Cyber Warfare 2021-2022

Cibersicurezza: dalla collaborazione Pubblico-Privato alla difesa dello Stato

a cura di Umberto Gori

FrancoAngeli

Collana di Scienza Politica e Relazioni Internazionali, diretta da Umberto Gori

Il progresso delle scienze sociali è strettamente legato alla ricerca interdisciplinare. Tale indirizzo non ostacola però l'applicazione di un approccio e di un metodo rigorosamente unitari. L'approccio è quello dei sistemi, il metodo è quello della scienza politica più avanzata. L'uno e l'altro mirano a conoscere il reale nella sua complessità, a partire da dati e variabili fattuali, con l'ausilio, anche, di discipline diverse, teorie empiriche e quindi previsioni aventi valore probabilistico.
C'è una fortissima domanda, oggi, di strumenti aggiornati atti ad interpretare fenomeni complessi e talora privi di precedenti ed a consentirne la previsione, data l'accelerazione dei tempi storici.
A questa domanda la «Collana di Scienza Politica e Relazioni Internazionali» si propone, ambiziosamente, di rispondere, cercando anche di rimuovere, in misura progressiva, le resistenze, ancora vive nel nostro Paese, dovute al tradizionale convincimento che il campo sociale non sia coltivabile con gli strumenti euristici che hanno determinato lo sviluppo eccezionale delle scienze della natura.
La denominazione della collana si giustifica per due aspetti: primo, perché di solito quando si parla di scienza politica si pensa al quadro interno e qui invece si vuole accreditare la tesi che anche il sistema internazionale è analizzabile in tale prospettiva; secondo, perché anche per l'analisi corretta del sistema interno è ormai impensabile non fare un sistematico riferimento al contesto internazionale (e viceversa).
La collana svilupperà sia una parte di metodologia e di tecniche analitiche, sia una parte teorica e di ricerca sugli aspetti di sostanza del vasto campo preso in considerazione. Contribuiranno all'una e all'altra metodologi e scienziati politici, sociologi della politica e studiosi dell'amministrazione, comparatisti e cultori di relazioni internazionali.
La collana ha essenzialmente un taglio operativo. I suoi naturali destinatari saranno quindi, oltreché gli specialisti, anche tutti coloro che, ai diversi livelli, sono detentori di responsabilità decisionali. Scopo ultimo è infatti la progressiva «modernizzazione» dell'Italia nel campo della valutazione scientifica dei fatti politici, interni ed internazionali, che è premessa insieme di razionalizzazione dei processi decisionali e di un corretto funzionamento delle istituzioni e della vita democratica del Paese.

Cyber Warfare 2021-2022

Cibersicurezza: dalla collaborazione Pubblico-Privato alla difesa dello Stato

a cura di Umberto Gori

FrancoAngeli

Il presente volume racchiude l'edizione, svoltasi in forma digitale, del 15 dicembre 2021 e le due edizioni tenutesi nel 2022, rispettivamente a Firenze il 9 giugno 2022, presso l'Istituto di Scienze Militari Aereonautiche, e a Milano il 30 novembre 2022, presso il Belvedere Jannacci – Grattacielo Pirelli.
Gli eventi sono stati promossi dal Centro universitario di Studi Strategici, Internazionali e Imprenditoriali (CSSII), European Center for Advances Cyber Security (EUCACS), Cyber Academy, in collaborazione con NetConsulting, Associazione Italiana Professionisti Security Aziendale (AIPSA), Associazione Italiana per la Sicurezza Informatica (CLUSit), Regione Lombardia, ICMQ, CERSA, d'intesa con InTheCyber Group.

Il curatore ringrazia Simonetta Gallucci, Davide Manico e Francesca Pierdominici per la preziosa collaborazione nella revisione e messa a punto redazionale del volume.

Il curatore si scusa con le lettrici e i lettori per l'abuso della fraseologia cyber in testi italiani.

Indice

Edizione 2022
Politica Interna e Politica Estera nell'era cibernetica: verso la Ciberocrazia?

Prefazione

di *Paolo Lezzi*[1]

Questo volume contiene gli atti di 3 edizioni della Conferenza Nazionale sulla Cyber Warfare, una nel 2021 e due nel 2022. Tali appuntamenti si sono svolti, come ormai consuetudine, in forma ibrida, ovvero un ristretto numero di persone in presenza, per lo più speaker ed autorità, e la restante parte dell'audience connessa in videoconferenza. La prima edizione si è svolta a Roma il 12 dicembre sul tema "Agenzia per la Cybersicurezza Nazionale: funzione di guida per la resilienza Cyber ed opportunità di sviluppo economico del Paese" che ha salutato la nascita dell'agenzia e del potenziale nuovo assetto Cyber del Paese. La seconda ha avuto luogo il 9 maggio presso la suggestiva ex Scuola di guerra aerea ora Istituto di Scienze Militari aeronautiche (ISMA) di Firenze incentrata sull'innovativo tema "Politica Interna e Politica Estera nell'era cibernetica: verso la Ciberocrazia?" dove sono emersi opportunità e rischi del profondo cambiamento che l'era Cyber sta portando nella Res Publica, nella sua gestione e nelle relazioni internazionali. La terza ed ultima del 30 novembre è stata ospitata al 30' piano del Grattacelo Pirelli sul tema "Le sfide della Cyber Security al Comparto Produttivo", dove a partire dalla fotografia dello stato dell'arte della postura di sicurezza delle principali aziende italiane, si è evidenziata la road map necessaria ad un'evoluzione fattiva e collaborativa con il coordinamento pubblico-privato da parte di ACN.

L'Italia ha intrapreso un importante percorso verso la Ciberdifesa complessiva del Paese ed ha assegnato compiti e ruoli ben distinti tra le diverse istituzioni. Ora è necessario perseguirlo e realizzarlo con entusiasmo e decisione, coinvolgendo attivamente le migliori risorse presenti, siano esse le stesse istituzioni come le imprese private e le accademie.

[1] Vicepresidente Esecutivo EUCACS, CEO InTheCyber Group.

Riconoscimenti

Edizione 2021
Agenzia per la cybersicurezza nazionale: funzione di guida per la resilienza cyber ed opportunità di sviluppo economico del Paese

Promotori
European Center for Advanced Cyber Security (EUCACS)
Centro universitario di Studi Strategici, Internazionali e Imprenditoriali (CSSII)
Cyber Academy

Ideato d'intesa con InTheCyber Group

Con la collaborazione di
NetConsulting
AIPSA
CLUSit
ICMQ
CERSA

Con la sponsorship di
Accenture
Cisco
Capgemini
RSA
Tinexta Cyber
TIM
Google Cloud

Con il patrocinio di
Ministero della Difesa

Riconoscimenti

Edizione 2022
Politica Interna e Politica Estera nell'era cibernetica: verso la Ciberocrazia?

Promotori
European Center for Advanced Cyber Security (EUCACS)
Centro universitario di Studi Strategici, Internazionali e Imprenditoriali (CSSII)
Cyber Academy

Ideato d'intesa con InTheCyber Group

Con il patrocinio di
Ministero della Difesa

Riconoscimenti

Edizione 2022
Le sfide della Cyber Security al comparto produttivo

Promotori
European Center for Advanced Cyber Security (EUCACS)
Centro universitario di Studi Strategici, Internazionali e Imprenditoriali (CSSII)
Cyber Academy

Ideato d'intesa con InTheCyber Group

Con la collaborazione di
Regione Lombardia
NetConsulting
AIPSA
CLUSit

Con la sponsorship di
Cisco
DedaCloud
NetWitness
NTT Data
RSA
ZScaler
Corvallis
OVH Cloud

Con il patrocinio di
Ministero della Difesa

Edizione 2021

Agenzia per la cybersicurezza nazionale: funzione di guida per la resilienza cyber ed opportunità di sviluppo economico del Paese

Prolusione

di *Michele Colajanni*[1]

Benvenuti alla XII edizione della conferenza nazionale sulla Cyber Warfare, una conferenza che viene da molto lontano. Nasce nel 2010 grazie a due grandi persone: il Senatore Generale Luigi Ramponi e il Professor Umberto Gori, che mi hanno incaricato di prendere il testimone di questo evento che ha avuto, al suo nascere, altre due importanti figure: il Professor Roberto Baldoni, uno dei fondatori di questa conferenza, e l'Ingegner Paolo Lezzi, persona chiave dal punto di vista operativo e principale artefice anche della giornata odierna.

La giornata sarà densa di interventi della massima importanza. Si aprirà con i saluti del Senatore Adolfo Urso, Presidente del Copasir, cui seguirà l'intervento del Professor Baldoni, oggi a capo dell'ACN. La prima tavola rotonda vedrà i rappresentanti della sicurezza e cybersecurity delle principali aziende nazionali che sarà conclusa dall'intervento dell'Onorevole Giorgio Mulè, sottosegretario del Ministero della Difesa. È prevista, infine, una seconda tavola rotonda con rappresentanti delle principali aziende italiane.

Iniziamo la giornata invitando il Presidente del Comitato parlamentare per la sicurezza della Repubblica, Senatore Adolfo Urso, che ci onora della sua presenza, per introdurci al fondamentale tema della sicurezza del Paese che oggi passa anche attraverso la cybersecurity e la difesa cyber delle infrastrutture critiche ed economiche nazionali.

[1] Presidente European Center for Advanced Cyber Security (EUCACS), Ordinario di Ingegneria Informatica presso l'Università di Bologna.

Indirizzo di saluto

di *Adolfo Urso*[1]

Rivolgo un ringraziamento agli organizzatori di questo meeting annuale per l'invito che mi avete inoltrato.

Il Comitato Parlamentare per la Sicurezza della Repubblica di cui sono presidente è, come voi sapete, un organo parlamentare che ha come peculiarità quella di svolgere i propri lavori in segretezza e riservatezza.

Tuttavia, in questo caso, si tratterà di parlare di un argomento di cui vi è assoluto bisogno; non solo per gli addetti ai lavori, quali voi siete, ma anche, e più in generale, per i nostri cittadini affinché, qualunque sia la loro attività, ne siano pienamente consapevoli e soprattutto perché la cybersicurezza, come è stato dimostrato con chiarezza dagli eventi degli ultimi mesi, riguarda ciascuno di noi.

Nell'epoca del lockdown, è bastato che un lavoratore portasse il proprio lavoro nel proprio domicilio per far venir meno gli elementi di sicurezza, e diventare una finestra d'accesso a una rete estremamente vulnerabile.

Ebbene, il Comitato Parlamentare per la Sicurezza della Repubblica, già nella scorsa legislatura, è più volte intervenuto a tal proposito con un documento al Parlamento.

Ai tempi della prima relazione pubblica alle Camere e dopo un anno di indagine secretata, l'allora presidente Guerini ed io, in quanto suo vice, elaborammo un documento approvato all'unanimità dal Comitato. In tale documento chiedevamo al Parlamento, e di conseguenza al Governo, di intervenire per colmare una lacuna e per realizzare una struttura (all'epoca si parlava di una fondazione o di un'agenzia) che poi finalmente è nata, seppure con oltre dieci anni di ritardo rispetto ad altri Paesi europei. Mi riferisco innanzitutto alla Germania e alla Francia che, essendo tra i Paesi fondatori della Comunità Europea e quelli dalla più larga dimensione demografica e industriale, hanno qualche diritto e dovere in più rispetto agli altri Paesi dell'Unione.

Finalmente questa lacuna è stata colmata. È stato riconosciuto al Comitato il ruolo di garanzia, di controllo, di impulso più ampio, seppure ne

[1] Presidente del COPASIR.

svolgesse già uno, in delega del Parlamento, per le agenzie di intelligence ovvero i nostri servizi segreti. E questo ruolo più vasto è chiaro sin dalla denominazione "Comitato Parlamentare per la Sicurezza della Repubblica" che, a differenza dell'organismo precedente ovvero il Comitato parlamentare di controllo sui servizi segreti (COPACO), sovrintende a tutta l'ampia e sempre più estesa sfera della sicurezza nazionale.

In questo ambito certamente vi è la cyber security o comunque tutta la tematica del cyber perché tale è nell'evoluzione del contesto interno e internazionale. Di conseguenza anche l'Agenzia fa riferimento al Comitato parlamentare per la sicurezza della Repubblica (COPASIR).

In queste ore, per esempio, stiamo attendendo l'ultimo schema di regolamento per completare l'assetto istituzionale dell'Agenzia.

Come prevedeva la legge, ne abbiamo già esaminati tre, dando celermente il nostro parere anche sull'ultimo che riguarda l'assetto e le norme inerenti gli appalti e le forniture. Questo perché, essendo il nostro Paese vulnerabile forse più di altri, riteniamo impellente il fatto di realizzare al più presto l'Agenzia per la Cybersicurezza Nazionale. Impellente non solo per la Pubblica Amministrazione nella quale, come ha detto ripetutamente il ministro Colao, vi sono i dati dei nostri cittadini: (dati sanitari, dati delle imprese, dati fiscali e tutto quello che poi è la vita di ogni cittadino e di ogni impresa), ma anche perché credo che l'Agenzia possa contribuire a far acquisire una maggiore conoscenza ai cittadini e alle aziende rispetto a come tutelare il proprio "giardino di casa".

Ciascuno deve tutelare il proprio computer, il proprio cellulare, perché questo non diventi l'elemento di vulnerabilità del Sistema. È evidente che il lockdown e le misure attuate per contrastare la pandemia hanno allargato a dismisura la superficie vulnerabile. Quello che sarebbe avvenuto nell'arco di qualche anno o decennio; per decisione del Governo è avvenuto in poche settimane allargando a dismisura la superficie dell'attacco.

E di cosa parliamo? Parliamo di quello che l'Alleanza Atlantica ha recentemente definito il quinto dominio bellico ovvero della Cyber, paragonandolo così agli altri quattro domini tradizionali.

Per millenni siamo stati abituati ad avere due domini: quello del mare e quello della terra. Nel secolo scorso, durante la Prima guerra mondiale, si è aggiunto il dominio del cielo. In tempi più recenti si è aggiunto il quarto dominio, quello dello spazio, che ha messo in competizione le potenze di ogni parte del globo.

Il dominio della Cyber è significativo perché innerva ogni attività. Esso riguarda non solo lo spazio tecnologico e quindi le difese che vanno prese.

Ricordo, per esempio, che in quella relazione all'inizio della legislatura individuammo una vulnerabilità di sistema anche nell'utilizzo della tecnologia cinese nel nostro sistema di telecomunicazione.

Il dominio della Cyber è significativo anche perché la Cyber invade ogni ambito della nostra vita, della nostra esistenza, della nostra economia: per questo necessita di una resilienza del Paese. Ed è per questo che è giusto dire che tutti devono essere capaci di tutelare il proprio giardino di casa.

Questo credo sia importante comprenderlo e mi fa piacere essere stato invitato in un meeting alla sua dodicesima edizione. Vuol dire che qualcuno ne aveva compreso l'importanza dodici anni fa, quando Paesi come la Francia e la Germania facevano i loro primi approcci nelle loro strutture simili alla nostra Agenzia e l'Italia, purtroppo, era in ritardo per tanti motivi.

Per colmare questo ritardo ci fu un tentativo del governo Gentiloni, senza risultati e del governo Conte due, anche questo senza risultati. Infine vi è riuscito il governo Draghi con il supporto del Parlamento e anche grazie allo stimolo del Comitato Parlamentare per la Sicurezza della Repubblica, chiunque l'abbia presieduto in questi tre anni.

In conclusione, mi fa piacere ricordare una figura importante tra coloro che hanno avuto l'intuizione di creare questo meeting. Mi riferisco a un caro amico, il Generale Luigi Ramponi.

È stato colui con il quale mi confrontai nella mia prima avventura elettorale. Nel 1994 egli era candidato nel collegio senatoriale di Prati e di Primavalle, a Roma. In quelle prime elezioni maggioritarie, io ero candidato nel medesimo collegio, ma per la Camera dei Deputati. In quell'occasione svolgemmo insieme la campagna elettorale. Lo conobbi pochi mesi prima perché lui fu uno degli artefici della Fondazione di Alleanza Nazionale ed io, come coordinatore dei comitati promotori, ne accolsi l'ingresso in politica. La sua fu un'esperienza importante non solo come comandante generale della Guardia di Finanza, ma anche per l'intelligence italiana. Aveva la capacità di capire cosa stesse accadendo e, soprattutto, cosa sarebbe accaduto. Una capacità che lo ha accompagnato anche nella sua attività parlamentare e, a conclusione di questa, anche nell'ideazione di questo particolare e significativo meeting. Un meeting che, evidentemente proprio quando pochi comprendevano cosa stesse per accadere, è servito a tenere accesa una lampadina nel buio dell'ignoranza del Paese.

Oggi il Paese si è svegliato, esprimo il mio augurio all'Agenzia per quello che in poco tempo dovrà fare affinché il Paese sia più attrezzato a confrontarsi con questa nuova realtà.

Buon lavoro a tutti.

Il ruolo guida dell'Agenzia per la Cybersicurezza Nazionale (ACN) verso la Cyber-Resilienza Nazionale: sinergie pubblico-private

di *Roberto Baldoni*[1]

Sono felicissimo di essere qui a parlare di un tema ormai strategico per il Paese quale la cybersicurezza. É chiaro che di strada, negli anni, ne abbiamo fatta tanta e, alla fine, come ricordava il Presidente Urso, siamo arrivati, seppure con vent'anni di ritardo, alla definizione di una struttura che dovrà guidare la resilienza nazionale.

È un lavoro complesso e chiunque conosca o abbia un'idea della complessità che ha portato il mondo digitale, sa di quello di cui parliamo. Lavoro che non si fermerà alla parte tecnica perché avremo, come ha detto anche il Presidente, la gestione della politica di consapevolezza a livello nazionale, che dovrà essere portata avanti insieme a una politica di creazione di competenze e a una politica legata allo sviluppo tecnologico.

Sentiamo infatti spesso parlare del concetto di sovranità digitale, soprattutto coniugato a livello europeo. Ma tutti noi sappiamo che non si può parlare di sovranità digitale senza produrre tecnologia. Non si può parlare di sovranità digitale senza avere una workforce adeguata. Non si può parlare di sovranità digitale senza una consapevolezza diffusa.

Quindi dobbiamo migliorare in modo rapido e marcato all'interno di tutti questi settori ed è per questo che è nata l'Agenzia per guidare e sostenere questo miglioramento.

Negli ultimi anni non abbiamo corso come hanno corso gli altri Paesi su questi aspetti chiave. Ma non partiamo da zero: sono quattro anni che lavoriamo per creare una capacità nazionale di cybersecurity. Lo abbiamo fatto all'interno di un comparto che non finirò mai di ringraziare per l'opportunità di crescita che ci ha dato.

Questo impegno ha portato, come risultato più eclatante nel mondo aperto, al perimetro di sicurezza nazionale cibernetica che ha permesso, in modo sistematico e usando un concetto di analisi del rischio, di vedere come

[1] Direttore dell'Agenzia per la cybersicurezza nazionale, ACN.

si potevano andare a mettere in sicurezza gli asset più importanti del nostro Paese.

La cyber security, tuttavia, rispetto al mondo dell'intelligence, è information sharing, è collaborazione continua con le aziende e la pubblica amministrazione, è collaborazione con i cittadini, è consapevolezza diffusa. Credo sia stato questo uno dei fattori più importanti che ha poi portato alla nascita dell'Agenzia.

Quindi l'Agenzia per la Cybericurezza Nazionale ha già una serie di linee sulle quali operare.

Mi riferisco, in particolare, alla parte di prevenzione e mitigazione degli incidenti. Abbiamo un Computer Security Incident Response Team (CSIRT) attivo all'interno dell'Agenzia, che rappresenta un capo maglia di una rete a cui appartengono tutte le organizzazioni strategiche del Paese e a cui bisogna guardare, seguendo le mitigazioni suggerite in quelle situazioni particolari in cui vanno messi in sicurezza i sistemi. Il CSIRT rappresenta uno dei pilastri delle iniziative che l'Agenzia vuole portare avanti.

Un percorso molto difficile e complesso che però ha visto i primi passi di realizzazione negli scorsi mesi, con una modalità talmente veloce da essere inusuale per una Pubblica Amministrazione. Come ha detto il Presidente Urso, il 10 aprile è stata presa la decisione politica di portare avanti l'Agenzia. Il 14 giugno è stato portato in Consiglio dei ministri il Decreto-legge che la istituiva e il 1° settembre l'Agenzia è nata con dieci persone. Ora siamo settantacinque e veleggiamo verso i novanta, che è il numero di persone che dovremmo avere in prima fase (n.d.r. dicembre 2021). Ci confrontiamo con Paesi che hanno milleduecento persone all'interno delle loro agenzie e questo è un confronto né facile né semplice.

Tuttavia, i passi in avanti fatti dalla cyber security a livello nazionale sono riscontrabili attraverso documenti e fatti inoppugnabili.

Si pensi al toolbox per il 5G approvato in Europa, che ha visto l'Italia come Paese leader, ora base del lavoro legato all'applicazione dell'articolo 1-bis della legge Golden-Power Nazionale. Si pensi alla rete CyCLONe, che ha messo in contatto tutte le agenzie europee e che ha permesso di coordinarci per l'uscita dei bollettini sull'ultima vulnerabilità, impatti e mitigazioni, dove Francia e Italia hanno trainato le altre nazioni alla sua realizzazione.

Nel 2022 l'Agenzia avrà l'inizio della grande crescita.

Quando avremo i regolamenti pubblicati in gazzetta ufficiale inizieremo una fase di reclutamento; ipoteticamente da febbraio (n.d.r. 2022) considerando che ci aspettiamo la loro pubblicazione per fine dicembre. Una fase importante nella quale, anche grazie all'equiparazione dei salari degli appartenenti all'Agenzia a quelli di Banca d'Italia, recluteremo i migliori talenti che vogliono dare una mano al nostro Paese. Riportando a casa alcuni di quei milioni di ragazzi e ragazze, tecnici e professionisti di ogni tipo, che, negli ultimi venti anni, hanno lasciato l'Italia senza che nessuno muovesse un dito.

Il più grande regalo che abbiamo fatto ai Paesi a noi limitrofi sia agli Stati Uniti depauperando forse in modo irreversibile la classe dirigente nazionale di oggi e del prossimo futuro.

Sappiamo che i nostri ragazzi sono bravi. Abbiamo un sistema universitario che è in grado di creare ottime professionalità, ma è chiaro che, in un mondo così complesso, queste professionalità vanno mantenute all'interno del nostro Paese. Non possiamo parlare di sovranità digitale senza una workforce adeguata.

E questo è un problema che dobbiamo affrontare in modo chiaro e deciso.

Lo dobbiamo affrontare dal punto di vista motivazionale, dal punto di vista salariale e dal punto di vista valoriale. È ineludibile avere un grande piano, perché servono professionalità in questo settore e non solo in ambito tecnico.

Servono professionalità all'interno della parte giuridica, della parte di relazioni internazionali, in quella della psicologia e delle scienze sociali. Tutto dovrebbe essere rimodellato perché la trasformazione digitale porterà via dei lavori, questo lo sappiamo tutti, ma ne creerà anche di altri. Per cui, per evitare che il Paese si trovi in grande difficoltà, dobbiamo avere una forza lavoro in grado di intercettare e di andare su quei lavori. Allo stesso momento serve che anche chi non è coinvolto direttamente nella parte tecnologica abbia quelle basi "digitali" per afferrare al volo quelle opportunità create dal digitale nella società, nelle arti, nella cultura e nella vita di tutti i giorni.

Questo è uno sforzo importante che dovremmo fare tutti insieme.

Prima rendercene conto e poi agire perché non è scolpito nella pietra il fatto che rimarremo all'interno dei Paesi più industrializzati. Stiamo sicuramente subendo una trasformazione. Ci basti paragonare quello che abbiamo oggi rispetto a come eravamo e agli strumenti che usavamo vent'anni fa, ma per rimanere agganciati al treno che ci porterà a quella futura prosperità che ci aspettiamo per i nostri figli, è necessario eseguire una trasformazione digitale in sicurezza. Una trasformazione digitale che abbia alla base criteri che possano minimizzare il rischio di attacchi. Fermo restando che purtroppo il rischio non può essere zero.

Parliamo di grande attività di prevenzione ma anche attività di mitigazione, perché prima o poi un attacco arriva. Basti pensare che nel 2021 abbiamo dovuto gestire, all'interno dei nostri sistemi, oltre 30.000 vulnerabilità censite dal database delle Common Vulnerabilities and Exposures. È chiaro che all'interno di questo mare magnum, gli attacchi, anche ad asset strategici, possono avvenire. Abbiamo dunque bisogno di un sistema nazionale che funzioni per mitigare gli attacchi che andranno a buon fine. Tutto deve essere calibrato in funzione del rischio di quell'asset. Ad esempio, se l'impatto dell'incidente dovesse compromettere la sicurezza nazionale allora dovremmo imporre sull'asset digitale strategico delle misure di sicurezza preventive che siano molto forti.

Man mano che si scende sulla sensibilità dell'asset si può anche rendere le misure di sicurezza meno stringenti. Se ci venissero rubate, ad esempio, le foto del Colosseo, o di altre nostre meraviglie nazionali, potremmo rischiare che la loro diffusione invogli altre persone a visitare il nostro Paese, ma, ovviamente, ciò non vale se parliamo della manomissione di una infrastruttura o di una dorsale di energia elettrica o di una pipeline, per quanto riguarda il gas. Non vale per quanto riguarda l'infrastruttura che gestisce il mercato dei titoli di Stato o tutta la parte spaziale.

Tutto questo deve tener conto della funzione essenziale che ha quello specifico asset per lo Stato. Questo è il razionale che è dietro alla Legge del "Perimetro di sicurezza nazionale cibernetica".

Bisogna far sì che questa mentalità di prevenzione e mitigazione sia fatta propria da tutti, inclusi i cittadini, perché anche quando si agisce su uno smartphone è necessario avere buone pratiche di prevenzione. Nello stesso tempo è importante mitigare se, per un'operazione avventata, abbiamo preso qualche virus o malware.

Lo dobbiamo fare come cittadini nelle nostre famiglie.

Lo dobbiamo fare all'interno delle nostre aziende o nelle organizzazioni nelle quali lavoriamo.

Lo dobbiamo fare, infine, attraverso una modalità collettiva affinché, come abbiamo sempre evidenziato, la cybersicurezza non sia legata solo ai dipartimenti di Information Technologies, i cosiddetti CED (Centro Elaborazione Dati), ma penetri all'interno di tutta l'organizzazione fino agli amministratori delegati, ai consigli di amministrazione, i quali devono apportare opportuni piani per la resilienza delle loro infrastrutture.

D'altronde la trasformazione digitale è il cuore di ogni organizzazione. Lo abbiamo visto con gli ospedali e lo vediamo con le aziende che vengono attaccate, non solo in Italia, ma in tutto il mondo. Stento a pensare ad organizzazioni che non abbiano il loro funzionamento scandito e gestito da una infrastruttura digitale.

Dunque, se è questo il cuore di un'organizzazione allora bisogna adottare le cure necessarie e disporre un appropriato budget per mettere in funzionamento un sistema e farlo operare correttamente. Le persone che lavorano perché questo cuore resti funzionante devono essere retribuite adeguatamente. Altrimenti iniziano a saltare da un posto di lavoro all'altro e può accadere che, in uno di questi salti, lascino l'Italia. Riportarli indietro sarebbe poi estremamente difficile come sperimentano giornalmente i professionisti delle risorse umane.

Per questo non dobbiamo permettere questa depauperazione di competenze matematiche, informatiche e ingegneristiche. Nel momento stesso in cui mancano queste competenze, aumentano gli attacchi e i sistemi non funzionano più bene rallentando di fatto lo sviluppo e il benessere della società.

Un Paese non potrà essere competitivo se non ha eseguito un processo di trasformazione digitale resiliente rispetto al rischio di attacchi cibernetici.

È importante capire che non si tratta soltanto di un problema di sicurezza informatica, si tratta di un problema di mancanza di competenze legate alla governance dell'IT di una organizzazione.

La consapevolezza di questi problemi sta diventando sempre più importante anche rispetto a dieci anni fa, quando circa mille persone si materializzarono – in modo anche inaspettato – in Sapienza alla presentazione del framework nazionale per la cyber security. Quelle persone erano già consapevoli del cambiamento culturale che avevamo di fronte. Dobbiamo evangelizzare il Paese e far sì che quei mille diventino cinquanta milioni. Forse utopico, ma dobbiamo spingere in modo convinto in quella direzione e i conti li faremo tra quattro anni alla fine del mio mandato.

Trascrizione sintetica della Tavola Rotonda 1

modera *Michele Colajanni*[1]

Michele Colajanni. Quando, dodici anni fa, all'inizio di questa conferenza parlavamo di protezione delle infrastrutture critiche da attacchi cyber e di sensibilizzazione sui temi della *Cyber Warfare* ci guardavano con sospetto. Purtroppo, avevamo ragione. Non perché eravamo in possesso di magiche sfere di cristallo, ma perché, studiando, facendo ricerca e assistendo a una imponente quanto fragile digitalizzazione, riuscivamo a scorgere trend evidenti. Anche oggi, siamo in grado di prevedere che il prossimo decennio non ci porterà verso una maggiore sicurezza delle infrastrutture e della società dal punto di vista cyber. Almeno fino al 2030 ci aspettiamo il continuo avvento di nuove tecnologie e la loro integrazione con dispositivi definibili "smart" solo dal punto di vista del marketing. E se è vero che un mondo "smart" è accettabile quando si parla di vendere un televisore o un frigorifero, nel momento in cui si comincia a parlare di reti elettriche smart, di autostrade smart, di infrastrutture smart è bene cominciare a porre maggiore attenzione. La verità è che non abbiamo ancora consolidato il presente, ma ci troviamo ad affrontare le vulnerabilità del prossimo futuro. Gli adulti, e voi presenti lo siete, hanno anche delle responsabilità nella costruzione di una società digitale che sia sicura e resiliente per i nostri figli. Va benissimo la realizzazione dell'Agenzia della Cybersecurity Nazionale, vanno benissimo le ricerche dei professori universitari così come le soluzioni tecnologiche dei principali fornitori, ma siete tutti voi a portare a terra i nostri servizi, le procedure e le tecnologie di sicurezza. Tutti hanno il dovere di fare qualcosa in più per consentire che nel 2030 il nostro Paese sia più sicuro per i cittadini di quanto lo sia attualmente. La vostra guida e le vostre decisioni saranno fondamentali per tutte le filiere produttive, sociali ed economiche. Lo stesso termine *supply chain* è antiquato nel senso che restituisce un'idea monodimensionale dei fornitori. Preferisco parlare di *supply network* perché dietro ciascun fornitore c'è un mondo complesso, una costellazione di PMI che le grandi aziende dovrebbero aiutare a portare a un livello di sicurezza

[1] Prof. Ordinario di Ingegneria Informatica, Dip. di Informatica – Università degli Studi di Bologna.

adeguato. Un livello tale da creare e garantire un mondo più sicuro per noi e per i nostri figli. Cari panelist, come vedete il presente e cosa pensate rispetto al futuro della nostra società proiettato in questo decennio? Partiamo da Antonio Ceccarelli di Telespazio al quale chiedo cosa si intende per *space economy* e come questa, che non riguarda più una nicchia, ci aiuterà a costruire una società più sicura.

Antonio Ceccarelli[2]: come esponente dell'ingegneria di Telespazio, una delle società della filiera nazionale della space economy, inizierei con lo spiegare cosa significa space economy e in che modo sta abilitando tutta una serie di servizi utili alla nostra società per il presente e il futuro. In questi anni, l'evoluzione della space economy si è basata sul fatto che quella nicchia è stata notevolmente abbattuta grazie alla possibilità di avere oggetti in orbita. Dunque, oggetti nello spazio che possono ospitare funzionalità diverse. Semplificando, l'architettura di un sistema spaziale ha oggetti in orbita e oggetti a terra che dialogano con loro. Grazie alle evoluzioni, gli oggetti possono essere messi in orbita con costi bassi e sfruttando orbite diverse; a varie distanze dalla terra e non più, come invece si usava tanti anni fa, soltanto nelle orbite geostazionarie. Queste erano, sostanzialmente, orbite in cui lavoravano piattaforme che ospitano delle funzionalità. Queste piattaforme, questa sorta di hosting infrastrutturale che abbiamo nello spazio, ci permettono di inserire al loro interno funzionalità di ricetrasmissione, di processamento e di sensoristica. Quindi abilitano tre domini importanti. Per esempio, abbiamo sensori ottici e radar per l'osservazione della Terra. Abbiamo ricetrasmettitori in particolari frequenze, la possibilità di avere posizioni e tempi standard da usare in una serie di applicazioni di navigazione. E, non ultimo, abbiamo quello che è stato storicamente il primo impiego dei satelliti, la capacità ICT di comunicazione, memorizzazione e processamento a bordo di queste piattaforme che abilitano le nuove funzionalità. La vision dei prossimi anni sta proprio nello sfruttare tutti i trend tecnologici che abbiamo a terra, mutuandoli e configurandoli su queste piattaforme in orbita in modo da abilitare funzionalità complementari a quelle terrestri. Si parla, ad esempio, di space cloud che seppure sembrino cose visionarie, stanno già partendo come dimostratori in cui una capacità di processamento in orbita, opportunamente ricollegata con canali di comunicazione a terra, va a integrare, backuppare e rendere più resiliente un edge processing che è in orbita avvicinando certi utilizzatori. Vale in contesti particolari, scenari emergenziali o di guerra, ma hanno anche un contatto con applicazioni civili rendendo possibili funzionalità molto importanti. Nel caso del dominio delle comunicazioni, ad esempio, queste capacità di processamento rendono il satellite qualcosa in più rispetto a quello che era in passato. Non più un mero ritrascrittore di frequenze, ma

[2] Responsabile ingegneria della Linea di Business Satellite Communications (Telespazio).

qualcosa con una capacità di processamento in grado di abilitare una delle infrastrutture terrestri in orbita. Una base station 5G, se si mutua il concetto e la si integra in un contesto spaziale, rende possibile un'interazione diretta col satellite di una interfaccia 5G. Cito 5G perché è un paradigma di armonizzazione delle reti che si sta affermando a livello di standardizzazione. In questo paradigma esiste già il satellite come connettività, cosa che nel passato non era possibile. Dunque, restringendo il campo alle comunicazioni, quello su cui si sta lavorando in Italia e in Europa ha a che fare con queste nuove possibilità infrastrutturali che usano nuove bande e che usano una protezione di questi canali a livello di sicurezza, già valutata e implementata nella fase di design. Alcune di queste tecnologie permettono anche di sviluppare particolari funzionalità. L'uso delle comunicazioni quantistiche abilita un corollario importante: la possibilità, ad esempio, di gestire le chiavi crittografiche quantistiche è una frontiera che si sta studiando. Si tratta di tool che possono essere sfruttati anche nelle comunicazioni a terra per aumentare la nostra capacità di difesa anche nella crittografia delle comunicazioni. È chiaro che in questo serbatoio di idee, di attività e di progettazione, la Telespazio, come altre componenti della filiera nazionale, sta lavorando a studi europei che mettono a fuoco queste nuove costellazioni narrow e broadband. In questo**,** la Telespazio si muove con la sua governance per la security che è consolidata nel tempo e le ingegnerie, che io qui rappresento, lavorano insieme alla security industriale e ai referenti verso l'Agenzia per il Perimetro Cibernetico Nazionale. Tutto questo sfruttando l'esperienza che abbiamo consolidato nel tempo con un accreditamento di infrastrutture come COSMO-SkyMed o Galileo che gestiamo dal Fucino, il centro di controllo. E l'accreditamento di un'infrastruttura è stato fatto con una forte cooperazione con le autorità nazionali di sicurezza, ma anche con un coordinamento delle autorità nazionali di sicurezza europee.

Michele Colajanni: dallo spazio passiamo alla terra con un'altra realtà come Terna. Parliamo con Francesco Morelli, grande esperto di sicurezza. Anche in Terna siete in transizione verso le smart grid che immagino diventeranno sempre più autonome, veloci, sempre con più capacità elaborative. Una transizione anche rispetto al Green, al mondo dell'energia e ai suoi prosumer.

Francesco Morelli[3]: sicuramente la transizione energetica è in corso. Siamo in roadmap, per cui la spinta è forte. Terna, per il ruolo che ha in Italia ossia quello di trasmettere energia ad alta tensione, si trova proprio nel mezzo di questa situazione. Da poche decine di produttori, che avevamo qualche anno fa, siamo passati a decine di migliaia. Per noi che siamo nel campo della cybersicurezza, la zona di confine dove ci si interfaccia con altre realtà, che

[3] CISO (Terna).

chiamiamo terze parti, è sempre quella più delicata. Per questo, sentendo anche le parole di oggi del direttore dell'Agenzia per la Cybersicurezza Nazionale, sarebbe importante avere un capo maglia che definisca appunto le maglie di comunicazione, per rimanere in un gergo militare. E su questo andare poi a formare dei veri e propri centri di competenza secondo il modello ENISA (Agenzia dell'Unione europea per la cybersicurezza). Quindi dei centri di information sharing e analysis center settoriali che confluiscono ad un capo maglia che, proprio come ha detto il professor Baldoni, guidi e governi questo scambio informativo. Un altro aspetto importante appena toccato è stato quello di andare a investire nello sviluppo tecnologico. Sicuramente nel campo della cybersecurity il mercato è esuberante. Vi sono tecnologie per ogni esigenza, eppure in settori come il nostro, dove ci sono esigenze peculiari, c'è ancora qualcosa da fare. Ricordo che Terna è un Transmission System Operator (TSO). In Italia ce n'è uno, uno anche in Francia, quattro in Germania per cui si parla di realtà settoriali e peculiari. E noi abbiamo intenzione di investire e creare dei centri di competenza che possano andare a sviluppare qualcosa che, oltre che testare a livello certificativo, testi anche a livello interno. È importante andare a creare queste competenze. Il mercato è esuberante, ma le grandi aziende devono avere la forza di investire e di fare qualcosa in più sul piano settoriale-specialistico, in modo da dare il vantaggio competitivo. I satelliti sono una realtà. Noi li guardiamo sia sotto l'aspetto della comunicazione sia sotto l'aspetto della sicurezza cyber. Pensare a un satellite che elabora diventa ancora più spaventoso in termini di cyber security. La cyber security satellitare è uno di quei settori in cui ci sono poche realtà e pochi esperti che vi operano. Ricordo un film con Will Smith, in cui il protagonista intercettava qualsiasi satellite con un portatile da casa. Dunque, l'attenzione su questo tema sta crescendo. Anche riguardo alla sensoristica, quello che percepiamo a livello di rete di trasmissione nazionale, è il fatto che possa dare grandi vantaggi a livello di gestione smart, di visibilità immediata. Tuttavia, come è riportato in diverse relazioni, il rischio degli effetti collaterali delle innovazioni tecnologiche è altissimo. Un rischio che il World Economic Forum, che fino a due anni fa lo poneva in alto a destra, lo scorso anno lo ha sostituito con le pandemie. Al momento, il rischio degli effetti collaterali delle nuove tecnologie è, a mio giudizio, quello che più ci può cogliere alla sprovvista. Perché basta veramente poco per andare a toccare l'equilibrio di una rete che comunque è delicata e sensibile. Pensiamo a un banale sensore di temperatura che indica l'operatore di centro di controllo che può far passare più corrente su una linea. Se qualcosa si mette in mezzo tra il centro di controllo e questo sensore mandando una temperatura più bassa in sala, il rischio è che si vada a sciogliere una linea.

Michele Colajanni: recepiamo due messaggi importanti per chi ci ascolta, soprattutto per i giovani. Due tematiche tecnologiche: una sullo

spazio dove non siamo secondi a nessuno; l'altra ha che fare con gli investimenti che andranno effettuati non solo sui servizi tradizionali, ma anche su tematiche cyber physical, creando così opportunità. La parola passa a Giovanni Ciminari di SOGEI. Parliamo di una realtà che, forse non tutti sanno, ha una capacità di dati ed elaborazione tra le più potenti in Italia. Una realtà che, in passato, ha sempre garantito continuità di servizi svolti in maniera robusta, seria ed efficace. Ma che cosa ci riserva il futuro?

Giovanni Ciminari[4]: siamo una società in-house del Ministero dell'Economia e delle Finanze. Il nostro business più importante è quello di gestire i dati fiscali di tutti i cittadini italiani, dati molto critici e sensibili. Operiamo, inoltre, sul bilancio dello Stato, su tutti gli strumenti per gestire la finanza pubblica. Sul tema del PNRR realizziamo i sistemi con cui dovrà essere monitorata la spesa del Piano Nazionale di Ripresa e Resilienza. Questo rientra nella nostra mission principale. Questa mission negli anni è cambiata parecchio. Si pensi ad Immuni, la famosa app, che è stata realizzata da SOGEI su richiesta del Ministero della Sanità. Inoltre, in questo periodo di pandemia, i sistemi realizzati e gestiti da SOGEI sono di supporto al Generale Figliuolo. Possiamo dire di avere una delle infrastrutture di una certa rilevanza e, secondo la caratterizzazione che è stata fatta qualche tempo fa dall'Agenzia per l'Italia Digitale (AGID), rispondiamo alle migliori pratiche. Questo è il motivo per cui molte Pubbliche Amministrazioni ci stanno riconoscendo. Siamo in un momento veramente effervescente dal punto di vista dell'acquisizione dei clienti, seppure per noi non siano semplici clienti; considerando che abbiamo un mandato che ci viene riconosciuto anche per legge. Abbiamo un obbligo verso questi Enti e, di conseguenza, verso i cittadini. Un ruolo estremamente delicato che sentiamo molto come missione verso il Paese. In questo senso, il tema della cyber security è estremamente delicato e intendiamo gestirlo in maniera sempre più efficace e su questo abbiamo anche una partnership particolarmente intensa con l'Agenzia per la Cybersicurezza Nazionale. Un ruolo di collaborazione bidirezionale in quanto noi cerchiamo di aiutarli per quelle che sono le nostre capacità e, viceversa, loro collaborano fortemente aiutandoci a gestire l'enorme patrimonio informativo che SOGEI deve utilizzare. Quindi per noi la sfida è avere un perimetro che si sta allargando in maniera molto significativa e che può attirare attenzioni da parte di malintenzionati. Quindi che cosa vogliamo fare? Abbiamo un piano di evoluzione della nostra postura di sicurezza su cui stiamo lavorando da alcuni mesi. Questo ci ha permesso di determinare quelli che sono i punti di forza e i punti di debolezza, ma vogliamo implementare questo piano utilizzando anche nuove risorse umane a supporto. Essendo noi una parte della Pubblica Amministrazione, abbiamo delle caratteristiche peculiari della Pubblica

[4] Responsabile Funzione Cyber & Defense (SOGEI).