SOCINT - *Società Italiana di Intelligence*

AGENZIA NAZIONALE CYBERSICUREZZA

"nuove sfide per il futuro"

Le proposte della Commissione di Studi Cyber Threat Intelligence e Cyber Warfare

Premessa di Mario Caligiuri

Contributi di:

Mattia Siciliano (Presidente commissione CTI & CW)
Massimiliano Alzetta
Francesco Arruzzoli
Fabrizio d'Amore
Andrea Giordani
Andrea Leoni
Annita L. Sciacovelli
Glicerio Taurisano

2021

SOCINT

La Società Italiana di Intelligence è un'associazione scientifica senza fini di lucro il cui obiettivo è promuovere lo studio e la cultura di Intelligence in Italia. Costituita nel 2019, la sede generale, è ubicata presso l'Università della Calabria, ed è presieduta dal prof. Mario Caligiuri, professore ordinario di Pedagogia della Comunicazione. Avendo come scopo la promozione dello studio dell'Intelligence nel nostro paese, nonché sostenere l'insegnamento e la ricerca, ha da subito coinvolto docenti e ricercatori di tutta Italia, istituendo nel 2020 le Sezioni Regionali con sedi presso i vari Atenei nazionali, al fine di individuare e sviluppare il punto d'incontro dei saperi umanistici e scientifici. Ad oggi, oltre alle molte adesioni, conta su specifiche commissioni di studi le quali, al fine di approfondire temi di rilievo e attuali per gli studi di Intelligence, contribuiscono con i loro lavori alla mission della Socint.

Commissione di Studi
Cyber Threat Intelligence e Cyber Warfare

La Commissione di Studi CTI & CW nasce in seno alla SOCINT verso la fine del 2020 entrando da subito in piena attività ed è presieduta dal Prof. Ing. Mattia Siciliano. Al suo interno collaborano esperti professionisti e docenti sulla materia cyber, intelligence e sicurezza, provenienti da tutta Italia. Scopo della commissione è sensibilizzare sulle problematiche Cybersecurity, istituire ed erogare corsi di formazione, fare ricerca sulle minacce cibernetiche e proporre soluzioni di difesa, distribuire ai soci Socint newsletter ad interesse cyber, pubblicare papers e testi scientifici, organizzare webinar e convegni e proporsi alle istituzioni, alle aziende e ai privati con contributi tecnici e scientifici, al fine di contrastare le minacce informatiche sempre più aggressive e invalidanti per la sicurezza nazionale.

Contatti:

Socint – Società Italiana di Intelligence
c/o Università della Calabria
Cubo 18/B, 7° piano – 87036 – Arcavacada di Rende (CS)
info@socint.org
www.socint.org

Commissione di Studi CTI & CW
www.socint.org/commissioni-di-studio/
Mail: commissione.cyberwarfare@socint.org

Proposte da parte della

Commissione Cyber Threat Intelligence e Cyber Warfare

per la realizzazione della nuova

Agenzia per la Cybersicurezza Nazionale

Il presente documento rappresenta il punto di vista di esperti accademici e professionisti del settore cyber security e intelligence, ed è rivolto principalmente alle istituzioni del Parlamento Europeo, Governo Italiano, Agenzie d'intelligence e Organi di supporto alla presidenza del Consiglio dei Ministri.

2021

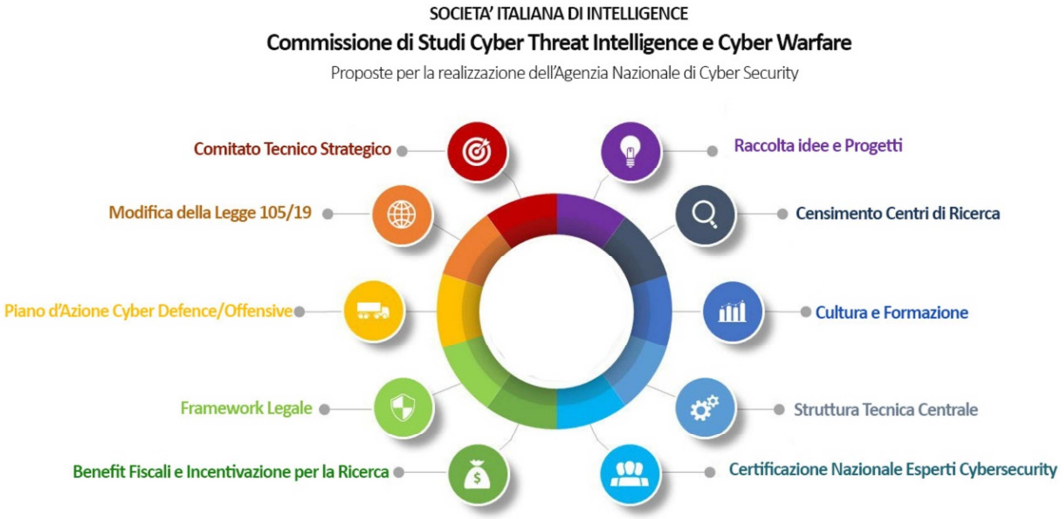
INDICE

PERCHE' QUESTO DOCUMENTO

La recentissima istituzione dell'Agenzia per la Cybersicurezza Nazionale pone nuove sfide, come la predisposizione di regole, strumenti e politiche che consentano di tutelare l'interesse nazionale nel cyberspazio, che ormai rappresenta l'ambiente economico, sociale, politico ed educativo prevalente, dove già oggi si misurano i rapporti di forza tra gli stati.

La sicurezza del cyberspazio diventa quindi obiettivo irrinunciabile se combinato alla sicurezza del territorio fisico; da ciò deriva l'esigenza per gli Stati di creare entità deputate alla gestione delle minacce cyber. La creazione dell'Agenzia risulta un passo di fondamentale importanza per il nostro Paese. L'attività dell'Agenzia dovrà muoversi secondo tre direttrici principali che possono essere esplicitate nell'adozione di nuovi modelli di gestione strategica del cyberspazio, sia dal punto di vista della cornice legale che delle azioni concrete da attuare, nella redazione di una mappatura delle conoscenze attuali e desiderate in futuro con l'individuazione delle esigenze dei soggetti pubblici e privati coinvolti nel cyberspazio, nella definizione di efficaci modalità di azione per lo sviluppo di strumenti tecnologici, in ottica di una postura sia passiva, di difesa degli asset del Paese nel cyberspazio, che attiva. Le conoscenze richieste non possono limitarsi al puro settore della Cybersicurezza bensì devono essere integrate con elementi di geopolitica, diritto internazionale e intelligence.

Appare opportuno quindi un approccio multidisciplinare nell'affrontare le sfide crescenti della sicurezza informatica con l'apporto imprescindibile del settore industriale pubblico e privato. Un attacco informatico in grande stile agli asset nazionali non è una mera ipotesi di studio ma una concreta possibilità, la cui incertezza riguarda solo il "quando" avverrà. L'Agenzia dovrà quindi dotarsi di adeguati strumenti d'intelligence capaci di gestire gli attacchi cyber, i quali possono provenire da possibili attori nel mondo del cyberspazio quali organizzazioni criminali e gruppi organici ad entità statuali avversarie. A tale riguardo la commissione Cyber Threat Intelligence e Cyber Warfare, della Società Italiana di Intelligence, ha il piacere di condividervi i 10 punti di azioni pensati per la nuova Agenzia di Cybersicurezza Nazionale.



PREMESSA

Il futuro non si aspetta: il futuro si prepara. Questa può essere la riflessione principale sulla recente istituzione dell'Agenzia Nazionale sulla Cybersecurity che emerge dal contributo predisposto dalla commissione Cyber Threat Intelligence e CyberWarfare della Società Italiana di Intelligence.

Con oltre metà della popolazione mondiale collegata in Rete, che diventerà la quasi totalità tra meno di dieci anni, il web rappresenta l'ambiente economico, sociale, politico ed educativo prevalente, dove si misurano già i rapporti di forza. Non a caso c'è chi sostiene che presto il *rating* di uno Stato dipenderà anche dal suo livello di sicurezza informatica[1].

E questo vale soprattutto per il nostro Paese che non moltissimi anni fa veniva definito "un paradiso per gli hacker", appunto per la disattenzione nella protezione del web[2]. In una società che si fonda sui dati, quindi sulla quantità, è facile prevedere una decadenza spirituale sempre più accentuata, nel solco di un processo che dura da diversi secoli[3]. Nel frattempo, però, dobbiamo occuparci dell'esistente e delle tendenze inarrestabili che lo caratterizzano, per cui occorre predisporre regole, strumenti e politiche che consentano di tutelare l'interesse nazionale in quest'ambito sociale sempre più decisivo. Le evoluzioni sono talmente veloci che anche le teorie geopolitiche tradizionali sono messe a dura prova. Oggi chi comanda il mondo potrebbe non essere chi controlla i mari, l'heartland, lo spazio aereo o quello stellare, ma chi riesce a dominare il *continente invisibile* del cyberspazio, che potrebbe comportare un declino della democrazia[4].

Da questa impostazione discendono altri due sviluppi collegati: chi controlla l'intelligenza artificiale domina il mondo e di conseguenza chi controlla le menti attraverso il web domina il mondo. Sembra quindi materializzarsi una "geopolitica delle emozioni"[5]all'interno di quelli che William Davies definisce "stati nervosi", dove le opinioni pubbliche sono in balia delle emozioni[6], e quindi della disinformazione[7].In un contesto di questa natura, difficilmente prevedibile quindi fuori controllo, come le vicende della pandemia, gli Stati devono riorganizzarsi profondamente. È bene quindi affrontare con decisione la dimensione del web, dove vivono e operano gran parte delle persone, inducendo presto gli stati a definire due distinte politiche: una per i cittadini fisici e un'altra, parallela, per quelli che

---

[1] *Dichiarazione di Giulio Terzi di Sant'Agata, Ministro degli Esteri del governo Monti, presidente Cybaze. Il rating di uno Stato dipenderà presto dal suo grado di cybersecurity?, 3.12.2018, https://www.agi.it/innovazione/rating_sicurezza_informatica_difesa-4694301/news/2018-12-03/.*

[2] *G. MICALESSIN, Hacker scatenati, Italia primo bersaglio, 3.2.2013. in www.ilgiornale.it.*

[3] *"La civiltà moderna appare nella storia come una vera e propria anomalia: fra tutte quelle che conosciamo essa è la sola che si sia sviluppata in senso puramente materiale, la sola altresì che non si fondi su un principio di ordine superiore. Tale sviluppo materiale, che prosegue ormai da parecchi secoli e va accelerandosi sempre di più, è stato accompagnato da un regresso intellettuale che esso è del tutto incapace di compensare". R. GUÉNON Simboli della scienza sacra, Adelphi, Milano 2008, p. 15.*

[4] *K. OHMAE, Il continente invisibile, Fazi, Roma 2001, p. 12.*

[5] *D. MOÏSI, Geopolitica delle emozioni. Le culture della paura, dell'umiliazione e della speranza stanno cambiando il mondo, Garzanti, Milano 2009.*

[6] *W. DAVIES, Stati nervosi. Come l'emotività ha conquistato il mondo, Einaudi, Torino 2019.*

[7] *M. CALIGIURI, Come i pesci nell'acqua. Immersi nella disinformazione, (prefazione di Luciano Floridi), Rubbettino, Soveria Mannelli 2019.*

operano sul web[8]. La simbiosi è evidente, come anche le esperienze del co-working e della didattica a distanza mettono davanti agli occhi di tutti. La sicurezza della Rete diventa quindi speculare alla sicurezza del territorio fisico, circostanza che giustifica il ruolo degli Stati, che nascono principalmente per difendere la vita dei cittadini ed è appunto in tale quadro che si legittima il ruolo fondamentale dell'intelligence[9].

Infatti la sicurezza è la premessa di tutti gli altri diritti, come precisa anche la sentenza della Corte Costituzionale n. 86 del 1977, che ha dato la spinta per definire al prima legge sui Servizi in Italia, approvata poco dopo[10]. Non per nulla, nel nostro ordinamento, all'intelligence è stato assegnato finora un compito prioritario nell'ambito della sicurezza informatica perché investe direttamente la sicurezza dello Stato[11]. Il tema è sempre più centrale anche a livello internazionale, in quanto l'ordine mondiale si sta ridefinendo anche attraverso le tecnologie della comunicazione. Lo scontro USA e Cina sul 5G va inquadrato in questo contesto.

L'Unione Europea solo nel 2012 ha cominciato ad aumentare le prime indicazioni in materia e a seguire anche il governo italiano[12]. Pertanto sono circa dieci anni che si sta affrontando una materia delicata e in espansione, anche sotto il profilo centrale dell'intelligence[13]. La recente proposta della costituzione di una Agenzia Nazionale sulla Cybersicurezza avanzata dal governo Draghi ha ricevuto sostanziali consensi. Pertanto, appunto in questa fase di avvio, potrebbero essere utili gli apporti che provengono dal mondo scientifico per contribuire fin dall'inizio all'impianto di fondo di questo organismo nel modo più efficace possibile.

A questa logica risponde il presente documento. E' stata infatti elaborata una proposta in 10 punti, suddivisa in tre ambiti: *adottare nuovi modelli di gestione strategica del fenomeno cyber, sia dal punto di vista della cornice legale che delle azioni concrete da attuare; redigere preventivamente una mappatura delle competenze esistenti e in formazione che i soggetti pubblici e privati dovrebbero possedere in ambito cyber; definire modalità di azione per un efficace sviluppo di strumenti tecnologici, in ottica Cyber Defence e Active Defence*. In tale quadro questo documento ha lo scopo di proporre un contributo di idee agli interlocutori istituzionali per meglio definire la strategia e l'operatività della Agenzia Nazionale sulla Cybersecurity.

Prof. Mario Caligiuri
Presidente della Società Italiana d'Intelligence - SOCINT

---

[8] *E. SCHMIDT, J. COHEN, La nuova era digitale. La sfida del futuro per cittadini, imprese e nazioni, Rizzoli Etas, Milano 2013, pp.25-93.*

[9] *F. SIDOTI, Morale e metodo nell'intelligence, Cacucci, Bari 1998.*

[10] *Legge n. 801 del 24.10.1977, Istituzione e ordinamento dei servizi per le informazioni e la sicurezza e disciplina del segreto di Stato.*

[11] *D.P.C.M. del 24.1.2013, Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale. Un ruolo centrale viene assegnato all'intelligence nelle politiche nazionali della sicurezza cibernetica e in particolare al Direttore del DIS.*

[12] *IBIDEM.*

[13] *M. CALIGIURI, Cyber Intelligence. Tra libertà e sicurezza, Donzelli, Roma 2016.*

1. COMITATO TECNICO SCIENTIFICO

"Prevedere un comitato tecnico strategico permanente in seno alla Presidenza del Consiglio dei Ministri che si occupi della definizione delle politiche di Cybersecurity/Cyberintelligence composto da componenti del CISR, mondo accademico, industriale e ordini professionali".

La nuova Agenzia per la sicurezza cibernetica, è chiamata a svolgere un ruolo impegnativo nella progettazione della sicurezza così come nelle attività di cyber intelligence, nonché delicato nella sua funzione di risposta immediata in caso di minacce.

Un comitato tecnico strategico di consulta, permanente e preparato in materie multidisciplinari, può costituire un primo fondamentale passo nello svolgere attività politico-strategiche in risposta immediata (ridurre i danni) e/o futura (prevenire le minacce e creare scudi difensivi). Il comitato tecnico strategico dovrebbe possedere conoscenze relative alla Cyber Security (difensiva e offensiva), geopolitica, diritto internazionale, intelligence sia sui temi IT che OT.

I membri dovrebbero far parte principalmente del mondo accademico, associativo, nonché industriale, sia con competenze di business sia con competenze "strutturate di settore". Inoltre, il comitato dovrebbe avere funzione di stabilire gli obiettivi a breve, medio e idealmente lungo termine riguardo la sicurezza cyber del Paese e definire inoltre la postura di fronte ad azioni cyber estere, indirizzo delle modalità di raccolta informativa, intelligence cyber ed aspetti di cyber operation, in particolare nei confronti soggetti istituzionali potenzialmente esposti.

In merito alla componente "industriale" del tavolo tecnico strategico, la stessa dovrebbe essere formata da rappresentanti di tutte le categorie industriali, in primis partendo dalle infrastrutture critiche del Paese.

Tali istanze dovrebbero pervenire non solo da aziende marcatamente strutturate sul lato cyber (Eni, Leonardo, Poste, Enel, etc.), bensì anche da piccole/medie aziende altamente specializzate, per meglio contribuire a definire le politiche di Cybersecurity/Cyberintelligence.

2. Modifica della Legge 105/19

"Modifica della legge 105/19 "Perimetro Cibernetico" in cui si preveda l'adozione da parte delle aziende, di un esperto cyber nel processo di procurement per la valutazione delle tecnologie da adottare, al fine di limitare i rischi di progettazione delle infrastrutture/servizi".

La continua evoluzione tecnologica, la globalizzazione e l'iperconnettività offre sul mercato tecnologie sempre più sofisticate e spesso economiche. Questo unito alla sempre più esasperata esigenza delle aziende di essere competitive sul mercato genera dei "vulnus" nella gestione della sicurezza delle informazioni delle organizzazioni, sempre maggiori.

La recente attuazione (8 maggio 2021 DPR.45) della prima parte della legge sul perimetro cibernetico, che prevede appunto l'istituzione di centri di valutazioni e certificazione nazionali (CVCN) e di centri di valutazione del Min. degli Interni (CV), va in questa direzione: valutare gli acquisti ICT di specifici asset ritenuti sensibili la cui lista è aggiornata periodicamente. Tuttavia focalizzare l'attenzione solo su determinati asset può rivelarsi non efficace in quanto non si tiene conto delle potenziali interazioni che hanno questi asset con altre organizzazioni (fornitori, utenti, etc..) ne d'altronde è ipotizzabile che i suddetti CVCN e CV possano effettuare controlli a tutte le forniture ICT grandi e piccole del paese.

Per questo sarebbe efficace regolamentare la figura di un esperto cyber qualificato e certificato in grado di assimilare le specifiche di volta in volta rilasciate dal CVCN e calarle nella propria realtà professionale, in modo da verificare la presenza di elementi potenzialmente pericolosi e segnalarli. In questo modo si potrebbe sviluppare in maniera granulare il monitoraggio dei sistemi ICT di tutte le organizzazioni. La figura dell'esperto cyber potrebbe inoltre ricoprire ulteriori ruoli, se fosse utilizzato anche come riferimento da un centro nazionale per la gestione di crisi cibernetiche rivelandosi un attore fondamentale, distribuito su tutto il territorio nazionale, nel contrasto e la mitigazione ai cyber attacchi. I vantaggi di una tale figura (professionista) sarebbero significativi, in termini di conoscenza e valutazione delle organizzazioni su cui si opera, di enforcement di audit di sicurezza, di rapidità di intervento sul territorio, nonché' come punto di riferimento nella programmazione e attuazione delle misure di sicurezza delle informazioni.

In ambito IT e OT , la possibilità della presenza di una figura di esperto nel mondo cyber, capace di cogliere all'istante le direttive nazionali in materia di cyber security, sapere creare e programmare processi di sicurezza informatica e conoscere le tecnologie più avanzate di cyber sicurezza, porterebbe al rafforzamento delle difese strutturali informatiche dell'azienda, far parte di una Rete Nazionale di Esperti della Cyber Security (che fa capo all'Agenzia Nazionale) e condividere con questa informazioni e dati utili alla difesa dei singoli asset. Tale esperto porrebbe essere assimilabile (come ruolo) al RSPP o simile, operando in questo modo su tutte le realtà imprenditoriali, piccole, medie e grandi con l'obiettivo di definire un piano di gestione degli incidenti, che goda delle caratteristiche di accounting, autenticità e non ripudio definito già in parte nel framework di cybersecurity nazionale.

3. Piano d'Azione Cyber Defence - Offensive

"Definire un piano di azione a livello Centrale in caso di crisi cibernetica che tenga conto degli aspetti di Cyber Defence e Cyber Offensive".

Al fine di contrastare un'eventuale crisi cibernetica sarebbe fondamentale poter sviluppare un'azione preventiva di difesa avanzata persistente, cioè evitare di limitarsi a rispondere agli attacchi, in quanto si cederebbe terreno agli avversari, ma effettuare nel cyber space un continuo "pressing" sui perimetri cibernetici dei paesi ostili, spingendo, in questo modo, gli avversarsi a concentrarsi sulle difese, scoraggiando campagne di attacco e rendendogli palese una credibile minaccia di rappresaglia. In questo scenario

in caso di cyber attacco il livello di scontro sarebbe innanzitutto più bilanciato e la capacità di reazione più immediata.

L'azione di difesa e contrasto dovrebbe prevedere un coinvolgimento ed un coordinamento centrale di tutti i vari attori interforze, in quanto un attacco cyber può compromettere strutture e servizi del "mondo reale" da qui la necessità di coordinare anche le forze di difesa convenzionali e di ordine pubblico. A tale riguardo dovrebbe essere redatto e testato un piano di azione in caso di crisi cibernetica (quindi di evento cyber che comprometta il funzionamento o la sicurezza di parti critiche dello Stato), che coinvolga Ministero della Difesa, Ministero degli Affari Esteri, agenzie di intelligence e che abbia come centro di contatto e coordinamento la Presidenza del Consiglio (magari nella figura della nuova agenzia cyber).

Il piano dovrebbe prevedere un sostegno difensivo alle infrastrutture colpite, aiutando in azioni di ripristino e difesa, e agevolando comunicazione tra il soggetto vittima e i referenti del piano. Dovrebbe prevedere inoltre un aspetto di "kickback attack", identificando tramite fonti diplomatiche e di intelligence (anche humint) le fonti dell'attacco e rispondere generando pressione e potenzialmente diminuendo quella subita dallo Stato Italiano, difatti una postura passiva solamente difensiva nell'ambito cyber pone intrinsecamente in svantaggio.

Detto piano di azione dovrà inoltre essere periodicamente sottoposto a revisione, riprogrammazione, rivisitazione a seconda o meno delle necessità che si presentano nel panorama difensivo o offensivo, e che tenga presente, continuamente, delle inferenze, degli indicatori e delle informazioni raccolte al fine di individuare o scorgere nuove minacce o attacchi.

L'obiettivo principale del piano di azione dovrà essere composto da una strategia sequenziale tipo: individuare e definire le attività da adottare, costruire modelli di difesa, suggerire metodi e azioni, analizzare dati di attacchi pregressi, attuali e probabili.

In pratica dovrà contenere anche e soprattutto valutazioni, osservazioni e analisi per una cyber defence predictive, nonché' di modalità di risposta offensiva, se previste dal patto atlantico. Considerando la capacità di un cyber attacco di colpire potenzialmente qualsiasi soggetto e servizio all'interno del paese, diviene strategico predisporre un'adeguata rete di nuclei operativi cyber all'interno di soggetti pubblici e privati (in primis gli asset sensibili) preparati ad essere coordinati a livello centrale; in caso di crisi cibernetica questo permette di intervenire rapidamente nelle azioni di contrasto e mitigazione. I nuclei operativi cyber dovranno essere presenti in qualsiasi realtà produttiva ed economica del paese, anche nelle realtà più piccole andando ad individuare un referente (ad es. IT manager interno o esterno, azienda partner, etc..) che possa essere qualificato (sempre rapportato alle dimensioni dell'organizzazione che deve gestire) a svolgere simile attività, come ad es. oggi avviene con la figura del DPO per il GDPR.

Una rete di "human firewall" gestiti centralmente ed addestrati ad operare e collaborare, attraverso procedure ordinarie e straordinarie, con un centro di controllo nazionale, questo inoltre permetterebbe di sviluppare una rete di intelligence permanente distribuita su tutto il territorio nazionale in grado, se ben organizzata, di inviare continui feed informativi anche in tempi normali. La nuova agenzia svolgerebbe a questo punto un ruolo strategico centrale nel coordinamento e la gestione in caso di attacco cibernetico in

ambito civile , nonché' militare e d'intelligence, gestendo direttamente i nuclei operativi cyber e mantenendo un continuo coordinamento con i centri di cyber security presenti in altri organi istituzionali (AISI, AISE, etc..).

I nuclei operativi cyber svolgerebbero invece un ruolo tattico/operativo. La logica di una simile struttura permetterebbe anche di individuare i profili più idonei alle componenti delle varie strutture, brevemente:

• Profili ideali per l'aspetto strategico (quindi come personale della nuova agenzia) sono da individuare nell'ambito del comando militare e accademico, per peculiari caratteristiche di gestione delle risorse, visione e ricerca e sviluppo.

• Profili ideali per i nuclei operativi cyber sono professionisti e aziende specializzate nella cybersecurity in grado attraverso le conoscenze e l'expertise sempre aggiornato, dovuto alla rapida evoluzione dei prodotti e delle soluzioni tecnologiche su cui quotidianamente lavorano e certificano le proprie competenze, di intervenire tecnicamente in maniera più rapida ed efficiente.

4. Framework Legale

"Prevedere un framework legale sulla base del diritto internazionale, europeo e nazionale, in caso di risposta cyber".

La complessità e l'incremento esponenziale delle attività illecite e degli attacchi, anche terroristici, commessi nel dominio cibernetico nei confronti di infrastrutture strategiche rende essenziale l'impegno della costituenda Agenzia per la Cybersicurezza nazionale (Agenzia) nella elaborazione di nuove modalità di condotta e criteri di attribuzione (accountability), sul presupposto che il cyber spazio è un non-luogo in cui sono quasi del tutto inapplicabili le tradizionali fattispecie giuridiche in materia penale e processual penalistica. A ciò si aggiunga che la tutela dei beni giuridici da proteggere in tale spazio (pubblici, privati, immateriali e/o collettivi) si fonda anche su un sistema normativo internazionale ed europeo "integrato", multilivello e in continua evoluzione, data la natura transfrontaliera di tali attacchi.

Ciò impone una radicale attività di rilettura delle tipologie di attacchi al Perimetro di sicurezza nazionale cibernetica, i quali, come avvenuto nel caso degli attacchi all'Estonia (2007) e Georgia (2019), richiedono una ridefinizione della legittima difesa potendo esprimere un potenziale altamente distruttivo nel mondo reale, specie se di intensità tale da comportare l'attivazione dell'art. 51 della Carta ONU e/o dell'art. 5 del Trattato NATO. Ne consegue la necessità di elaborare una normativa di cyber warfare e la previsione di una capacità difensiva e offensiva ibrida - innovativa e compartecipata con il mondo del privato – che includa l'impiego delle armi cibernetiche alle quali va applicato il diritto internazionale umanitario (art. 36 Prot. I del 1977 annesso alle 4 Conv. di Ginevra del 1949), nelle more della adozione di una convenzione internazionale attualmente in fase di elaborazione da parte delle Nazioni Unite (United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security). Infatti, in caso di consistenti, continuativi e generalizzati attacchi

cyber non dovrebbe essere esclusa una reazione ibrida operata sia nello spazio cibernetico, sia nello spazio fisico tesa alla distruzione dei cyber presidi da cui hanno avuto origine gli attacchi. A tal fine, e anche in risposta agli attacchi di minore intensità, l'Agenzia deve poter avviare un rapido e diretto coordinamento sia con il **Cyberspace Operations Centre** della NATO sia con le attività di cyber-resilience previste dalla Cyber security strategy dell'UE con l'ENISA e il Centro di competenza cyber dell'UE di Bucarest.

Altresì, è necessario uno staff di coordinamento in caso di attacchi di cyber terrorismo e di possibili interferenze suscettibili di influenzare i processi elettorali attraverso la Rete, per i quali manca, ad oggi, un'apposita normativa, e di cui l'Italia, per il tramite dell'Agenzia, potrebbe farsi promotore in seno all'Unione europea. L'importanza del framework giuridico brevemente indicato e proposto, nonché l'alta specializzazione richiesta dal diritto cyber, giustifica che l'Agenzia si doti di un Think Tank, composto da esperti giuristi del mondo militare e accademico, che individui apposite Cyber Guidelines in collaborazione con la NATO, l'ENISA e il Centro di competenza cyber dell'UE di Bucarest (da rendere disponibili in una banca-dati). Tale Think Tank dovrebbe operare altresì quale ente responsabile di un costante aggiornamento delle attività normative, operative e di intelligence messe in atto da Stati terzi (Stati Uniti, Cina, Federazione Russa, Israele, Korea del Nord e Iran).

Infine, compito dell'Agenzia dovrebbe essere quello di redigere delle Guidelines di digital forensic e di coadiuvare le indagini digitali (una sorta di CyberPol) per i casi di attacchi più gravi per fissare un vademecum circa la determinazione del luogo dell'evento, della legge applicabile e dell'eventuale giurisdizione competente, anche al fine di svolgere rogatorie cyber internazionali. Riguardo al diritto dell'Unione europea, a seguito dell'entrata in vigore del Regolamento sulla cibersicurezza (1° giugno 2021), atteso che l'Agenzia fungerà da base per il "Centro di coordinamento per la cybersecurity" ivi previsto, occorrerà predisporre il richiesto "toolbox" europeo per gli attacchi cibernetici.

5. Struttura Tecnica Centrale

"Prevedere una struttura tecnica centrale in capo alla Presidenza del Consiglio dei Ministri che si occupi di integrare le informazioni sia d'intelligence classica "HUMINT" sia di Cyber Intelligence per le infrastrutture critiche (IT e OT), in collaborazione con DIS e Consigliere Militare".

Parimenti ad un sistema informazioni di difesa, l'Agenzia, dovrebbe prevedere un organismo che interagendo con attività di intelligence e cyber security costituisca una risorsa, strutturata e organizzata, che si occupi di analisi, valutazione, collazione e diffusione dei dati processati e servienti alla sicurezza cibernetica. Tali attività possono essere incardinate all'interno del comitato tecnico strategico.

6. Censimento Centri di Ricerca

"Prevedere un censimento dei centri di ricerca nazionale sui temi di cybersecurity al fine di definire un framework nazionale di applicazione nei diversi ambiti IT e OT".

Si suggerisce la creazione di un registro aggiornato sui centri di ricerca e studi sui temi cyber i quali collaborino con l'Agenzia a livello nazionale sia per la sicurezza nei settori dell'Information Tecnology sia in quelli dell'Operational Technology. Il censimento dovrebbe essere in primis rivolto alle iniziative accademiche o comunque Inter-accademiche, senza trascurare consorzi come il Laboratorio Nazionale di Cybersecurity, Cyber 4.0 che già riuniscono le eccellenze nazionali.

7. Incentivazione della Ricerca e Benefit Fiscali

"Definire un modello di sgravi fiscali per le aziende che investono in ricerca sui temi di Cyber Security o che adottano tecnologie volte alla protezione dei dati e dei sistemi".

Visto i dati non soddisfacenti in merito alle aziende e infrastrutture che poco si interessano allo sviluppo della sicurezza interna aziendale, laddove pare addirittura vi sia stato un calo di investimenti in relazione alla cyber security, dovrebbero essere incentivate, oltre che per la cultura della sicurezza cibernetica, anche all'utilizzo di tecnologie e risorse deputate alla protezione dei sistemi informatici aziendali.

Si suggerisce pertanto la creazione di un modello di sgravi e detrazioni fiscali simile a quello già utilizzato per l'edilizia (bonus ristrutturazione, ecc.) al fine di creare un bonus di "ristrutturazione cyber", rivolto principalmente alle PMI. Incentivare sia acquisto di prodotto che di servizio, con maggior peso al servizio in quanto contribuisce a generare più occupazione e a mantenere un livello di sicurezza tendenzialmente maggiore.

La logica di un simile modello di sgravi fiscali dovrebbe:

- vincolare l'utilizzo delle detrazioni a investimenti con aziende paganti tasse in Italia, in modo da evitare una fuoriuscita di fondi pubblici.
- riconoscere punteggi extra negli appalti pubblici, a coloro che seguono il modello Framework Nazionale di cybersecurity.
- riconoscere una percentuale di sconto per chi ha sviluppato piani formativi che si rivolgano agli utilizzatori dei sistemi aziendali attraverso i quali si può diffondere una minaccia cyber.

8. Certificazione Nazionale Esperti Cybersecurity

"Predisporre dei percorsi di certificazione univoci chiari per gli esperiti di Cybersecurity sul modello SANS, ISO27001, GDPR o CertING, riconosciuti a livello Nazionale per gli operatori del settore".

Si suggerisce di pianificare, supportare e incrementare la cultura cyber security, attraverso la diffusione di una comunicazione mirata, chiara ed univoca; sostenere le iniziative volte alla conoscenza e alla formazione, in tutti gli ambienti; e organizzare percorsi di studi nazionali per operatori della cyber security dando loro possibilità di certificarsi come esperti nel settore.

In particolare, per le risorse inserite nel previsto CVCN, appare indispensabile il possesso di certificazioni specifiche di prodotto inerenti i vari ambiti e tecnologie oggetto della valutazione compiuta dal Centro.

Le attività di valutazione delle infrastrutture tecnologiche e di sicurezza operate su aziende pubbliche o private definite come Operatori di Servizi Essenziali vanno esperite da risorse in possesso di certificazioni di sicurezza di più alto livello derivanti dall'adozione di modelli quali NIST, ISO, CertING, GDPR allo scopo di poter effettuare un'effettiva valutazione complessiva dei livelli di sicurezza delle infrastrutture tecnologiche esaminate.

Occorre inoltre prevedere una formazione delle risorse orientata alla valutazione del rischio che consenta un'analisi interdisciplinare sullo stato in essere delle infrastrutture analizzate nonché sulle opportune azioni da intraprendere allo scopo di conseguire un soddisfacente livello di mitigazione del rischio.

9. Formazione e Aggiornamento

"Prevedere un'apposita formazione all'interno della scuola dell'obbligo nonché l'aggiornamento obbligatorio dei formatori".

Si suggerisce di definire un programma di diffusione nelle scuole dei principi e delle best practices della cybersecurity. Prevedere un percorso parallelo di formazione destinato sia a docenti che agli studenti. Nell'ambito degli investimenti previsti per elevare le conoscenze dei docenti, è necessario prevedere nei percorsi di selezione la presenza di skill adeguati preesistenti così come la possibilità di accedere a materiale didattico da illustrare agli studenti. I docenti devono essere messi in grado di trasmettere le conoscenze interagendo con gli studenti. Per questi ultimi è necessario predisporre un programma di formazione a partire dalla scuola primaria, nella quale dovranno essere trasmesse conoscenze basiche di informatica e di cybersecurity.

Il percorso dovrebbe essere arricchito a partire dalla scuola secondaria con approfondimenti su base volontaria delle tematiche di cybersecurity, stimolando gli studenti con attività pratiche e simulazioni, come la costituzione di gruppi cibernetici di difesa (cd. Blue Team) ed offesa (cd. Red

Team). Obiettivo finale è la formazione di risorse umane già in grado di accedere al mondo del lavoro qualora non interessate a proseguire un percorso di formazione universitario.

A tale riguardo dovrebbero essere previsti meccanismi di incentivazione (borse di studio) per studenti meritevoli che possano accedere a studi universitari attinenti ai diversi aspetti della cybersecurity. Mentre l'elaborazione di un livello idoneo di competenze dovrebbe essere affidata a figure accademiche di comprovata esperienza e capacità didattica.

10. Sviluppo di Tecnologie Cyber – Defence

"Prevedere lo sviluppo di tecnologie di Cyber Defense e Active Defense nel contesto Nazionale".

Si suggerisce di sviluppare dei programmi di ricerca, basati su fondi Europee e Nazionali, che puntino allo sviluppo di tecnologia nazionale e/o all'integrazione di diverse tecnologie esterne di alto valore tecnologico, con l'obiettivo di sviluppare piattaforme di Cyber Defense e Active Defense.

L'integrazione di componenti dovrebbe avvenire con il contributo dei diversi centri di ricerca nazionali e con eventuali partner esteri già qualificati a livello, sia sui i temi di Cyber Defense sia sui temi di Active Defense.

Commissione di Studi
Cyber Threat Intelligence & Cyber Warfare
SOCINT
Società Italiana di Intelligence