COMMISSIONE IV
DIFESA

RESOCONTO STENOGRAFICO

INDAGINE CONOSCITIVA

30.

SEDUTA DI MERCOLEDÌ 3 NOVEMBRE 2021

PRESIDENZA DEL PRESIDENTE **GIANLUCA RIZZO**

INDICE

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; Italia Viva: IV; Coraggio Italia: CI; Liberi e Uguali: LeU; Misto: Misto; Misto-L'Alternativa c'è: Misto-L'A.C'È; Misto-MAIE-PSI-Facciamoeco: Misto-MAIE-PSI-FE; Misto-Centro Democratico: Misto-CD; Misto-Noi con l'Italia-USEI-Rinascimento ADC: Misto-NcI-USEI-R-AC; Misto-Minoranze Linguistiche: Misto-Min.Ling.; Misto-Azione-+Europa-Radicali Italiani: Misto-A-+E-RI.

PAGINA BIANCA

PRESIDENZA DEL PRESIDENTE GIANLUCA RIZZO

La seduta comincia alle 9.

Sulla pubblicità dei lavori.

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

Audizione di rappresentanti della Telsy S.p.A.

PRESIDENTE. L'ordine del giorno reca – nell'ambito dell'indagine conoscitiva sulla pianificazione dei sistemi di difesa e sulle prospettive della ricerca tecnologica, della produzione e degli investimenti funzionali alle esigenze del comparto difesa – l'audizione di rappresentanti della TELSY S.p.A.

Saluto e do il benvenuto al dottor Eugenio Santagata, Amministratore delegato, che è accompagnato dal dottor Antonio Iannamorelli, *government affairs Director*, che ringrazio per la partecipazione ai lavori della Commissione.

Do il benvenuto ai colleghi presenti ai colleghi che parteciperanno alla seduta secondo le modalità stabilite dalla Giunta per il Regolamento del 4 novembre 2020, ai quali rivolgo l'invito a tenere spenti i microfoni per consentire una corretta fruizione dell'audio.

Ricordo che dopo l'intervento del nostro ospite darò la parola ai colleghi che intendano porre domande o svolgere osservazioni. Successivamente, il nostro ospite potrà rispondere alle domande poste. A tal proposito chiedo ai colleghi di far pervenire fin da adesso la propria richiesta di iscrizione a parlare al banco della Presidenza.

Do, quindi, la parola al dottor Eugenio Santagata. Prego.

EUGENIO SANTAGATA, *Amministratore delegato della TELSY S.p.A.* Buongiorno a tutti. Ringrazio il presidente e tutti gli onorevoli deputati. Grazie dell'opportunità; è sempre un piacere tornare in questi luoghi che, a mio e a nostro modo di vedere, sono sacri per ciò che riguarda l'analisi, l'elaborazione e la presa di decisioni importanti ad altissimo impatto per il comparto industriale della difesa e, conseguentemente, anche per la nostra società.

Si era abituati a pensare all'industria della difesa secondo una visione da *bricks and mortar*, come si suole dire, ovvero molto orientata sull'*hardware* e sulle piattaforme. Così come sta avvenendo nel mondo della sicurezza informatica, di cui anche ci occupiamo, nel quale ogni giorno che passa sempre più pezzettini di digitale diventano *cyber security*, anche nell'industria della difesa il perimetro di questo comparto si sta dilatando giorno per giorno al punto che pezzi di industria che prima non erano necessariamente riconducibili al mondo dell'industria difesa, oggi lo sono per vari motivi.

Il principale motivo è – questo è un fenomeno già noto – che si sta assistendo a una progressiva smaterializzazione o, in altri termini, a un'importante, ineludibile e inevitabile fenomeno di digitalizzazione di ciò che è industria della difesa e il materiale d'armamento.

Già normative a livello europeo, poi recepite nel nostro ordinamento, hanno posto degli importanti paletti a riguardo, ma sempre di più oltre alla piattaforma, intesa nella sua importantissima e centrale

fisicità, vi è anche tutto ciò che ruota intorno ad essa, tant'è vero che gli investimenti più importanti - non necessariamente da un punto di vista economico ma certamente dal punto di vista del peso specifico che queste piattaforme rivestono - sono sempre di più in ciò che non si vede rispetto a ciò che si vede.

Questo pone il tema assai centrale delle cosiddette « architetture distribuite » e, quindi, del *software* che indirizza una data piattaforma al fine di consentirle di svolgere il proprio compito in ambito operativo o in uno scenario operativo; *software* che, inevitabilmente, si porta dietro un tema di dati e di informazioni. Ecco che comparti dell'industria – in questo caso italiana – sempre più rilevanti diventano inevitabilmente d'interesse per l'industria della difesa, in quanto sempre di più asserviti a scopi di sicurezza nazionale e di difesa.

Prendiamo, ad esempio, il *Fighter* di sesta generazione: nessuno più pensa a una complessa piattaforma di questo tipo come un sistema identificabile con una struttura fisica così come era qualche tempo fa, bensì è un concetto di architettura distribuita. In altre parole, l'insieme non è necessariamente più monolitico e, a sua volta, l'aspetto più importante di piattaforme di questo tipo non è tanto il *software* che sta a bordo, ma il *software* che sta a terra, che lo comanda e che permette la trasmissione di dati o che ne consente anche a molta distanza l'interoperabilità.

Che significa ? Che sempre più soggetti – questo è un segno positivo, purché accompagnato come fenomeno da un'attenta regia politica – dell'industria della difesa o dell'industria *high tech* italiana fanno parte di un ecosistema. Questo ecosistema vede sempre più partecipanti a un grande gioco di tipo industriale, laddove ci sono anche dei rischi, perché nel momento in cui i contorni del comparto si allargano, diventano anche più labili le protezioni a questo tipo di sistema.

Ecco allora che nella selezione degli investimenti occorre porre particolare attenzione più a ciò che non si vede rispetto a ciò che, in realtà, è immediatamente riconducibile a un tradizionale materiale di armamento.

Dov'è TELSY in tutto ciò ? Come è noto, TELSY è parte del gruppo Tim che è il principale *telecom operator* italiano e, come tale, è strutturalmente inserito nell'ambito e nell'alveo della cosiddetta « *national security* », storicamente azienda impegnata nello sviluppo di algoritmi proprietari di cifratura che consentono la trasmissione o la conservazione sicura dei dati.

Anche in questo mondo tradizionalmente legato a un concetto di intangibilità si sta verificando una progressiva digitalizzazione, perché sempre di più sistemi tradizionali come, ad esempio, – per citarne uno dei tanti – le cifranti, che nella loro dimensione meccanica e fisica hanno un punto focale, si stanno smaterializzando e si sta parlando sempre di più di cifranti completamente virtualizzate da una parte e, quindi, basate su *software*, dall'altro.

Su questo pongo un tema a nostro avviso importantissimo, di centrale e vitale dimensione all'interno dei dibattiti che si stanno facendo. È noto come soprattutto in Occidente si stiano facendo enormi passi in avanti nel campo del *quantum computing*, ovvero della computazione accelerata che utilizza i princìpi della fisica quantistica. È anche noto che i princìpi della fisica quantistica non rispondono alle teorie e alle regole della fisica tradizionale e, probabilmente, è anche noto il famoso esempio del gatto di Schrödinger, che è dato per vivo e per morto allo stesso tempo. Questo tipo di applicazioni è alla base degli sviluppi del *quantum computing*. Noi sappiamo, anche da un punto di vista applicativo, che l'avvento del *quantum computing* renderà tutte le chiavi di cifratura inutili o, comunque, molto più fragili rispetto a prima.

La risposta, anche e soprattutto in campo difesa, a tutto ciò che è *quantum computing* si chiama « *quantum communication* »; quindi, la comunicazione basata sui princìpi della fisica quantistica.

Su questo TELSY ha posto importantissime basi per uno sviluppo a breve e medio termine – non dico « lungo », perché in questo settore il lungo perde di significato – attraverso il lancio di una prototipazione

di un sistema che viene chiamato « *quantum key distribution* », ovvero una chiave di cifratura indistruttibile per la trasmissione di dati da un punto a un altro che utilizza le leggi dell'ottica. Fondamentalmente significa sfruttare la strutturale fragilità di queste piccolissime particelle che sono i fotoni per cercare di comprendere se, nel trasmettere questi dati da un punto « A » ad un punto « B », vi sia stata qualunque forma di compromissione.

Questo è un settore su cui diversi Paesi stanno facendo importanti investimenti. Gli Stati Uniti, per quanto noto, si stanno concentrando più sul *quantum computing*, mentre in Cina si stanno concentrando sia sul *quantum computing* che sul *quantum communication*.

Questo tipo di prototipo verrà messo a sistema con tecnologie come quelle a fibra, di cui il gruppo Tim dispone attraverso altre articolazioni per cercare di realizzare dei sistemi di cifratura che possano trasmettere dati a distanze sempre più elevate – oggi abbiamo un limite intorno ai 100 chilometri circa – con la certezza, anche alla luce delle sfuggenti regole della fisica quantistica, dell'indistruttibilità di questo tipo di chiave.

Questo tipo di investimenti è un *unicum* nel suo genere, perché in Italia TELSY è uno dei pochissimi *player* a tecnologia avanzata su questo tipo di settore. Quindi, con particolare piacere e anche orgoglio, condivido in questa sede istituzionale questo tipo di informazioni perché sarà sempre più centrale in tutte le discussioni che verteranno su importanti decisioni relative a investimenti su piattaforme, perché inevitabilmente ciascun sistema aperto ha bisogno di comunicare con un altro in maniera sicura e in maniera tale da rendere il tutto coerente con i vari *framework* di sicurezza anche di tipo regolatorio che saranno posti in essere.

Per completare questa breve illustrazione su come si inserisce TELSY e, quindi, Tim all'interno del comparto difesa, mi soffermo brevemente sul fatto che vi è sempre più convergenza tra il mondo della cifratura e quello della *cyber security*.

Cito soltanto, a titolo di esempio, il *ransomware*, che preoccupa tutti noi e che non è altro che un *software* criptato. Per poter contrastare questo tipo di minaccia è necessario unire le competenze che un tempo non necessariamente erano unite.

Inoltre, aggiungo che nella sicurezza delle comunicazioni, che passa anche attraverso la sicurezza dei dispositivi mobili, si verificherà sempre di più e vi sarà una pesante e importante ricaduta anche in ambito difesa della cultura volta a mettere in sicurezza un sistema operativo con quella che è impegnata a mettere in sicurezza il cosiddetto « *firmware* », quindi ciò che apparentemente non si vede anche all'occhio dell'utente, ma che sta sotto e che diventa sempre di più l'*humus* tecnologico connettivo all'interno del quale questi due mondi tenderanno a convergere.

TELSY sta investendo pesantemente in questo tipo di settore e lo sta facendo cercando di collaborare con altri *player* dell'industria italiana. In questo senso è sempre auspicabile una forte convergenza con le istituzioni politiche, con le Forze armate, con il mondo della ricerca e con l'ecosistema di piccole e medie imprese che da questo punto di vista – ricollegandomi a quanto dicevo all'inizio – essendo sempre più parte di un comparto fondamentale per l'industria della difesa, diventano a loro volta un *target* che va messo in sicurezza. Grazie.

PRESIDENTE. Dottor Santagata, grazie a lei per la sua relazione esaustiva, certamente molto dettagliata e sicuramente utile ai lavori d'indagine che la nostra Commissione sta svolgendo. Ho una prima richiesta di intervento da parte della collega Occhionero a cui do la parola. Prego.

GIUSEPPINA OCCHIONERO. Grazie, presidente. Grazie al dottor Santagata per la sua compiuta relazione che, come ha già detto il presidente, sicuramente ci aiuterà anche nei lavori di questa Commissione. Per cui ben vengano queste audizioni quando possono essere di stimolo e di riflessione anche e soprattutto per noi, perché le istituzioni devono essere vicine al tessuto in-

dustriale nazionale. Ritengo molto importante sviluppare la nostra sensibilità anche attraverso questa attività di audizione.

Sfogliando la documentazione che lei ci ha lasciato, oltre che ascoltando le sue parole, mi è venuta in mente una riflessione che mi piacerebbe condividere con lei o quantomeno sapere il suo punto di vista rispetto a una delle grandi *mission* del Piano nazionale di ripresa e resilienza PNRR, che è la digitalizzazione della pubblica amministrazione e quindi le infrastrutture digitali.

Uno degli obiettivi è tentare di migrare nel *cloud* il 75 per cento dei dati della pubblica amministrazione, se non erro, entro il 2025 e tra le varie *slide* vedo che chiaramente il *cloud* nazionale interesserà sicuramente i lavori di TELSY, anche perché, anche da quello che ho ascoltato, ritengo che TELSY abbia grandi competenze tecnologiche. Lei ha giustamente vantato – noi ne siamo orgogliosi – le tecnologie avanzate di cui TELSY è dotata.

Sostanzialmente, il nostro tessuto industriale si caratterizza per competenza e per tecnologia, quindi può essere sicuramente uno di quegli attori qualificati di cui sarà necessario avvalersi per la realizzazione dell'obiettivo.

Siccome nel corso della nostra attività abbiamo audito amministratori delegati di altre società e i grandi attori italiani che lei ha citato come Tim, Fincantieri, Leonardo, Rheinmetall e abbiamo parlato di progetti di aggregazione al mondo della difesa italiana, le chiedo e mi chiedo una cosa: è necessario dialogare con tutti i *partner* dell'industria italiana, perché sono le nostre eccellenze, ma lei ritiene che queste grandi sfide possano essere vinte esclusivamente dall'Italia, oppure c'è sempre bisogno in questo piano di aggregazione al mondo della difesa di guardare anche ad altri attori ? È di poche ore fa il protagonista attore del G20, ovvero il multilateralismo. Ritiene che l'Italia da sola possa affrontare questa sfida, avvalendosi delle vostre particolari capacità, o è necessario guardare anche oltre i confini ed eventualmente chi potrebbero essere gli altri attori a cui guardare per questo piano di aggregazione ?

Ad ogni modo, ritengo sempre assolutamente necessario – lei me lo può confermare – preservare in ogni caso la sovranità tecnologica. Questa era un po' la mia riflessione e volevo sapere il suo punto di vista rispetto a questo tema. Grazie.

GIOVANNI RUSSO, *intervenendo da remoto*. Buongiorno a tutti. Purtroppo per ragioni di salute, questa mattina non potrò partecipare in presenza, però ringrazio TELSY per la sua analisi molto importante, che ha messo giustamente in risalto l'importanza di un'azienda che a livello nazionale si occupa di un settore così importante come la difesa cibernetica.

Ho sempre pensato che l'Italia dovesse dotarsi di una capacità anche di aggressione e di attacco di difesa, quindi non soltanto di poter rispondere a quelle che sono le eventuali minacce, ma anche, in accordo con altre agenzie statali, di poter disarticolare eventuali minacce in maniera preventiva, dotandosi di una capacità di attacco dal punto di vista informatico.

Volevo chiedere quale era lo stato dell'arte e in che modo TELSY si pone in questo ambito così delicato, ma così importante.

Come abbiamo visto, altri Stati si stanno dotando di capacità di attacco informatico rilevanti, anche perché anche questo tipo di operazioni comporta un progresso tecnologico e una ricerca specifica rilevante, con investimenti mirati e con delle capacità di acquisizione di *know how* importanti che possono far fare un salto qualitativo anche ai vari sistemi di difesa dei Paesi. Grazie.

ALBERTO PAGANI. Grazie dottor Santagata per l'illustrazione assolutamente chiarissima e che mi suscita una domanda forse un po' banale, ma che trovo importante sul tema.

Il punto centrale del ragionamento che ha sviluppato muove dal cambiamento del prodotto oggetto del *procurement* militare, che è sempre più tecnologicamente ricco. Naturalmente questo prodotto comporta la necessità di avere capacità tecnologica nel sistema industriale; e comporta anche che

tali capacità siano sostenute al pari di quanto lo sono le capacità delle aziende che producono la parte *hardware*, perché se un prodotto è metà piattaforma e metà sistemi, bisogna che il sostegno all'industria che produce sistemi sia pari a quello all'industria che produce le piattaforme. In alcuni casi probabilmente l'azienda è la stessa, ma in altri no e se vogliamo sviluppare un sistema industriale dobbiamo vedere l'ecosistema complessivo e non solamente i punti più di eccellenza.

La mia domanda è questa. Deduco che le sfide delle nuove tecnologie richiederanno anche una forte capacità di investimento per stare al passo e immagino che, come tutte le altre aziende, anche queste aziende siano in grado di sostenere investimenti, se hanno una stabilità nella programmazione e un minimo di certezza nelle risorse che il mercato è in grado di garantire negli anni.

Ci sono delle accortezze, delle attenzioni che, non tanto il legislatore, ma bensì il committente, ovvero la Difesa, può cominciare ad adottare per sostenere la crescita, la robustezza di un sistema industriale che si occupa della parte dei sistemi e non della parte *hardware* di costruzione delle piattaforme ? A suo avviso ci sono delle mancanze di attenzioni che fanno perdere opportunità di crescita, di capacità di investimento, di capacità di sviluppo di prodotti e di sistemi ?

A noi interessa l'acquisizione nel sistema nazionale, ma anche la capacità di esportazione dell'industria nazionale e la capacità di stare su mercati più ampi di quelli del nostro stretto interesse.

ROBERTO ROSSINI. Ringrazio il dottor Santagata per la relazione. Andrò diretto al punto. Rispetto alla Francia e a tanti altri Paesi europei, stiamo investendo molto poco nella dimensione cibernetica. Sicuramente in questo momento siamo molto più indietro e questo ci penalizza a livello di digitalizzazione del nostro Paese.

In parte mi lego a quello che ha detto adesso il collega Pagani. Lei ha detto che gli Stati Uniti si stanno concentrando sul *quantum computing*, mentre la Cina sia sul *quantum computing* che sul *quantum communication*. Se ho capito bene, una volta che saranno sviluppati questi strumenti, i codici di cifratura sanno quasi completamente inutili e la nostra sicurezza sarà ancora molto più labile. Dove ci dovremmo spingere anche per avere un rapporto con questi Paesi che ci stanno già lavorando, affinché si riescano a trasferire anche in parte al nostro Paese le loro conoscenze e i loro *know how* ?

Sicuramente in questo momento non abbiamo quelle potenzialità economiche che hanno Paesi come la Cina e gli Stati Uniti; quindi, dire che domani investiremo i soldi che stanno investendo questi Paesi è follia.

Dove dovremmo concentrarci, anche a livello parlamentare o comunque a livello di aziende per poter magari recuperare quelle conoscenze che già altri Paesi stanno portando avanti ?

Sarà importante essere preparati nel momento in cui anche il nostro Paese, a livello di difesa, avrà degli attacchi o dovrà difendersi da certi tipi di attacchi. Grazie.

FRANCESCO D'UVA, *intervenendo da remoto*. Buongiorno. Ho due domande. Secondo lei cosa dovrebbe fare il Governo italiano per favorire la collaborazione a livello europeo per quanto riguarda l'investimento delle tecnologie di cui vi occupate ?

Ho letto che vi state occupando dell'intelligenza predittiva. Non sarà Minority Report, però mi chiedo quanto ci possiamo avvicinare effettivamente a modelli che permettano veramente di poter prevedere le mosse future, perché questa è una cosa veramente molto innovativa, quasi da fantascienza. Chiedo a voi la reale fattibilità. È ovvio che se ci sta investendo, però fino a che punto si potrà spingere questa tecnologia ?

Grazie, presidente. Grazie a lei, dottore.

PRESIDENTE. Do adesso la parola al dottor Santagata. Prego.

EUGENIO SANTAGATA, *Amministratore delegato della TELSY S.p.A.* Grazie delle domande pertinenti. Vado in ordine per come sono state poste.

Credo che la storia ci insegni che tutte le volte che l'Italia ha fatto cose buone, le ha fatte insieme a qualcuno. Anche nell'industria della difesa, con particolare riferimento a quella di riferimento di TELSY – ma vale anche, ad esempio, per la compagine industriale dalla quale provengo, che è quella dell'elettronica per la difesa –, vale il motto che nessuno si salva da solo.

È la stessa cosa che avviene su tematiche altrettanto importanti. La partita diventa: chi sono i miei compagni di viaggio ? Con chi mi accompagno ? Questo è un tema di tipo squisitamente politico, prima ancora che industriale: insieme alla politica, insieme alla industria e insieme al tecnico occorre identificare una serie di priorità. Cosa per me è importante ?

Nella nostra evoluzione storica ed economica questo si è avuto nel tempo e ci sono stati dei momenti laddove le divergenze di tipo politico e le diverse visioni di fronte a temi importanti hanno lasciato il passo a un sentimento e a una volontà di voler convergere su qualcosa che, inevitabilmente, riguarda e tocca la vita di tutti.

Dalla mia visuale dico sempre: « Se sei in serie B e vuoi migliorare la tua *performance*, devi cimentarsi con quelli che stanno in serie A. ». Noi siamo in Europa e non siamo un Paese di serie B.

Direi che storicamente le più fruttuose e proficue collaborazioni, anche nel campo della Difesa – non per questo senza attenzione a temi di sovranità legittima e sicurezza nazionale –, le abbiamo fatte con Paesi come la Germania e la Francia. Senza nulla togliere agli altri, se andiamo a fare una somma delle principali industrie della difesa di Francia, Italia e Germania e del loro indotto, probabilmente avremo una rappresentazione molto importante e maggioritaria di ciò che c'è e che gira in Europa e anche in questo concetto di Europa allargata con la quale dobbiamo fare i conti e con cui amiamo anche cimentarci tutti i giorni.

A mio avviso non c'è un limite concettuale a dire che un sistema lo si fa insieme, ma occorrono regole chiare a monte. Quando vi sono regole chiare a monte, in questo contesto vale quello che vale nel tema degli investimenti stranieri: ad eccezione di alcuni particolari tipi di investimenti, il problema non è tanto l'investimento in quanto tale, ma il come lo si fa fare, le condizioni alle quali lo si fa fare e se vi è coerenza tra implementazione e le premesse a monte di tipo politico sul definire quali siano state le nostre priorità.

È anche vero che non è facile, perché poi a un certo punto ci si trova a parlare e diventa tutto prioritario per tutti. Però, inevitabilmente, così facendo è impossibile raggiungere alcunché e alcun tipo di accordo.

Con chiarezza di intenti – c'è anche un *no deal* quando questo non può essere rispettato – devono essere ben individuate le priorità di tipo nazionale su un certo tipo di tecnologia che per me dovrebbe essere il criterio « Dove sto e a che punto sto in un certo settore e in cosa dovrei partire completamente da zero ? ».

È chiaro che il settore in cui si parte completamente da zero non deve essere la priorità, perché ci vorrebbero troppo tempo e troppi soldi per poter reinventare la ruota. Da questo punto di vista credo occorra un sistema di geometrie intelligenti, che non necessariamente significa « Vado con tutti », a 360 gradi in Italia sul nocciolo duro nel settore della difesa, che è proprio uno di quei settori su cui l'Italia ha saputo dimostrare insieme all'*automotive*, al lusso e ad altri settori che se vuole le cose le sa fare e le sa fare anche in unità di intenti.

Passando alla domanda sull'opportunità di dotarsi di capacità di risposta, a mio avviso è un tema che trova la sua naturale conseguenza in due cose: non c'è sufficiente protezione e difesa senza un adeguato deterrente. Questo non significa violare princìpi costituzionali che vedono l'Italia come un attore non belligerante, che non cerca nell'offesa uno strumento o un *modus operandi* atto a implementare una sua politica espansiva, però così come abbiamo un'industria della difesa che è in grado di sviluppare materiali d'armamento a scopo difensivo, attivati solo a ragion veduta e predisposti quando serve, analogamente dovrebbe essere nel mondo della

sicurezza informatica per quanto riguarda le capacità di risposta.

A mio avviso il secondo elemento a supporto di questa necessità è che soltanto ponendosi dal lato dell'attaccante si riesce a tracciare, anche tecnologicamente, una linea di difesa sufficientemente avanzata e tale da esprimere una capacità di deterrenza.

Anche qui la premessa è di tipo politico, poiché occorre fare un po' di chiarezza su chi debba essere il soggetto che porta avanti questo tipo di attività all'interno di attività del nostro ordinamento, che è molto più chiaro rispetto a prima e lo dico a onore di tutti coloro i quali ci hanno lavorato e anche dell'industria.

Tuttavia, questo ce lo chiede anche la NATO. Infatti, si parla chiaramente di *cyber offensive operations* come strumento che oggi può essere compreso all'interno dei vari *course of action* di un conflitto asimmetrico, anche perché ormai tutti i conflitti sono asimmetrici ed essendo asimmetrici, non necessariamente tutti gli strumenti e gli *asset* a disposizione devono essere ibridi. Va da sé che se uno strumento deve essere ibrido, a maggior ragione si deve portare dietro sia una capacità di difesa, sia una capacità di risposta a ragion veduta.

Anche qui si complica un po' lo scenario, perché un'arma nucleare è impossibile nasconderla, ma un attacco *cyber* non fa rumore.

Su questo versante diventa complicato dire con certezza chi ha posto in essere un certo tipo di attacco, ma il tutto si risolve se si interpreta la capacità di risposta come inserita all'interno di un più ampio e poderoso sistema di *intelligence*. Infatti, un conto è porre in essere deliberatamente senza nessun sistema di comando e controllo un attacco *cyber* verso un supposto attaccante che, per ciò che concerne la sicurezza nazionale di tipo statuale, lo riesce a parare; altro è dire in tempo di pace – per usare un termine noto – che mi addestro perché ho necessità di comprendere come è fatta l'infrastruttura di coloro i quali potrebbero rappresentare una minaccia per la mia sicurezza nazionale e, quindi, comincio a modellizzare raccogliendo informazioni, mettendo a sistema le informazioni che mi arrivano dal comparto *intelligence* e allo stesso tempo simulando ed emulando gli attacchi in laboratorio, per dire anche al legislatore e alle autorità politiche: « Siamo arrivati qua. Possiamo spingerci oltre, ma sappi che questo tipo di capacità, ove necessario, può essere attuata in questo modo. ».

Oggi questo non c'è e credo che sia fondamentale che, quantomeno a livello integrato, se ne cominci a parlare. Non ne possono parlare da soli i politici senza il supporto dell'industria, non ne può parlare l'industria, perché non avrebbe titolo senza il supporto dei politici, delle università, delle Forze armate e del comparto *intelligence*. A mio avviso questo è un tavolo non più procrastinabile che va attivato il prima possibile.

Sulla parte del *procurement*, noi abbiamo un grande strumento che è quello del perimetro di sicurezza cibernetica, che finalmente ha definito gli attori in maniera abbastanza circostanziata.

Abbiamo fatto il perimetro, ma bisogna un po' fare i perimetrati. In questo tipo di battuta si racchiude in parte la risposta, perché è chiaro che se un soggetto qualunque – non deve necessariamente far parte dell'industria della difesa – realizza un *software*, un applicativo che rientra nel perimetro, questo va certificato.

Oggi il passo in avanti che bisogna fare è che all'interno di questo perimetro – anche questo è un concetto molto dilatabile – non possono rientrarci soltanto i soggetti che hanno un obbligo di certificazione su un *software* ritenuto fondamentale perché serve a erogare servizi essenziali, perché anche nel *software* non c'è una monoliticità di *value chain*, non è pensabile, non vi sono esempi di catena del valore concentrata in un unico soggetto con quella che si chiama normalmente « un'integrazione industriale verticale » al 100 per cento.

Quasi sempre c'è un ecosistema di fornitori e spesso questi fornitori, soprattutto nella parte *software*, ad oggi sono esteri. Devono essere certificati l'erogatore e l'azienda *original equipment manifacturer* di

un certo *software*, ma anche i suoi fornitori e i fornitori spesso non stanno in Italia, aprendo così un tema che rappresenta un *vulnus* all'interno del perimetro, perché diventa complicato andare a mappare questo tipo di *value chain*, imporre degli obblighi. Infatti, laddove questi vengono percepiti come dei paletti, si portano dietro il non voler continuare a erogare un certo tipo di *software*. Inoltre, a volte non è il *software* come lo intendiamo in quanto tale, ma è il moduletto in basso a destra che diventa chiave e diventa invisibile ai più. Il tema della *value chain* – la chiamo *value chain* e non necessariamente solo *supply chain* – diventa fondamentale all'interno di una sana politica di implementazione del perimetro di sicurezza cibernetica con inevitabili ricadute sulla sicurezza nazionale.

Dove dobbiamo andare ? *Quantum communication* o *quantum computing* ? In realtà in Italia si stanno facendo investimenti in entrambi i settori. Su questo penso che debba un po' prevalere il buonsenso. Non saremo i primi al mondo né nell'uno né nell'altro, ma questo non significa che dobbiamo rinunciare a dotarci di una base tecnologica.

Se non partiamo da zero in nessuna delle due, né del *quantum computing*, né del *quantum communication*, è bene portarle avanti, perché sono stati fatti investimenti. Inoltre, devo dire che i primi prototipi sono promettenti.

Noi, tanto tempo fa, abbiamo fatto una scelta di campo di tipo politico, di tipo di sicurezza del nostro ombrello. Su questo personalmente avrei pochi dubbi nel dire: « Se abbiamo fatto un 50 per cento, l'altro 50 per cento dove lo andiamo a prendere ? ».

Ho detto che negli Stati Uniti si sta dando molto spazio al *quantum computing*, ma non è che non si stia dando spazio al *quantum communication*. Quello del *quantum computing* è una bolla più grande e ci sono degli esempi anche di aziende che cominciano a commercializzare anche in America il *quantum key distribution*.

Direi che ciò che ci manca, lo dobbiamo prendere da fuori e io, inevitabilmente, non avrei dubbi su dove rivolgermi, così come anche sulle altre materie del *cloud*, purché siano chiare delle premesse a monte su alcuni pezzi, come la sovranità delle chiavi di cifratura che devono rimanere in Italia.

Necessariamente bisogna avere forza negoziale verso gli *hyperscaler*, cioè i grandi fornitori di servizi *cloud* nel dire: « Il mio *offset*, la mia condizione è che questo tipo di chiave debba necessariamente essere una prerogativa nazionale che risponde a questo tipo di regole. ».

Siamo alla fantascienza ? Su questo la mia visione è che abbiamo fatto passi avanti enormi. Se si mette su una *timeline* ideale l'accelerazione tecnologica, tutto è avvenuto più o meno negli ultimi cinque minuti rispetto a un'ipotetica e ideale *timeline* che vede l'uomo cominciare a trasformare artificialmente la natura. Si è davanti a un progresso tecnologico velocissimo.

Per qualche macroeconomista non c'è progresso tecnologico se questo non ha delle ricadute benefiche sull'intera società; quindi, più che chiamarlo progresso tecnologico, parliamo di avanzamenti della tecnica e della tecnologia, ma a mio modo di vedere il mondo del cosiddetto « Grande Fratello » va un po' demistificato, nel senso che l'algoritmo che riesce a fare *data correlation*, *data mining* e anche *data fusion* c'è e lo stiamo applicando anche noi.

Anche in ambito militare si va verso questa forte spinta sulla necessità di andare oltre il *big data*, quindi di estrarre da grandi dati eterogenei non solo una *picture* quadridimensionale, per quanto possa essere l'abile il concetto, ma un qualcosa che mi aiuti a decidere.

Sul fatto che, rievocando un po' di fantascienza, ci sia qualcuno che decida per noi, ad oggi devo dire che, per quanto noto e per quanto noi ne sappiamo, l'*artificial intelligence* deve fare ancora molti passi in avanti. Probabilmente direi che ancora per qualche anno – mi piacerebbe dire per qualche decennio, ma questa è la realtà – possiamo applicare un certo fattore di sconto sull'*artificial intelligence* intesa come macchina che ragiona come un uomo.

Non è un futuro troppo lontano. Secondo me questo tipo di applicazione non

è dei prossimi anni, ma è chiaro che di fronte a uno scenario di questo tipo ancora una volta ci deve essere la preminenza della politica volta a dire dove si devono fermare e farlo insieme, perché se è solo l'Italia come Paese o pochi altri – un po' come avviene per il tema del clima – a poter portare avanti una tesi di questo tipo, si va poco in avanti.

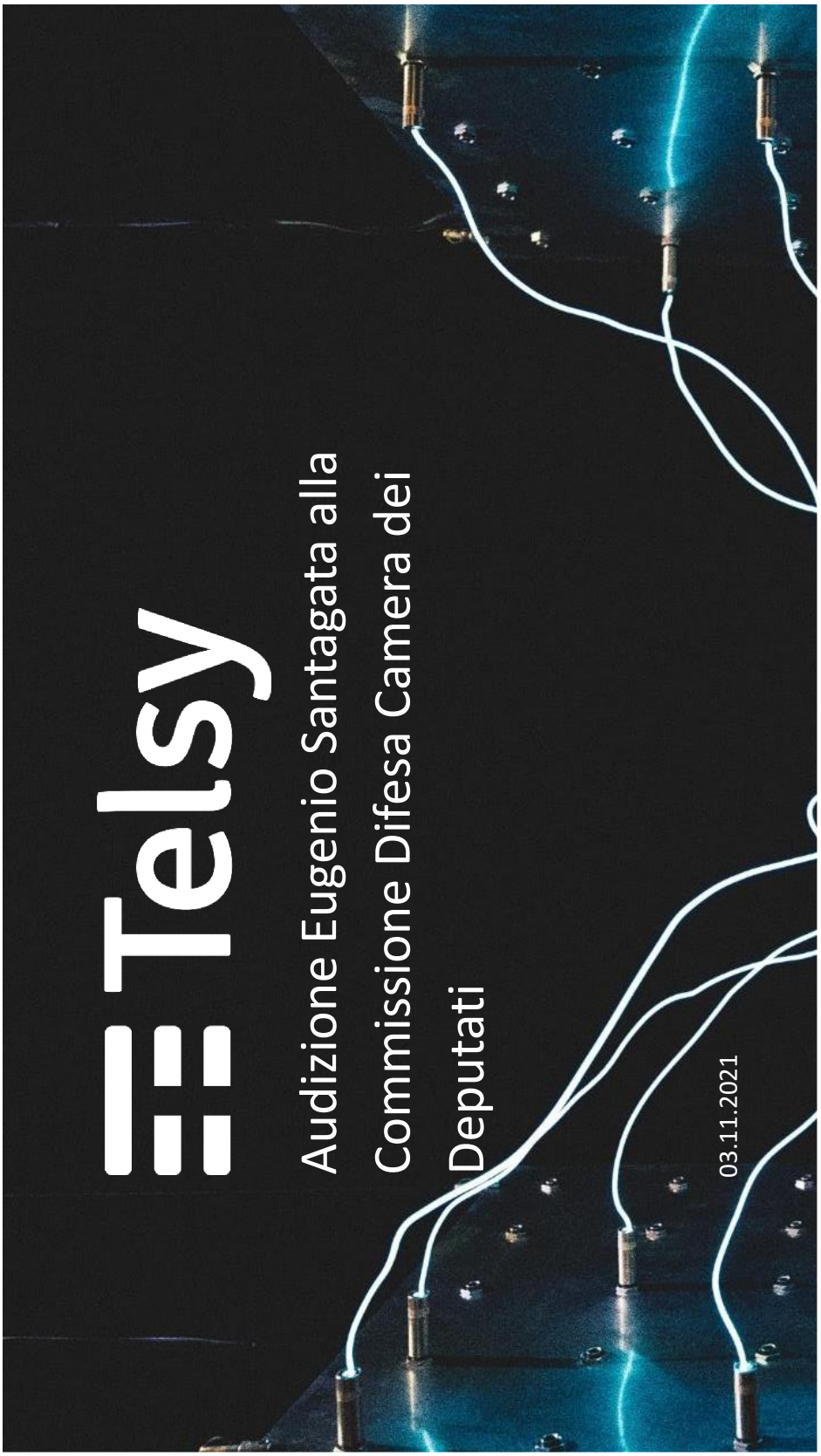
PRESIDENTE. Grazie, dottor Santagata. Io non ho altre richieste di intervento da parte dei colleghi. Rinnovo i ringraziamenti al dottor Santagata e al dottor Iannamorelli, anche per la documentazione che ci hanno consegnato e di cui autorizzo la pubblicazione in allegato al resoconto stenografico di questa audizione (*vedi allegato*). Ringrazio tutti gli intervenuti e dichiaro conclusa l'audizione.

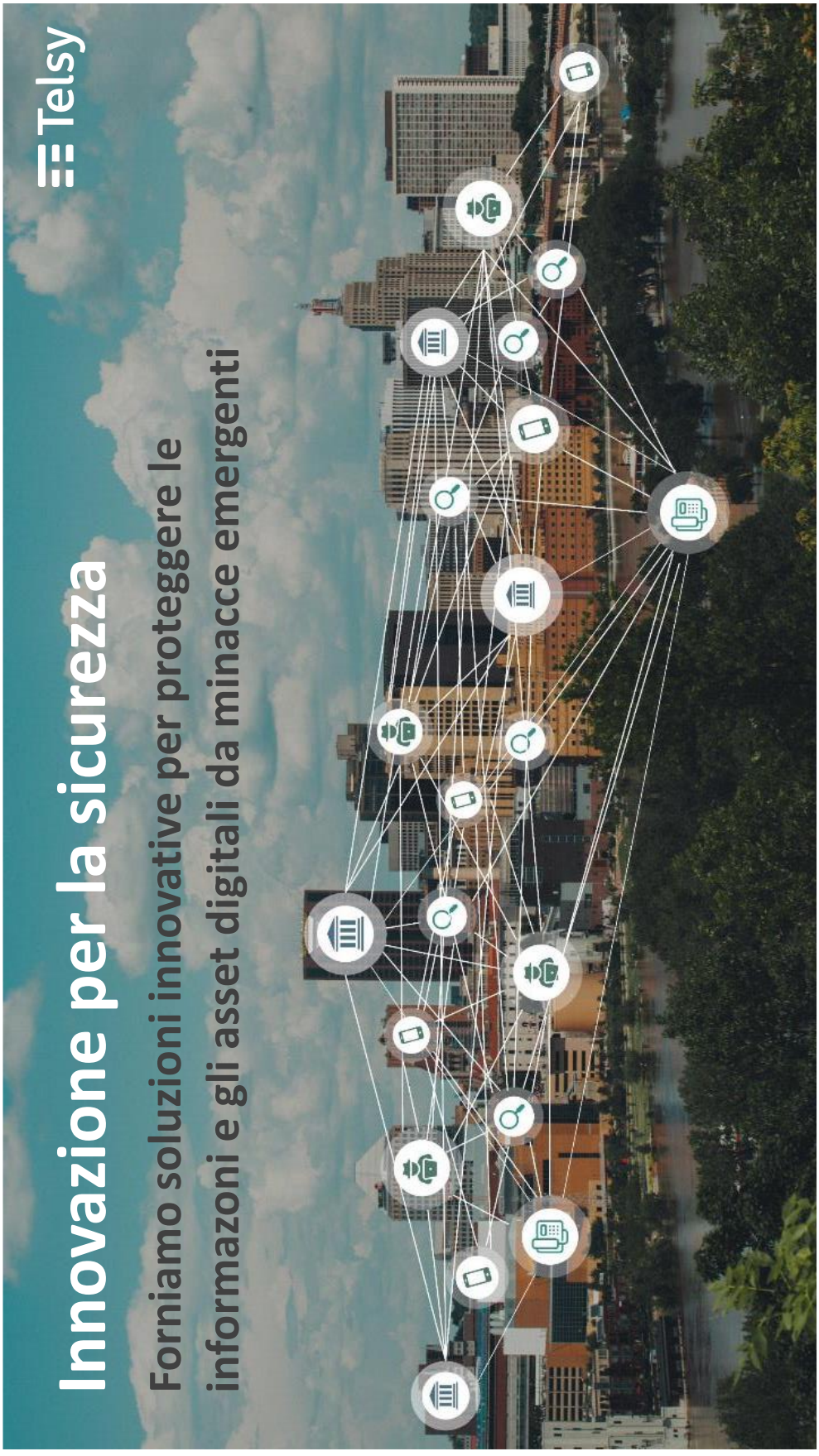
La seduta termina alle 9.50.

Licenziato per la stampa
il 24 marzo 2022

STABILIMENTI TIPOGRAFICI CARLO COLOMBO

ALLEGATO


Telsy
Audizione Eugenio Santagata alla Commissione Difesa Camera dei Deputati
03.11.2021


Telsy
Innovazione per la sicurezza
Forniamo soluzioni innovative per proteggere le informazoni e gli asset digitali da minacce emergenti

Storia

Telsy

Telsy **Elettronica e Telecomunicazioni Srl** nasce per fornire, alle forze armate e alle istituzioni governative, le soluzioni più all'avanguardia per la sicurezza delle comunicazioni radiofoniche e telefoniche

Telsy, all'avanguardia della tecnologia dell'epoca, sviluppa il suo primo apparato basato su "Digital Signal Processor" (DSP)

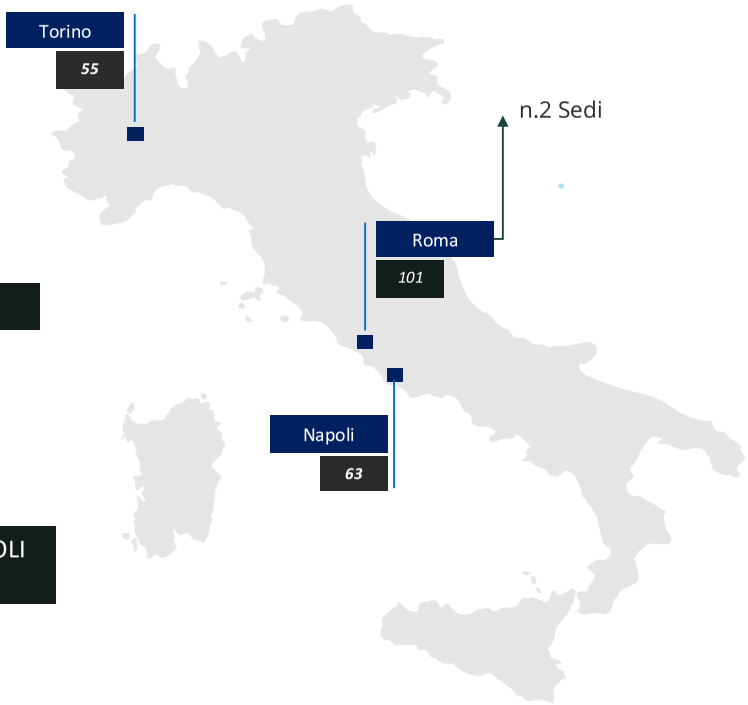
Coerente con il proprio ruolo di azienda innovativa, Telsy produce il suo primo **telefono VoIP sicuro**

Telsy entra nel Gruppo TIM, continuando l'innovazione nei sistemi di comunicazione e avviando nuove attività di ricerca ed innovazione nel settore IT

Telsy assume personale cyber altamente qualificato e diventa un **player della cybersecurity**.
Inoltre Telsy è inclusa nel **Perimetro Nazionale del Golden Power,** a prova della sua rilevanza strategica per la sicurezza nazionale

Telsy aumenta le proprie capacità cyber per supportare in maniera sicura sia la transizione verso il Cloud che l'integrazione di ecosistemi IOT con soluzioni di sicurezza firmware

Telsy oggi



219 Persone

Amministratore delegato

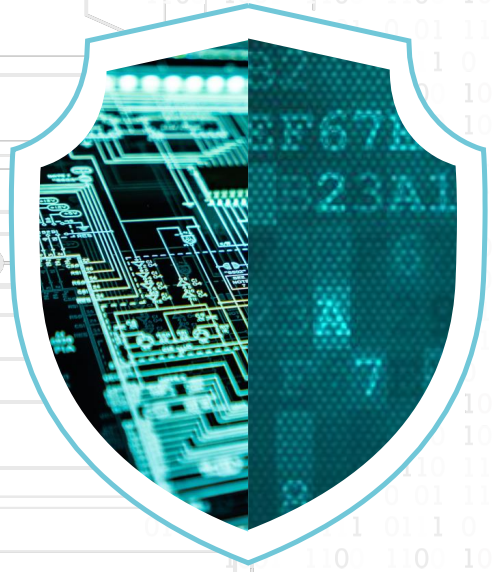
L'organico è distribuito su 3 Province: ROMA, TORINO e NAPOLI

UNA VALUE PROPOSITION INDISTRUTTIBILE

Telsy

CYBER

Proteggi la tua rete e difendi i tuoi asset digitali, con i giusti servizi cyber al momento giusto



CRYPTO

Costruisci la tua rete privata estesa per proteggere le informazioni critiche con le nostre soluzioni cripto

Telsy

Soluzioni CYBER

Decision Intelligence

IoT & Cloud Security

i-SOC & Piattaforme Proprietarie

Cyber Risk Plans & Governance

Dal design all'implementazione: lavoriamo per una strategia di sicurezza resiliente

Telsy

Disegniamo la strategia di cybersecurity più appropriata
- Cyber Risk Evaluation and Management
- Regulatory and Risk Compliance
- Business Continuity and Crisis Management
- Security Audit
- Security Training and Awareness
- Disaster Recovery Plan

Costruiamo una rete sicura con le giuste soluzioni
Firmware security
- Cloud security
- Infrastructure Security
- Data Protection

Continuo monitoraggio della rete e response
- Security Assessment
- Monitoring and Incident Response
- Incident Handling L1/L2
- Decision Intelligence
- Cyber Threat Intelligence

i-SOC PER SERVIZI AVANZATI DI SICUREZZA GESTITA

Telsy

Proteggere il network con i giusti servizi al momento giusto

Il SOC di Telsy offre una vasta gamma di servizi basati sulle ultime tecnologie, sia comuni che proprietarie, fornite da personale **altamente qualificato e certificato**

Il nostro **focus sull'innovazione e la nostra competenza** in prodotti di sicurezza ci rendono un partner fidato e un player ben consolidato nella gestione reti e di informazioni sensibili

Serviamo **clienti top tier**, gestendo l'intero ciclo di vita di un attacco cyber

- **Penetration Testing**
- **Vulnerability Assessment**
- **Blue Team/Red Team**
- **Incident Response Team**
- **Code Review**
- **Cyber Threat Intelligence & SOAR**

PIATTAFORMA PROPRIETARIA DI THREAT INTELLIGENCE

Telsy

Comprendere le minacce emergenti per proteggere le reti critiche con Odino

Proteggere infrastrutture critiche da minacce sofisticate e persistenti, come le APT, richiede approcci sofisticati basati sull'accesso tempestivo ad informazioni aggiornate

La piattaforma di threat intelligent di Telsy, Odino, è costruita per supportare la difesa predittiva e proattiva di fronte a minacce cyber che mirano a sabotare infrastrutture critiche

Valore Aggiunto

- Accesso diretto ad informazioni complete fornite da un database proprietario integrato con varie fonti e visualizzato attraverso un'interfaccia intuitiva
- Affina l'approccio difensivo dell'organizzazione accedendo a report su misura riguardo minacce classificate per verticali, grazie al team di threat intelligence di Telsy

IoT FIRMWARE SECURITY

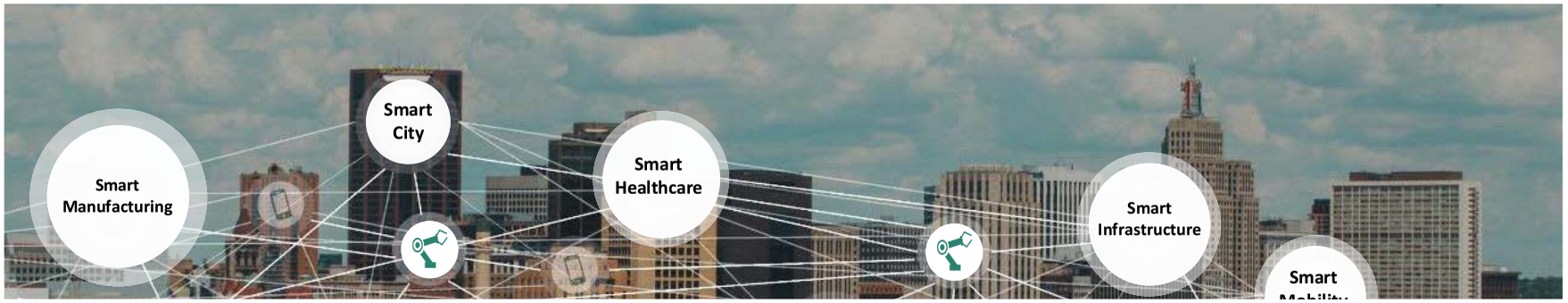
Sicurezza integrata con un approccio secure-by-design

Telsy

Mantenere un approccio **secure-by-design a livello firmware** non è solo essenziale per proteggere gli apparati edge dalle minacce cyber, ma permette anche ai produttori di **IoT di ottenere la visibilità, la sicurezza e il controllo** di cui necessitano per poter offrire al cliente dispositivi **connessi in totale sicurezza**

Il nostro approccio

- **Identificare** falle di sicurezza e porvi rimedio anticipatamente per minimizzare i rischi ed evitare di commettere violazioni di compliance rispetto ai nuovi regolatori
- **Integrare** la sicurezza a livello firmware fornendo ai produttori di IOT supporto nell'implementazione di buone pratiche, per rafforzare la sicurezza, che siano concrete e praticabili
- **Migliorare** la sicurezza dei dispositivi IoT lungo il loro ciclo di vita attraverso politiche di controllo degli accessi, aggiornamenti software e servizi data-driven



SERVIZI DI CLOUD SECURITY

Telsy

Mettere in sicurezza l'intero ciclo di vita dei tuoi dati

I servizi di sicurezza cloud di Telsy aiutano a disegnare una strategia di sicurezza cloud completa che include attività di **risk management e orchestration**, garantendo la sicurezza delle persone che lavorano da remoto, da qualunque posto

Valore aggiunto

- Definire una **strategia di sicurezza** cloud chiara e **omnicomprensiva**
- Navigare le complessità dei servizi cloud agendo a livello di **prevenzione rischi**
- **Soluzioni efficaci e convenienti** inclusive di pratiche e architetture standardizzate, potenziate dall'automazione

Cosa facciamo

CASB

Visibilità, compliance, data security, e threat protection per i servizi basati sul cloud, garantendo un accesso utente sicuro, anche da remoto

SASE

Proteggere il network ampliato e il software-defined edge networking, tramite autenticazione focalizzata sull'utente e il controllo degli accessi, il tutto integrato in maniera seemless nel cloud

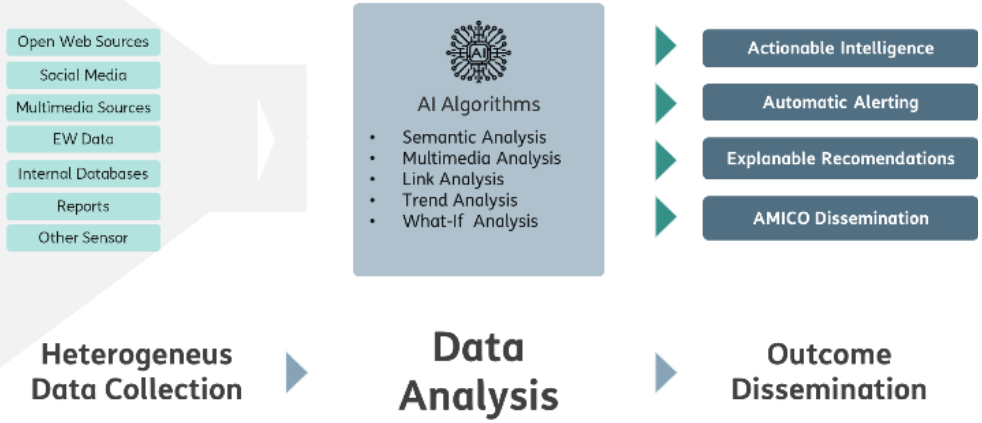
DECISION INTELLIGENCE AVANZATA

Processi di decisione aumentati ed automatizzati

Telsy

Prendi le **giuste decisioni** con una piattaforma basata su **algoritmi di IA** che trasforma i dati in informazioni di valore e fornisce Decision Augmentation

System Architecture



Telsy

Soluzioni CRYPTO

App di messaggistica sicura & videoconferenza

Telefoni cripto

Cifranti

CIFRANTI TELSY (1/3)

Proteggere le informazioni sensibili costruendo un network privato

Telsy

Sirio
Risponde al bisogno di proteggere le reti delle varie architetture e di garantirne l'adattabilità a qualsiasi utilizzo, sia desktop che rack

Vega
Disegnato per assicurare alta velocità, bassa latenza e la crifratura e la decifratura del traffico fino a 10 Gb/s. Ideale per scambiare informazioni tra il Centro di Elaborazine Dati e il sito di backup per eventuali piani di Disaster Recovery

Hypnos
L'ultima innovazione tra le cifranti Telsy, concepita per soddisfare I nuovi bisogni di sicurezza dal momento che risulta compatibile con dispositivi QKD

Valore Aggiunto

- Supply chain italiana garantita
- Pieno controllo della soluzione con la possibilità di implementare algoritmi nazionali proprietari e di ispezionare la piattaforma
- Soluzioni Quantum Resistant

TELEFONI CRYPTO TELSY

Estendere la rete privata garantendo la crifratura end-to-end delle comunicazioni

Telsy

Telefoni cripto T2

Il più iconico dei telefoni crypto Telsy. Garantisce la cifratura delle comunicazioni sia sul protocollo pubblico PSTN (Public Switched Telephone Network) sia su quello VoIP (Voice over IP).

SETEL T1 “Pillow”

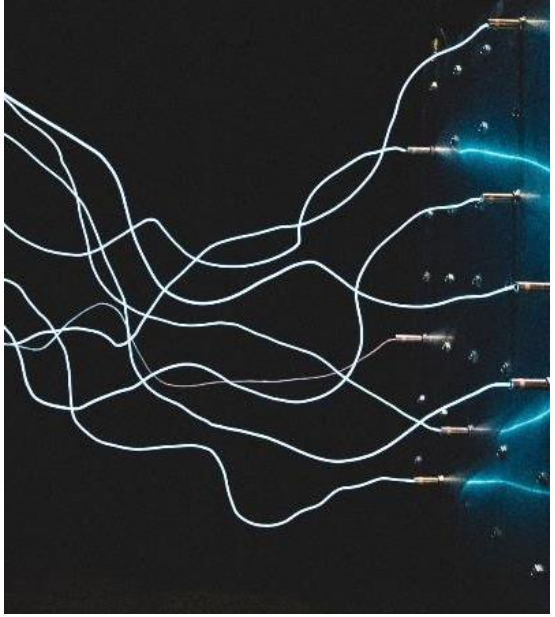
Transforma gli apparati commerciali in telefoni cifranti aggiungendo capacità crittografiche senza sostituire l’attrezzatura fornita.

Valore aggiunto

- Eccelente facilità d’uso, garantendo una user experience simil free-to-air terminals e alta qualità audio tramite l’utilizzo di codecs avanzati
- Garantisce il più alto livello di sicurezza quando connesso ad altri telefoni cripto, permettendo allo stesso tempo di effettuare chiamate in chiaro su regolari telefoni (PSTN or VoIP)
- Disponibile in versione SCIP (Secure Communications Interoperability Protocol) compliant con le specifiche NATO

TELEFONI CRYPTO TELSY

Fornire telefoni cripto altamente sicuri



Telsy

Telefono cripto T2
Un telefono che agisce da gateway per accedere ai servizi forniti dal TSCS (Telsy Secure Communication System), come ad esempio e-mail, fax criptato e file sharing

SETEL T1 "Pillow"
Costituito dalla cifrante desktop SETEL T1 "Pillow," il suo token crittografico, e da un Key Distribution Center KDC SETEL. Attualmente disponibile nella versione SCIP compliant con le specifiche NATO

APP DI MESSAGGISTICA PROPRIETARIA

Telsy

Connettersi alla propria rete ovunque, in qualunque momento

App
Un sistema di comunicazione istantanea costruito per condividere informazioni sensibili in assoluta sicurezza pur mantenedo la stessa usabilità delle app di comunicazione più commerciali

Smartphone hardenizzati
Aumentano la sicurezza di telefoni mobili commerciali al massimo livello, bloccando l'apparato da intrusioni esterne

Valore aggiunto

- Pieno controllo sull'infrastruttura e sulle informazioni attraverso l'installazione on premise
- Sicurezza in semplicità grazie alla cifratura end-to-end e ai protocolli proprietari, pur mantenedo una user experience intuitiva
- Prevenire intrusioni nel proprio network attraverso la gestione centralizzata delle iscrizioni utente

SOLUZIONE DI VIDEOCONFERENZA

Proteggere il lavoro in team riducendo le distanze

Per rispondere al crescente bisogno di proteggere le comunicazioni in smartworking, la soluzione di videoconferenza di Telsy permette agli utenti di condividere informazioni sensibili e critiche senza doversi fidare di terze parti commerciali

Telsy

Valore aggiunto

- Pieno controllo sull'infrastruttura e sulle informazioni attraverso l'installazione on-premise
- Fornisce crittografia end to end garantendo allo stesso tempo l'usabilità di simili piattaforme commerciali

Telsy

R&D

APT Detector

SOC Automation

Soluzioni
Quantum Resistant

19

I NOSTRI OBIETTIVI DI RICERCA

Imparare ed innovare per rimanere al passo con i bisogni in evoluzione

Telsy

Quantum Resistant

Guidati dal bisogno di garantire **la sicurezza delle informazioni in un mondo quantum**, pur raccogliendo i benefici della tecnologia quantum per **rafforzare la sicurezza delle comunicazioni**

Stiamo lavorando a:

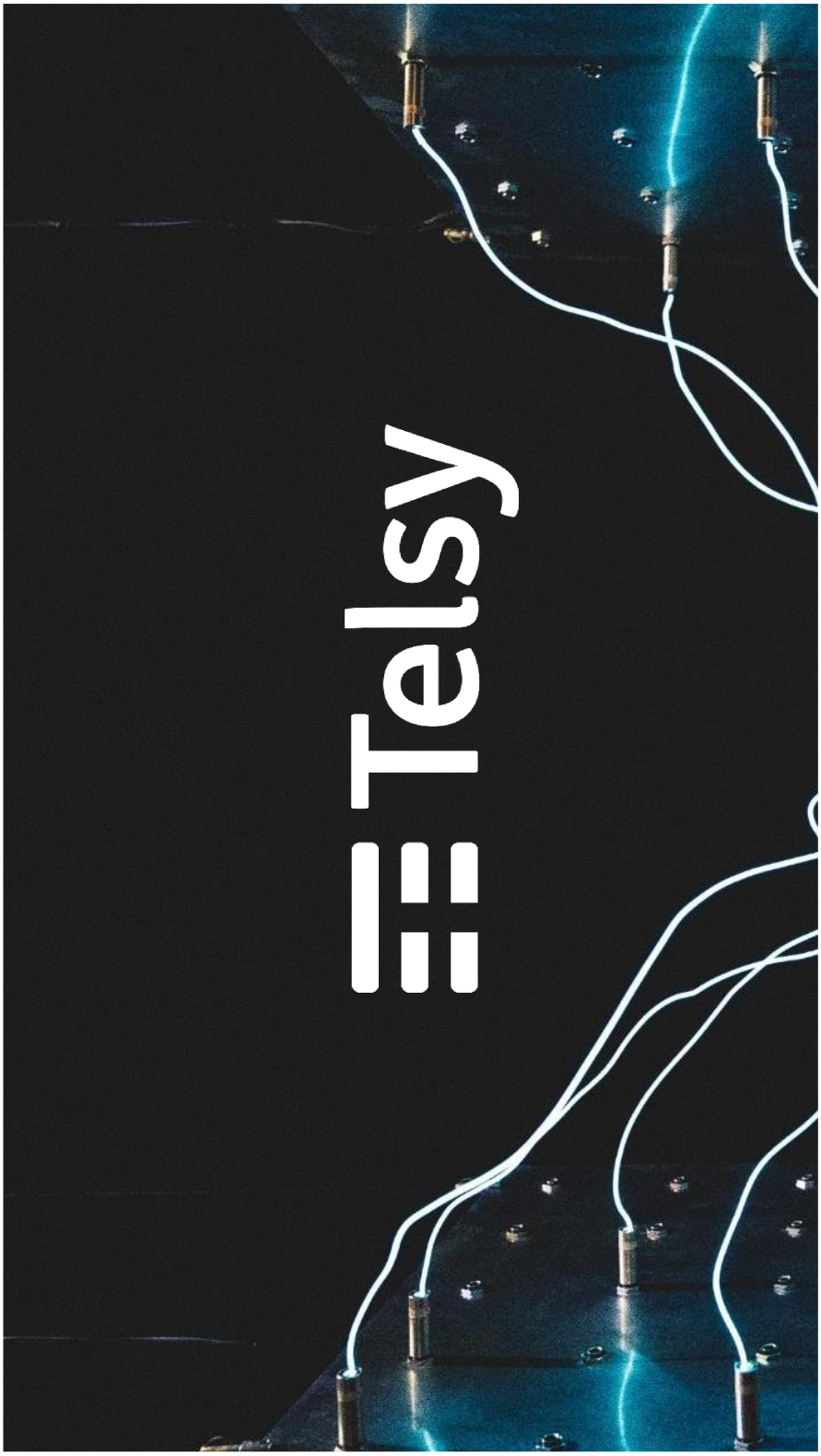
- Una soluzione **QKD (Quantum Key Distribution)**, che applichi le proprietà fisiche del quantum per garantire un più alto standard di sicurezza rispetto agli attuali metodi di cifratura
- **Crittografia Post Quantum**, che renda le soluzioni crypto resistenti alle future tecniche quantistiche e alla loro distruttiva capacità computazionale

SOAR Automation

Piattaforma di **Security Orchestration and Automation Response (SOAR)** che rafforzi le capacità del SOCs nell'analizzare e protamente mitigare minacce sofisticate ed automatizzate, attraverso l'implementazione di tecniche di machine learning

Stiamo lavorando ad una **piattaforma proprietaria** che:

- Garantisca una **detection estesa e real time**, per una mitigazione early-stage
- Combini attività uomo-macchina per un **vero approccio olistico** alla sicurezza



18STC0167100