizzo, le Istituzioni hanno focalizzato il loro intervento sul delicatissimo settore attinente la gestione delle Reti e dei Servizi, dai quali dipende l’esercizio di attività fondamentali per l’interesse dello Stato, con ampi risvolti sui settori civili, sociali ed economici del Paese,

ambiti tutti nei quali TIM, per tradizione e storia, riveste un ruolo primario.

Ritengo questa occasione di confronto, Signor Presidente, come la conferma di quanto sia fondamentale questa azione di coordinamento da parte di codesta Commissione.

Obiettivo comune, quindi, è fare "sistema Paese", aggregando, i diversi attori coinvolti in questa sfida di gestione del rischio cyber (dalle aziende che gestiscono asset strategici per lo Stato, alle infrastrutture critiche del Paese) e ponendo le basi per una *"unitaria strategia nazionale di sicurezza cibernetica"*.

Ritengo, in considerazione del processo continuo di trasformazione digitale in corso, che l'introduzione di questo nuovo Decreto - Legge sia una ulteriore fase per la realizzazione dell'architettura cibernetica nazionale, già delineata nel Piano Nazionale per la Protezione Cibernetica, del febbraio 2017, e nella Direttiva NIS del maggio 2018.

La minaccia cyber, rischio ormai pervasivo nelle società moderne, obbliga i più attenti osservatori a ridefinire il contesto in cui oggi le Aziende si muovono e che viene caratterizzato da una situazione di *"cyber guerriglia permanente",* svolta da avversari indefiniti e sconosciuti, con azioni eversive ed illecite, sempre aggiornate tecnologicamente, e altresì indirizzate – fattore innovativo – anche a furti di informazione per finalità geo-politiche.

L’apertura di tale nuovo fronte amplifica notevolmente il livello della minaccia e, di conseguenza, il rischio in rapporto all’utilizzazione di tali informazioni da parte dei cyber criminali.

Rispetto a tali scenari, quindi, in continua evoluzione, TIM quale operatore economico di servizi essenziali, sia per il settore privato che soprattutto a favore di tutta l’infrastruttura governativa, ha ormai maturato una consolidata esperienza, ponendosi, quale attore proattivo nel garantire la massima sicurezza delle proprie tecnologie.

Nel quadro di tale azione, si inserisce il lavoro svolto dall’ Organizzazione di Sicurezza di TIM, che ho il privilegio di dirigere.
La mia Organizzazione è, infatti, sempre più impegnata in una attività di continuo aggiornamento tecnico-professionale e nella ricerca di metodologie adeguate per contrastare l’evoluzione della minaccia informatica.

Lo scopo è quello di mettere in campo ed attuare misure di tutela e protezione del patrimonio interno e nazionale e rispondere, adeguatamente, al dettato governativo tradotto, negli ultimi due anni, in diverse sollecitazioni costituite dai decreti “Golden Power”, emanate a tutela delle infrastrutture tecnologiche definite come “essenziali” per la difesa e sicurezza nazionale.
Tali iniziative governative suonano come implicito riconoscimento sotto tutti gli aspetti della valenza strategica di TIM e a riguardo, quindi, si può obiettivamente affermare che l’azienda è protagonista dello sviluppo

digitale del Paese e si pone quale partner principale per gli interessi dello Stato.

A riguardo, mi permetta, Presidente, di menzionare solo qualche numero : 16 milioni di chilometri di fibra posata in Italia, 98% della popolazione raggiunta dal 4G e dal 4,5G e 6,4 miliardi di euro in investimenti industriali.

Completano il quadro oltre 48.000 dipendenti, 50.000 apparati di rete, più di 20.000 server, 36.000 siti, dei quali, 200 siti strategici, 8 data center, 10.800 km di cavi sottomarini, 900 applicazioni informatiche.

Rispetto all'obiettivo di assicurare la protezione di una tale dimensione patrimoniale, TIM, da molto tempo, ha perfezionato lo sviluppo di un adeguato modello operativo di cyber security, proporzionato alle potenziali minacce ed alla complessità tecnologica che deve gestire.

Nel quadro di tale forte risposta, sia a livello tecnico che organizzativo dell'azienda occorre collocare, nell'ambito della Direzione Security, il presidio diretto del rischio Cyber.

In tale contesto, riassumendo a grandi linee l'azione svolta, evidenzio, che è stato attuato, ormai da anni, un processo di ICT Risk Management, mirato alla valutazione e al trattamento dei rischi operativi sugli asset ICT.

Tale approfondita analisi, estesa e trasversale su tutta l'azienda, viene svolta in costante e sinergica collaborazione con le linee operative interne, ed è finalizzata a garantire la

completezza del processo di valutazione del rischio per ciascun asset inscritto in tale perimetro, con esame puntuale del grado di adeguatezza delle misure previste a protezione degli stessi.

Presidente, mi consenta, anche in questo caso, di fornire qualche numero per offrire alla Commissione elementi informativi sotto l'aspetto dimensionale e che definiscono quanto viene gestito in TIM.

Ad oggi sono stati individuati circa 3.000 asset: di questi, in esito alla classificazione del rischio riferita a ciascuno di loro, ne sono stati individuati 800, catalogati come a "criticità elevata" in funzione della tipologia delle informazioni trattate e dall'esposizione sulla rete internet.

Ulteriore attenzione e cura viene, pertanto, attribuita a questo particolare sottoinsieme entro il quale, evidentemente, rientrano anche gli asset attinenti il perimetro Golden Power (circa 40 piattaforme strategiche per il sistema di difesa e sicurezza nazionale), tra cui quelle di esclusivo uso al Comparto Intelligence.

Forte quindi è l'azione finalizzata al controllo prestazionale e di funzionamento di tali reti fisse e mobili, traducibile in circa 12.000 azioni di perfezionamento dei livelli di sicurezza svolte solo nel corrente anno.

Al contempo, sono stati incrementati i volumi di attività di controllo che, date le crescenti complessità tecnologiche, in futuro, dovranno sempre più basarsi su processi

automatizzati e guidati anche da logiche di "*threath intelligence*".

Anche in questo caso, ritengo utile fornire qualche numero di riferimento: incremento delle attività di controllo del 73% nel 2018, che hanno visto, in particolare, accresciuti, i controlli sulle applicazioni di oltre il 114%.

Sempre per offrire un quadro dell'azione svolta da Security, si evidenzia l'estremo impulso dato alla protezione delle reti dalle principali minacce (virus, malware, hacker, furto di dati, attacchi ddos), rispetto l'ampia tassonomia degli attaccanti (Cyber- Criminals, Cyber- Terrorists, Insiders, ecc.).

Nell'ambito di tale azione di protezione e contrasto, un ruolo fondamentale viene svolto in affiancamento al processo di ICT Risk Management, dalla struttura Cyber- Security, articolata nel Security Operations Center (SOC) e nel Security Lab.

Il SOC opera all'interno di TIM ed è impegnato nel monitoraggio H24*365 gg. del perimetro già indicato, finalizzando la propria azione nell'identificare con immediatezza e gestire gli incidenti di sicurezza informatica, in modo da contribuire, tempestivamente, al contenimento dei derivanti impatti.
Tale SOC lavora in sinergia con il Security Lab, struttura quest'ultima che, dialogando con una serie di interlocutori interni ed esterni all'azienda, studia costantemente le

evoluzioni delle minacce e raccoglie puntualmente una serie di “Indicatori”.

Il combinato di tali azioni aumenta le probabilità di poter rilevare, nei tempi più brevi possibili, le tracce di eventuali attacchi ai sistemi Aziendali, favorendo la più pronta reazione, con punte di efficienza, ad esempio nel caso di attacchi di DDOS, caratterizzati da riconoscimento in un tempo medio tra i 10 – 15 minuti.
In relazione, sempre per fornire qualche elemento di valutazione connesso a quanto sopra rappresentato, nel corso del corrente anno sono stati identificati in TIM circa 1,2 incidenti ogni ora e un trend in generale in crescita, con un aumento percentuale di quasi il 18% rispetto ai dati rilevati nel 2018.

In tale scenario, di per sé già complesso, si inserisce, ad oggi, anche la nuova tecnologia del 5G, che rappresenta una innovativa e stimolante sfida per TIM, con potenzialità enormi dal punto di vista dello sviluppo di mercato e dei servizi commerciali/sociali/industriali per il cliente, ma con sensibili risvolti di sicurezza, che l’azienda è pronta a gestire e presidiare.

Per meglio comprendere i risvolti connessi all’evoluzione del 5G, si pensi, ad esempio, ai vantaggi offerti dall’architettura cloud, per la quale, viceversa, sotto il profilo della sicurezza diventa centrale la definizione di processi di controllo inter-company; il traffico not-Human e le potenzialità offerte dall’end to end, rispetto ai quali sarà dirimente individuare

opportune soluzioni di sicurezza sia per la certificazione dei dispositivi utente che degli apparati di rete - punto fondamentale su cui il DL 105/2019 pone la propria attenzione -.

Volgendo il mio intervento alla conclusione, rispetto più specificamente allo schema normativo contenuto nel DL 105/2019, nel condividere le istanze già proposte dalla nostra Associazione Asstel, vorrei sottoporvi alcuni ulteriori spunti di riflessioni.

In particolare tengo a trasmettere l'importante esperienza in corso con il Comitato di Monitoraggio della Presidenza del Consiglio dei Ministri, maturata attraverso un dialogo sempre positivo, nel quadro dei frequenti rapporti intercorsi, in relazione alle attività connesse con gli adempimenti prescrizionali disposti in materia di Golden Power.

Ritengo, evidentemente dar seguito a questa esperienza capitalizzando i frutti di questo apprezzato lavoro comune e auspico, anche rispetto all'attuazione del Decreto – Legge in trattazione, un analogo meccanismo di collaborazione.
In tal senso, vorrei esprimervi alcune osservazioni sull'opportunità di:

- Utilizzare lo specifico know-how acquisito dai laboratori TIM - in termini di competenze scientifiche, organizzative e di risorse strumentali, tecniche e tecnologiche - riconoscendogli un ruolo di supporto specialistico al costituendo Centro di Valutazione e Certificazione Nazionale –CVCN del MISE;

- fruire dell'esperienze accumulate in questi anni per la redazione dei Decreti attuativi del presente Decreto-Legge, in corso di redazione;
- evitare sovrapposizioni, nell'attività di controllo governativo sulla Società TIM, da parte di più Enti e negli adempimenti connessi alla normativa Golden Power e quella del DL 105/2019. Rispetto a quest'ultimo passaggio potrebbe, infatti, suscitare alcuni elementi di preoccupazione aziendale un complesso scenario, nel quale si preveda una doppia interlocuzione su temi e argomenti affini, connessi:

  – a quanto TIM deve effettuare per ottemperare ai DPCM 16 ottobre e 2 novembre 2017 e, in materia di 5G (DPCM 5 settembre 2019) che vedono una interlocuzione di TIM verso l'organo di controllo governativo rappresentato dal Comitato di Monitoraggio della Presidenza del Consiglio dei Ministri;
  – alle incombenze derivanti dall'introduzione del nuovo DL, verso il costituendo CVCN del MISE.

  Su questi ultimi punti, pertanto, sarebbe opportuno uno specifico approfondimento che chiarisca le modalità operative da attuare, da parte di TIM, su verso tali organi di controllo.

  Altro aspetto rilevante e da tener presente in tale quadro di riferimento, è quello rappresentato dal peculiare ruolo di TIM, quale gestore di circuiti di Reti e di Sistemi "classificati".

Tale sensibile perimetro, per l'importanza che riveste nel quadro della sicurezza nazionale, andrebbe, a mio avviso, armonizzato meglio.

Nello specifico sarebbe opportuno tale chiarimento anche in relazione al ruolo del CVCN del Mise - art. 1 comma 7 lettera a. - che prevede fra i suoi compiti quello di contribuire all'elaborazione delle misure di sicurezza per ciò che concerne l'affidamento di forniture di beni, sistemi e servizi ICT.

Ciò proprio nella considerazione che, allo stato attuale, il Decreto Legge di che trattasi, sembra orientato a prevedere per le aziende private, quale unico interlocutore il MISE, non tenendo conto di quanto disposto dalle normative nel contesto classificato.

In tale ambito, infatti, come noto, la Presidenza del Consiglio dei Ministri, per il tramite dell'UCSe, è l'organo deputato ad emanare indicazioni sulle misure di sicurezza da attuare per la protezione delle informazioni classificate anche gestite con sistemi elettronici.

In questo, mi si permetta, non chiaro, scenario, si potrebbero, infatti, configurare ipotesi di omissioni di comunicazione (sanzionati anche penalmente dal Decreto-Legge), o, ancor peggio, involontarie violazioni di segreto di Stato.