Commissione Trasporti, Poste e telecomunicazioni della Camera dei deputati

Nicola Grandis

Memoria in relazione all'esame del disegno di legge C. 3161, di conversione del decreto-legge 14 giugno 2021 n. 82 recante "Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale.

Desidero ringraziare le Commissioni Trasporti, Poste e telecomunicazioni della Camera dei Deputati per l'opportunità di presentare un contributo nell'ambito dell'esame parlamentare del disegno di legge di conversione del decreto legge sulla costituenda Agenzia per la Cybersicurezza Nazionale. Metto a disposizione della Commissione, in questa memoria, la mia conoscenza di esperto del settore frutto di un'esperienza internazionale ventennale sul tema della CyberSecurity e la mia esperienza nel settore dell'Intelligenza Artificiale, applicata anche alla CyberSecurity.

L'occasione mi è opportuna per produrre una memoria articolata in due sezioni principali. La prima sezione contiene delle mie considerazioni di carattere generale/funzionale sui temi che saranno poi propri della Costituenda Agenzia, mentre la seconda riporterà alcune considerazioni sui specifici articoli presenti nel Disegno di Legge in discussione.

Per motivazioni legate alle mie capacità professionali ed alla mia formazione specifica, la presente memoria sarà focalizzata maggiormente sui passaggi più pratico-esecutivi del DL in discussione, rispetto a quelli più Istituzionali ed organizzativi il cui commento lascio a persone maggiormente preparate del sottoscritto.

Considerazioni Generali di Contesto

Tessuto Digitale

Il tessuto digitale che sottende alle attività economiche, sociali e strategiche di un Paese è, per sua definizione, un oggetto disomogeneo, ramificato, malleabile ed in continua evoluzione. Questa caratteristica intrinseca e sistemica definisce sia il valore del tessuto digitale come strumento di crescita e leva di progresso per il Paese che se ne dota, sia il valore premiante del potenziale capitale conseguito da un attaccante che mirasse a danneggiare il Paese stesso.

La struttura del tessuto digitale che connette le attività produttive della Nazione necessita di meccanismi di protezione che condividano con lo stesso le medesime caratteristiche costitutive e, che quindi siano efficaci nel proteggerlo verso criticità presenti e future.

Da un punto di vista logico, il tessuto connettivo che la costituenda Agenzia dovrà custodire e preservare si manifesta su livelli tecnologici e procedurali diversi. Oltre alla rappresentazione comune dello stack ISO/OSI che presenta il trasporto delle informazioni tra i livelli fisici e logici, dal più basso al più elevato, nel panorama della CyberSecurity bisogna considerare ulteriori livelli intermedi e laterali che sono paralleli ed adiacenti a quelli convenzionali. La superfice di attacco di un attore ostile si espande o si contrae rispetto alla struttura digitale target, in funzione del punto di vista che viene fornito per tentare la sortita; dunque non è infrequente che gli attacchi più catastrofici vengano condotti tramite canali e modalità che sfruttino tecniche e posture non convenzionali (supply chain attacks, side channel attacks, social engineered attacks, etc). L'Agenzia dovrà confrontarsi con questo spettro mutevole di tecnologie e possibilità, il compito istituzionale che gli viene affidato ne metterà duramente alla prova capacità e competenze per un periodo di tempo lungo nel quale fenomeni transienti ne caratterizzeranno le sfide, fino a disegnarne la portata del successo.

Tra questi fenomeni emergenti, va certamente annoverata l'Intelligenza Artificiale. Da Scienza nata negli anni '50 del secolo scorso, essa si configura come una tecnologia permeante nell'elaborazione delle informazioni nel periodo corrente. La nascente Agenzia dovrò confrontarsi con una classe di attacchi e di rischi che utilizzeranno l'Intelligenza Artificiale sia come leva di attacco che come obiettivo della fase predatoria.

Assenza di perimetro

In questo panorama in continua modifica, la duttilità dei rischi renderà meno efficiente la classificazione delle minacce. Alcuni degli eventi con maggiore impatto sulla resilienza delle infrastrutture strategiche che abbiamo visto negli ultimi mesi sono stati originati da nuove e poco presidiate aree di ingresso. L'osservatore poco attento potrebbe appiattire questi eventi sulla responsabilità dello Human-Factor, ma nella loro essenza si è tuttavia trattato di azioni che hanno tratto capacità dall'analisi tecnica di punti di ingresso molti specifici.

Da queste considerazioni si evince l'importanza dell'attività formativa che verrà affidata all'Agenzia, essa sarà determinante nel mitigare, contenere e possibilmente arginare tutta una classe di attacchi che mirerà a corrompere le nostre capacità prendendo slancio proprio da aree ed attori che noi avremo qualificato come meno sensibili e rilevanti nella catena della Sicurezza.

Dalla medesima analisi discende anche l'assenza di un "perimetro Cyber" da difendere. In troppi contesti, l'attività Cyber di protezione di un Paese viene assimilata a concetti propri della Teoria del combattimento militare quali quelli di Infrastruttura-Critica, Perimetro da difendere, Osservazione e simili. Uno Stato potrebbe lanciare un Cyber-attacco verso un'altra Nazione semplicemente sbilanciando o alterando artificiosamente i valori di specifiche criptovalute, allo stesso modo potrebbe portare un attacco fisico avvicinandosi ad un diplomatico in territorio terzo, oppure lo potrebbe fare generando false informazioni (fake news) su canali Social o Siti Web fisicamente residenti fuori dal territorio della Nazione Target. La casistica è ampia, oltre che in continua evoluzione; in questi ed in molti altri casi si noti come il concetto di perimetro o posizionamento geografico tende a sfumare rispetto al contesto dell'attacco. L'assetto della costituenda Agenzia dovrebbe tenere conto di questi fattori e della funzione di trasferimento prospettico che un Cyber-Attaccante può decidere di applicare nella scelta della strategia che lo condurrà a danneggiare il proprio Target.

Tecnologie emergenti ad alto impatto

La prossima imminente diffusione della rete 5G, la varietà di strumenti IoT che si aggiungeranno al tessuto digitale del sistema Paese, l'avvento dell'Intelligenza Artificiale che renderà questi oggetti capaci di assumere comportamenti differenti in funzione del loro contesto operativo ed altre innovazioni all'orizzonte, richiedono che la costituenda Agenzia venga messa in condizione di seguire sia i Trend tecnologici attuali, ma anche quelli che sono ancora da venire. Si pensi alle tecnologie quantistiche che porteranno con loro una serie di problemi in ambito crittografico ed una ridotta capacità di captazione delle informazioni, piuttosto che agli sviluppi nel settore spaziale che modificheranno il modo in cui i soggetti a terra accederanno alla rete ed altre innovazioni che già sono in fase di studio, per cui attendiamo solo una disponibilità su scala. Le tecnologie emergenti non solo potranno modificare l'attuale struttura del tessuto digitale del nostro Paese, influendo quindi anche sulle strategie difensive che ne preserveranno le capacità di resilienza, ma altresì potrebbero divenire disponibili per un attaccante prima che le stesse raggiungano una diffusione capillare. Nelle attività da delegare all'Agenzia è auspicabile che venga inclusa anche la ricerca e l'osservazione dei Trend emergenti.

Conclusioni generali di contesto

L'Agenzia sarà chiamata a compiti complessi e di importanza strategica per il nostro Paese. Essa sarà impegnata su molteplici fronti e dovrà necessariamente interagire con le Istituzioni e con le strutture dello Stato per proteggere gli interessi nazionali. Personalmente ritengo necessario che le sfide a cui sarà chiamata, siano coadiuvate dalla necessaria dotazione di strumenti, uomini e mezzi al fine di poter affrontare il tema della CyberSecurity Nazionale nel suo insieme, per il presente e per gli anni a venire. Sarà fondamentale il coordinamento a livello Europeo ed Inter-ministeriale per raggiungere l'obiettivo prefissato, ma sarà altresì importante che l'Agenzia stessa sia dotata di capacità e competenze di alto profilo e tasso tecnico elevato.

L'attuale problema delle strutture omologhe della nascitura Agenzia non risiede nel reperimento delle informazioni, quanto nella loro classificazione rispetto ai potenziali rischi a cui questi segnali espongono le infrastrutture che esse stesse sono deputate a proteggere.

Vorrei esortare la Commissione a tenere conto dei fattori esposti in queste considerazioni generali esposte. La sicurezza cibernetica di un Paese passa da molti fattori ed ha molte sfaccettature, l'architettura generale dell'Agenzia nascente è molto importante, ma va progettata tenendo conto della complessità dello scenario tecnico-sociale che dovrà affrontare. Di seguito le mie osservazioni che, alla luce delle considerazioni in premessa, vogliono portare all'attenzione della Commissione alcuni passaggi sugli articoli in valutazione.

Analisi dei singoli articoli

Art.1 Let. A

Cybersicurezza, l'insieme delle attività necessarie per proteggere

dalle minacce informatiche reti, sistemi informativi, servizi informatici

e comunicazioni elettroniche, assicurandone la disponibilità, la confidenzialità e l'integrità, e garantendone altresì la resilienza;

Si osserva che sarebbe opportuno indicare nella definizione di CyberSicurezza anche la disponibilità "nel futuro" delle caratteristiche di disponibilità, confidenzialità, integrità e resilienza; ovvero andrebbe indicato che la CyberSicurezza non ha solo un carattere "reattivo", ma anche "preventivo" rispetto a tecnologie e trend emergenti, anche quando questi possano essere assunti come lontani da venire.

Art.5 c.1

È istituita, a tutela degli interessi nazionali nel campo della

cybersicurezza, anche ai fini della tutela della sicurezza nazionale nello

spazio cibernetico, l'Agenzia per la cybersicurezza nazionale, denominata ai fini del presente decreto « Agenzia », con sede in Roma.

Si osserva che non è presente un riferimento alla protezione degli interessi nazionali anche rispetto ad azioni condotte nello spazio cibernetico da attori ostili che agiscano al di fuori del nostro Territorio o che utilizzino strumenti di

attacco del tutto immateriali e non geograficamente localizzati. Anche in questo articolo non è inoltre presente un riferimento alla protezione con azioni preventive condotte dalla nascente Agenzia.

Art.7 c.3 Lett. n

Sviluppa capacità nazionali di prevenzione, monitoraggio, rilevamento, analisi e risposta, per prevenire e gestire gli incidenti di

sicurezza informatica e gli attacchi informatici, anche attraverso il

CSIRT Italia di cui all'articolo 8 del decreto legislativo NIS;

Si osserva che non è presente un riferimento alla costruzione di scenari previsionali artificiali, costruzione di simulazioni ed analisi strategiche di possibili impatti nel futuro per le tecnologie emergenti. Si osserva inoltre che si potrebbe inserire anche in questo articolo un riferimento alla cooperazione con gli omologhi europei ed internazionali sui temi oggetto dell'articolo.

Conclusioni

L'importanza strategica per il nostro Paese della costituenda Agenzia è evidente e richiede il massimo sforzo per la definizione di un'Architettura che ne garantisca l'aderenza agli intenti dell'Esecutivo, ma che allo stesso tempo tenga conto della rapidità e della molteplicità delle azioni che essa dovrà affrontare e gestire nel corso dell'esercizio delle sue funzioni. Nel prossimo futuro, la costituenda Agenzia dovrà fronteggiare scenari e minacce che attualmente non possiamo prevedere, dovrà utilizzare strumenti e tecniche di valutazione del rischio che ad oggi non possiamo individuare né per Area di riferimento, né per tecnica di valutazione. E' dunque necessario che l'architettura illustrata nel Disegno di Legge in discussione sia sufficientemente tollerante ed adattabile agli scenari che possono attendere la costituenda Agenzia. Auspicando che l'Agenzia riuscirà a realizzare gli obiettivi di integrazione ed ottimizzazione che il legislatore intende trasferirle, ringrazio nuovamente la Commissione per aver voluto richiedere un mio contributo alla discussione in corso.

Roma, 01/07/2021