

COMMISSIONE IX  
TRASPORTI, POSTE E TELECOMUNICAZIONI

RESOCONTO STENOGRAFICO

INDAGINE CONOSCITIVA

18.

SEDUTA DI MERCOLEDÌ 10 LUGLIO 2019

PRESIDENZA DEL PRESIDENTE ALESSANDRO MORELLI

INDICE

|   | PAG. |   | PAG.    |
|---|------|---|---------|
| <b>Sulla pubblicità dei lavori:</b>   |      | <b>Audizione di rappresentanti di ZTE Italia Srl:</b>                                       |         |
| Morelli Alessandro, <i>Presidente</i> .....   | 3    | Morelli Alessandro, <i>Presidente</i> .....   | 3, 5, 7 |
| <b>INDAGINE CONOSCITIVA SULLE NUOVE<br/>TECNOLOGIE DELLE TELECOMUNICA-<br/>ZIONI, CON PARTICOLARE RIGUARDO<br/>ALLA TRANSIZIONE VERSO IL 5G ED<br/>ALLA GESTIONE DEI <i>BIG DATA</i>.</b> |      | Hong Zhong, <i>Responsabile mondiale della<br/>Cyber Sicurezza di ZTE Corporation</i> ..... | 3, 6    |
|   |      | Romano Paolo Nicolò (M5S) .....   | 5       |

N. B. Sigle dei gruppi parlamentari: MoVimento 5 Stelle: M5S; Lega - Salvini Premier: Lega; Partito Democratico: PD; Forza Italia - Berlusconi Presidente: FI; Fratelli d'Italia: FdI; Liberi e Uguali: LeU; Misto: Misto; Misto-Civica Popolare-AP-PSI-Area Civica: Misto-CP-A-PS-A; Misto-Minoranze Linguistiche: Misto-Min.Ling.; Misto-Noi con l'Italia-USEI: Misto-NcI-USEI; Misto-+Europa-Centro Democratico: Misto-+E-CD; Misto-MAIE - Movimento Associativo Italiani all'Estero: Misto-MAIE; Misto-Sogno Italia - 10 Volte Meglio: Misto-SI-10VM.

PAGINA BIANCA

PRESIDENZA DEL PRESIDENTE  
ALESSANDRO MORELLI

**La seduta comincia alle 14.30.**

**Sulla pubblicità dei lavori.**

PRESIDENTE. Avverto che la pubblicità dei lavori della seduta odierna sarà assicurata anche attraverso la trasmissione televisiva sul canale satellitare della Camera dei deputati e la trasmissione diretta sulla *web-tv* della Camera dei deputati.

**Audizione di rappresentanti di ZTE Italia Srl.**

PRESIDENTE. L'ordine del giorno reca, nell'ambito dell'indagine conoscitiva sulle nuove tecnologie delle telecomunicazioni, con particolare riguardo alla transizione verso il 5G ed alla gestione dei *big data*, l'audizione di rappresentanti di ZTE Italia Srl.

Ringrazio il signor Zhong Hong, responsabile della Cyber Sicurezza di ZTE Corporation, per aver accettato l'invito della Commissione e gli cedo la parola per lo svolgimento della propria relazione. *You are welcome.*

ZHONG HONG, *responsabile mondiale della Cyber Sicurezza di ZTE Corporation.* Signore e Signori, buon pomeriggio a tutti. Sono Zhong Hong, direttore generale della Cyber Sicurezza di ZTE. Sono molto lieto di essere qui con voi per uno scambio di idee e per parlare di cyber sicurezza

Vorrei, innanzitutto, presentarvi le due dichiarazioni sulla cyber sicurezza che ZTE ha diffuso quest'anno. La prima, la dichiarazione sulla cyber sicurezza del nostro

CEO, afferma che la ZTE pone il diritto alla sicurezza dei clienti al di sopra dei profitti e rispetta le leggi e i regolamenti relativi alla cyber sicurezza. La seconda dichiarazione è anch'essa una garanzia ed è stata diffusa da me stesso come responsabile della sicurezza di ZTE: la cyber sicurezza è il valore aggiunto più importante dei prodotti e dei servizi distribuiti da ZTE. Abbiamo creato una struttura di difesa a tre livelli per la cyber sicurezza, che integra le misure e i controlli di sicurezza in ogni fase del ciclo del prodotto, per garantire la sicurezza *end-to-end* dei prodotti e dei servizi.

Il secondo punto che vorrei affrontare riguarda la nostra visione e la nostra missione relativamente alla cyber sicurezza.

In ZTE abbiamo un motto secondo cui la sicurezza è nel nostro DNA e la fiducia nei nostri confronti da parte dei clienti e degli enti regolatori deve essere costruita attraverso la trasparenza. La nostra missione è creare un sistema d'avanguardia di *governance* globale della sicurezza per offrire ai nostri clienti la garanzia della sicurezza *end-to-end*.

Rapidamente, come possiamo tutelare la cyber sicurezza? Abbiamo tre direttrici principali lungo cui muoverci: la prima sono le persone, la seconda i processi e, la terza, le tecnologie che utilizziamo. Vediamo innanzitutto cosa facciamo per garantire la sicurezza delle persone e delle organizzazioni.

La ZTE ha creato una linea di difesa a tre livelli, o potremmo dire su tre linee, rappresentate con le abbreviazioni L1, L2 e L3. Abbiamo, inoltre, il comitato di controllo sulla sicurezza presieduto dal nostro CEO e di cui io, in qualità di *Chief Security Officer* (CSO) sono vice presidente.

Le tre linee di difesa si articolano così: sulla Linea 1 ci sono i *team* di esecuzione, le *business unit* che comprendono tutto il processo di produzione, dalla ricerca e sviluppo alla consegna dei prodotti. La Linea 2 è rappresentata dal dipartimento per la sicurezza dei prodotti, che è indipendente. La Linea 3 prevede audit e controlli effettuati da team di valutazione esterni.

Vorrei ora presentarvi il nostro processo di ricerca e sviluppo in ambito sicurezza.

Sappiamo che la sicurezza è importante in ogni fase della vita di un prodotto, per questo le misure volte a tutelarla e al monitoraggio della stessa devono integrarsi in tutte le fasi di ricerca e sviluppo. Partiamo dalla richiesta di sicurezza. Questa richiesta ha due aspetti: la richiesta di sicurezza da parte del nostro cliente e la necessità di conformarci a leggi e regolamenti e alle condizioni previste dai regolatori, integrandole con quelle dei clienti. In fase di progettazione e modellazione inseriamo alcune funzioni di sicurezza all'interno dei prodotti, funzioni che riteniamo molto importanti. In fase di ricerca e sviluppo inseriamo, quindi, dei codici di sicurezza ed effettuiamo una serie di valutazioni e revisioni dei codici per garantirne la sicurezza.

Al tempo stesso, è molto importante garantire la sicurezza nell'ambito di test, per cui abbiamo una serie di procedure, come test di revisione dei codici, test delle scatole nere, *scan* di vulnerabilità, test di penetrazione e così via, per testare la sicurezza. Come dicevo prima, abbiamo un sistema articolato su tre linee e la seconda e la terza linea sono indipendenti e possono quindi eseguire test di valutazione della sicurezza in modo indipendente. Eseguiamo test e *audit* per capire lo stato di sicurezza del prodotto fino al rilascio, ma anche in tutto il ciclo di vita del prodotto dopo il rilascio e per garantire la stabilità della versione rilasciata. Abbiamo delle operazioni di ricerca dei *virus*, di *scan* dei *virus*, controlli sulle scatole nere così via, per rafforzare la sicurezza nella fornitura dei prodotti: in questo modo garantiamo la gestione della sicurezza lungo tutto il ciclo di vita del prodotto. In tutti i processi,

abbiamo integrato la gestione della sicurezza nella pratica.

La seconda parte riguarda le tecnologie, come dicevo, che sono il secondo pilastro importante per garantire la sicurezza e le verifiche della stessa.

Possiamo dividere queste tecnologie di verifica in due tipologie. La prima è costituita da tutti i test che vengono effettuati sulle scatole nere per garantire la sicurezza dei prodotti e si effettuano tramite una serie di strumenti che ci vengono forniti dai nostri partner che vedete elencati in questa slide. La seconda tipologia riguarda i test di penetrazione. Abbiamo, ad esempio, dei test sulle scatole nere che prevedono la simulazione di attacchi e testano la capacità di resistenza agli attacchi dei nostri prodotti. Ovviamente, la sicurezza non è qualcosa che può essere portato avanti da un'azienda o da un operatore economico singolarmente. C'è bisogno di lavorare con altri attori di uno stesso settore, in cui tutti i partecipanti alla catena di produzione hanno un interesse comune nel tutelare e garantire insieme la sicurezza. La ZTE sta attuando una collaborazione a livello internazionale con terze parti e con gli enti regolatori per creare un sistema di controlli e certificazioni sulla sicurezza il più ampio possibile.

Attualmente, abbiamo tre laboratori per il controllo della cybersicurezza in tutto il mondo, che svolgono attività di controllo e collaudi della sicurezza dei prodotti, attività di revisione sui processi, sui codici sorgente e sui documenti tecnici che vengono analizzati e controllati, così come si effettuano analisi dei risultati dei test.

Nel mese di maggio, a Nanjing, in Cina, abbiamo aperto un primo laboratorio sulla sicurezza. Il secondo è stato inaugurato qui in Italia il 21 maggio 2019, ed è stato il primo fuori dalla Cina.

I principali servizi che i nostri laboratori possono offrire comprendono la revisione del codice sorgente, analisi statica e dinamica del codice; audit e analisi sui processi e su tutti i documenti tecnici prodotti da ciascuna delle fasi di lavoro precedentemente descritte per verificarne la conformità con gli standard di sicurezza e

per tenerne un registro. Un terzo tipo di servizio è considerare i prodotti come una scatola nera ed effettuare dei test sulla scatola nera partendo dalla scocca esterna del prodotto. Il quarto tipo di servizio è creare dei test di penetrazione, come ad esempio delle simulazioni di attacchi alle scatole nere, per testare la capacità di resistenza agli attacchi esterni ed interni dei prodotti. Inoltre, speriamo che la rete di laboratori per la cyber sicurezza di ZTE possa diventare una sorta di piattaforma sicura e aperta per collaborare con terze parti e per fornire i servizi di auditing che ho appena descritto sia ai clienti sia ad eventuali enti regolatori interessati a migliorare la sicurezza dei prodotti e simulare degli attacchi informatici.

Come dicevo poc'anzi, per garantire la sicurezza c'è bisogno del contributo di tutti gli attori coinvolti in un settore. ZTE sta cercando di dare il proprio contributo alla sicurezza del suo settore e noi ci stiamo impegnando insieme a tutti gli altri attori nel nostro settore per portare avanti la cyber sicurezza, stiamo lavorando a livello internazionale.

Stiamo portando avanti degli studi per la creazione di standard sulla sicurezza informatica. Abbiamo partecipato alla GSMA con una relazione sull'intelligenza artificiale e sulla cyber difesa basata sull'intelligenza artificiale.

Abbiamo poi portato avanti diverse altre collaborazioni, ad esempio contribuendo ai lavori per la SCAS sul 5G. Abbiamo iniziato nel 2017, e quest'anno a marzo abbiamo fatto un aggiornamento a questo lavoro di ricerca sul 5G con la pubblicazione di un libro bianco in materia, che vedete qui.

Per concludere, speriamo di poter portare avanti un approccio aperto e trasparente per i nostri clienti, per i nostri collaboratori e per gli enti regolatori per far sì che possano conoscere al meglio il nostro sistema di sicurezza informatica e diventare così un'azienda quotata in borsa completamente aperta e trasparente. Siamo pronti a collaborare con gli altri attori nel nostro settore per mostrare le nostre misure per la tutela della sicurezza informa-

tica e i risultati che abbiamo raggiunto finora.

Concludo qui. Grazie per l'attenzione.

PRESIDENTE. Grazie molte per il suo intervento.

Do ora la parola agli onorevoli colleghi che intendano intervenire per porre quesiti o formulare osservazioni.

PAOLO NICOLÒ ROMANO. Ringrazio i rappresentanti di ZTE per essere qui.

Ho tre domande da porre. Vorrei sapere se il vostro codice è totalmente aperto, se nei vostri apparati c'è solo codice *open source* o parte di codice secretato.

Inoltre, recentemente il Governo italiano ha emanato la norma sul *golden power* per riuscire a far partire la sperimentazione di due soggetti (Fastweb e Samsung): vorrei sapere se siete a conoscenza di questa norma e come l'avete interpretata, se per voi è positiva.

Ancora, visto che si è parlato solo di *cybersecurity*, ma non di sicurezza riguardante la salute, potete darci qualche rassicurazione in merito anche su questo aspetto? In Italia, c'è un acceso dibattito sulle radiofrequenze: gradiremmo sapere se sono stati fatti test anche su quest'aspetto.

PRESIDENTE. Vorrei intervenire anch'io su alcuni aspetti.

Mi fa molto piacere aver sentito più di una volta il termine « trasparenza ». È evidente che c'è la sensazione di voler dare all'opinione pubblica italiana, e chiaramente in questo caso ai rappresentanti degli italiani, la piena disponibilità su un tema che è *il* tema oggi all'ordine del giorno anche per rassicurare l'opinione pubblica su tale specifico profilo, come dicevo. Ben venga, quindi, la maggiore trasparenza possibile da parte di tutte le aziende coinvolte nelle nuove tecnologie in un processo che ci vedrà protagonisti.

Lei ha fatto riferimento a terze parti. Nella documentazione illustrata appare, tra le aziende, IBM: quali sono le altre aziende coinvolte? Ci sono anche aziende italiane

che fanno parte della strategia con la quale state investendo nelle varie parti del mondo?

È inutile nascondere che uno dei problemi, o almeno uno degli Stati che ha creato e sta creando maggiori attriti sono gli Stati Uniti: ci sono aziende statunitensi che collaborano con voi, mi auguro al meglio, per produrre il maggior servizio pubblico possibile?

Dall'altra parte, giusto per capire e per rendere edotti tutti i parlamentari al riguardo, quali sono i vostri investimenti sul tema del 5G? Quali sono i vostri investimenti per quanto riguarda la ricerca nelle nuove tecnologie?

Noi abbiamo un nostro termine di paragone, che sono le aziende italiane. Sappiamo che le aziende cinesi hanno probabilmente maggiori possibilità. Anche per avere noi stessi un'idea dei rapporti di forza presenti nel mondo, mi interesserebbe sapere quali sono i vostri investimenti su 5G e, in generale, nella ricerca per tutto quello che riguarda le nuove tecnologie.

Do la parola al nostro ospite per la replica.

ZHONG HONG, *responsabile mondiale della Cyber Sicurezza di ZTE Corporation*. Inizio dalla prima domanda sui codici sorgente.

Innanzitutto, il nostro codice è aperto e trasparente, ma non è *open source*. Permettiamo alle persone designate da clienti, istituzioni e regolatori di venire nei nostri laboratori ed effettuare controlli e analisi sul nostro codice, quindi la trasparenza del codice è assicurata. Questo, ovviamente, ci permette di tutelare la nostra proprietà intellettuale, ma al tempo stesso anche di accrescere la fiducia e la collaborazione con clienti licenziatari ed enti regolatori che possono accedere al codice sorgente e ai documenti tecnici. Ovviamente, servono delle competenze tecniche e i controlli possono, quindi, essere svolti da persone competenti approvate da enti pubblici, ad esempio. Questo ci permette di garantire anche la sicurezza del nostro codice sorgente. È possibile, verificare anche se c'è o meno una *back door* nel nostro codice: in questo modo si risolve una delle preoccupazioni

principali. Questo per quanto riguarda la trasparenza del codice. Il secondo aspetto riguarda la trasparenza delle informazioni sulla nostra società.

Come vi dicevo, siamo un'azienda quotata in borsa a Shenzhen e Hong Kong, e quindi è possibile avere tutte le informazioni sulla nostra azienda tramite i canali ufficiali, non abbiamo niente da nascondere. Questo è un altro aspetto di trasparenza importante per tutte le informazioni riguardo alle radiofrequenze che utilizziamo, che sono in conformità con i regolamenti e le leggi cinesi e di Hong Kong.

In merito al 5G e agli investimenti in Italia in ricerca e sviluppo, nel 2017 il 47 per cento del nostro *output* veniva dall'estero e il 25 per cento proveniva da Europa e Stati Uniti. Come vedete, una parte importante del nostro fatturato viene dall'estero e non dal mercato cinese. Il nostro investimento in ricerca e sviluppo era più del 49 per cento del nostro fatturato totale del 2018, piuttosto alta come percentuale e all'avanguardia nel settore.

Il punto focale del nostro lavoro di ricerca e sviluppo sono le nuove tecnologie, compreso il 5G e tutte le tecnologie collegate al 5G e alla banda ultralarga.

In generale, siamo una delle aziende all'avanguardia nel campo del 5G. Riguardo agli investimenti *end-to-end* sul 5G, siamo all'avanguardia a livello internazionale. Stiamo fornendo soluzioni *end-to-end* per tutti i servizi 5G, dalle infrastrutture fino ai prodotti che possono utilizzare il 5G.

In terzo luogo, abbiamo dei nuovi dati in relazione alla proprietà intellettuale e alle domande di brevetto. All'*European Telecommunications Standards Institute* (ETSI) abbiamo raggiunto il terzo posto per numero di domande di brevetto, con 1424 domande di brevetto presentate, e siamo stati per nove anni di seguito nella top 5 a livello internazionale.

Nel 2017 eravamo al primo posto a livello internazionale per i brevetti. A dicembre del 2018 avevamo più di 35.000 domande di brevetto presentate, con più di 200 collegate al 5G. Con riferimento ai

diritti di utilizzo commerciale del 5G, abbiamo contratti in venticinque Paesi.

Questi sono alcuni aspetti relativi al nostro lavoro di ricerca e sviluppo per il 5G. Non ho i dati specifici per il mercato italiano, ma so che insieme ai nostri partner sul mercato italiano stiamo portando avanti dei progetti importanti. Abbiamo già realizzato delle sperimentazioni interessanti in ambito 5G. Abbiamo un centro di sperimentazione per il 5G in Italia, il primo in Europa. Come vi ho detto, tra l'altro, il nostro laboratorio per la cyber sicurezza in Italia è il primo a livello internazionale fuori dai confini cinesi.

Questo mostra come diamo grandissima importanza all'Italia e al mercato italiano, e siamo pronti a continuare a investire in

Italia anche in cooperazioni tecnologiche e laboratori sulla sicurezza informatica. Tra l'altro, nel nostro laboratorio qui in Italia, l'80 per cento degli addetti sono italiani. Vogliamo collaborare con l'Italia, anche fornendo delle opportunità di lavoro, dando un nostro contributo.

PRESIDENTE. Ringrazio il responsabile mondiale della Cyber Sicurezza di ZTE Italia Srl per il suo contributo.

Dichiaro conclusa l'audizione.

**La seduta termina alle 14.55.**

---

*Licenziato per la stampa  
il 16 novembre 2019*

---



\*18STC0072880\*