CAMMINO DIRITTO
Rivista di informazione giuridica
https://rivista.camminodiritto.it

Articolo Divulgativo

GOVERNANCE DELLA CYBERSECURITY IN EUROPA E OLTRE: ANALISI COMPARATA TRA ITALIA, FRANCIA, GERMANIA E IL MODELLO ANGLOSASSONE

L'articolo analizza comparativamente le strategie di governance della cybersecurity adottate da Italia, Francia e Germania, evidenziando i principali pilastri strategici e il progressivo allineamento dell'Italia ai modelli internazionali. L'indagine si estende al contesto transatlantico, con particolare attenzione alla NATO, all'UE e al modello anglosassone del Regno Unito, caratterizzato da una precoce e costante politica di investimenti pubblici. Lo studio si conclude con una riflessione sulle criticità e le potenzialità dei diversi approcci, con focus sulla capacità degli Stati di tradurre le strategie in infrastrutture operative efficaci e resilienti.

di **Mara De Martino**
IUS/21 - DIRITTO PUBBLICO COMPARATO
Articolo divulgativo - ISSN 2421-7123

Direttore responsabile
Alessio Giaquinto

Pubblicato, Lunedì 16 Giugno 2025

CamminoDiritto.it
ISSN 2421-7123

Abstract ENG

The article provides a comparative analysis of cybersecurity governance strategies adopted by Italy, France, and Germany, highlighting key strategic pillars and Italy's gradual alignment with international models. The study expands to the transatlantic context, with particular attention to NATO, the EU, and the UK's Anglo-Saxon model, characterized by early and consistent public investment. It concludes with a reflection on the main strengths and weaknesses of the different approaches, focusing on the states' ability to translate strategic plans into effective and resilient operational infrastructures.

Sommario: 1. Principi strategici delle politiche di Cybersecurity; 2. Modello Italiano-Francese-Tedesco a confronto; 3. Esperienza anglosassone in materia di Cybersecurity; 4. Cybersecurity nei paesi N.A.T.O e cooperazione N.A.T.O – U.E; 5. Problematiche connesse alla cyber sicurezza: Il caso Estonia 2007; 6. Considerazioni conclusive e prospettive future della cybersecurity.

1. Principi strategici delle politiche di Cybersecurity

Le origini della cybersecurity risalgono alla seconda metà del Novecento, con lo sviluppo dei primi sistemi informatici interconnessi. Già negli anni '60, la crescente complessità delle reti e l'emergere di minacce informatiche rudimentali – come l'accesso non autorizzato ai terminali – iniziarono a porre il problema della protezione delle informazioni digitali. Tuttavia, è con la nascita di internet e la sua diffusione su scala globale tra gli anni '80 e '90 che la sicurezza cibernetica assume una rilevanza strategica.

Inizialmente trattata come un sottoinsieme delle politiche IT, la cybersecurity ha progressivamente acquisito una dimensione autonoma, intrecciandosi con tematiche di sicurezza nazionale, difesa, economia e protezione delle infrastrutture critiche.

Gli attacchi cibernetici di matrice criminale, terroristica o statale hanno contribuito ad accelerare la definizione di strategie normative e operative, ponendo le basi per le prime politiche nazionali e sovranazionali in materia.

Uno degli attacchi di maggiore rilevanza della cyber sicurezza è avvenuto nell'aprile del 2007 allorquando l'Estonia fu oggetto di una serie di attacchi informatici, di tipo DDoS. [1]

Questa serie di attacchi determinò una completa paralisi dell'intera infrastruttura informatica del paese.

CamminoDiritto.it
ISSN 2421-7123

Fu a partire da quel momento che il settore della cyber sicurezza è oggetto di particolare attenzione da parte di tutti i paesi del mondo.

Questi nuovi timori hanno determinato, sotto il profilo internazionale, da un lato la nascita di numerose opportunità di business e di mercato ma contestualmente dall'altro hanno attirato un numero sempre maggiore, sotto il profilo quantitativo e qualitativo, di attacchi informatici.

Il principale di questi attacchi, sulla base di informazioni pubbliche acquisite, è stato l'attacco realizzato attraverso il malware "Stuxnet", l'unico sino ad ora registrato, realmente capace di danneggiare soprattutto fisicamente, l'infrastruttura critica bersaglio sfruttando i sistemi informatici che la governano. [2]

Invero, alla luce dell'emergente scenario, non sorprende come a partire dal 2010, quando l'allora vicesegretario della Difesa americana William Lynn III definiva il cyber spazio come "quinto dominio", la maggior parte dei paesi si sia immediatamente mosso al fine di realizzare una propria cultura strategica idonea ad affrontare le problematiche legate al cyber spazio.

Un passaggio che è possibile definire ''obbligatorio'' per far fronte ad una minaccia che negli ultimi anni cresce a ritmi vertiginosi finendo per incidere profondamente sull'economia e sulla competitività di ciascuna nazione.

Sulla base del raffronto di una serie di documenti strategici in materia di cyber sicurezza è possibile estrapolare, in chiave di confronto, circa 13 pilastri strategici, comunemente ricorrenti, caratterizzanti le varie politiche di cyber sicurezza dei principali paesi euro e non. I pilastri de qui bus sono così sintetizzabili:

Identificazione e classificazione delle infrastrutture critiche da proteggere; Definizione di trattati, leggi e regole di condotta nazionali e/o internazionali; Sviluppare rapporti diplomatici al fine di rafforzare le partnership internazionali; Concentrarsi sulla protezione dei diritti fondamentali, sulla privacy e sulle principali libertà fondamentali; Concentrarsi sul cyber crime; Considerare il cyber spazio come un vero e proprio dominio, insieme ai quattro già esistenti di cui si è parlato in precedenza; Realizzazione di apposite strutture politiche e decisionali al fine di far fronte alla crescente minaccia; Sviluppare una politica dell'informazione per finalità preventive; Incrementare i livelli di sicurezza, affidabilità e resilienza delle reti e dei sistemi; Realizzare e rafforzare sistemi di Information Sharing tra il pubblico e privato nell'ottica del potenziamento del c.d. "early

CamminoDiritto.it
ISSN 2421-7123

warning"; Aumentare la consapevolezza pubblica della minaccia e l'importanza della cybersecurity; Incrementare il numero di figure specializzate al contrasto; Incentivare l'innovazione, lo sviluppo e la ricerca. Elemento a carattere generale, che emerge da una prima analisi in chiave comparata delle cyber-strategies ad oggi pubblicate, concerne sicuramente il numero di paesi membri che si sono dotati di una strategia già formalizzata.

Questo dato è sicuramente rilevante, atteso che ci consente di riflettere sull'attenzione e sul valore attribuito alla sicurezza informatica e delle informazioni.

Volendo riflettere nello specifico la nostra attenzione ai paesi dell'eurozona, tra le cyber strategy di matrice europea emergono alcuni elementi in comune tra i quali: la Realizzazione di trattati, regole e leggi nazionali ad hoc; lo sviluppo dei rapporti diplomatici e di partnership internazionali; il rafforzamento e la condivisione dell'information sharing.

Paesi come la Francia, Finlandia, Germania e Paesi Bassi, risultano essere gli unici paesi europei ad aver provveduto nell'ottica di tale rafforzamento, considerando il cyber spazio come dominio di warfare. Tra questi paesi solo la Francia ed i Paesi Bassi hanno esplicitamente formalizzato questo settore come settore strategico, riconoscendo la necessità di creare una strategia di deterrenza, con finalità di prevenzione. [3]

Sotto il profilo internazionale individuiamo tra i tratti comuni alle 29 cyber-strategy ad oggi rese pubbliche esclusivamente i seguenti pilastri: Lo sviluppo di rapporti diplomatici; l'incremento dei livelli di sicurezza ed affidabilità delle reti e dei sistemi; lo sviluppo ed il rafforzamento di un efficace sistema di information sharing.

Appare di tutta evidenza notare come la strada volta alla creazione di un approccio globale sia ancora fortemente incardinato sulle attività diplomatiche e di partenariato; così come appare di tutta evidenza come sia aumentato e sia in constante aumento il numero degli Stati che hanno provveduto a prendere seriamente in considerazione il cyber spazio come vero e proprio dominio.

Si considerino paesi come gli Stati Uniti, la Russia, la Corea del Sud, il Giappone, l'Australia, la Norvegia, la Colombia. Tra questi, solo gli Stati Uniti e la Russia hanno considerato di realizzare una strategia fondata sulla deterrenza, atta a prevenire eventuali conflitti nel cyber spazio.

Di formante completamente opposto le impostazioni strategiche di paesi come Cina ed Israele, di matrice prettamente "offensiva", di cui tuttavia i documenti strategici non sono

CamminoDiritto.it
ISSN 2421-7123

ancora pubblici. Sotto il profilo internazionale è altresì possibile estrapolare alcuni elementi di base che costituiscono l'epicentro dei documenti strategici analizzati, essi sono: La creazione di leggi e regole di condotta nazionali ed internazionali; la realizzazione di rapporti diplomatici; focus sulla protezione dei diritti fondamentali e sulle libertà di espressione; focus sul cyber crime; incremento dei livelli di sicurezza, affidabilità e resilienza delle reti e dei sistemi informatici; rafforzamento dell'information sharing e delle figure professionali.

A partire dal 2009, da quando l'allora Presidente americano Barack Obama ha posto l'accento sulla minaccia legata al cyber spazio annoverandola tra gli elementi principali della sua agenda politica e dichiarando apertamente trattarsi di una delle sfide più serie per l'economia e la sicurezza nazionale, il governo degli Stati Uniti si è imposto anche in questo settore come attore principale ed indiscusso trascinatore del pensiero strategico internazionale. [4]

Seppur considerandosi che il primo Piano Nazionale per la sicurezza dei sistemi informatici americani risale al 2000 e la prima strategia nazionale ufficiale in materia risale al 2003, è solo a partire dalla metà del 2009 che la materia ha iniziato a riscuotere crescente interesse. Artefice di questo improvviso interessamento globale: la spinta del governo americano verso i temi di cyber sicurezza e del cyber warfare; i cospicui finanziamenti riservati a quei settori nonostante la forte recessione economica; l'enorme attenzione mediatica per altro sempre in crescita; l'aumento della divulgazione pubblica degli attacchi informatici andati a buon fine. [5]

Fondamentale notare come la rapida evoluzione del pensiero strategico americano in materia di cyber sicurezza ha determinato nell'ultimo decennio l'ammassarsi di numerosi principi strategici e direttive del governo, difficili da raccordare ma soprattutto di complessa implementazione. Ciò ha comportato, di fatto, la circostanza che il governo americano, per quanto rappresenti uno dei principali attori in questa lotta, non sia esente da criticità.

Tra le evidenziate criticità spiccano difficoltà per le agenzie federali di effettuare un adeguata e corretta valutazione dei rischi derivanti dal cyber spazio; la difficoltà da parte delle Agenzie deputate alla protezione delle infrastrutture critiche, di comprendere correttamente quali siano le norme ed i regolamenti in materia di cyber security da applicare al loro specifico settore; la persistente difficoltà di rilevare e mitigare gli attacchi informatici, in ragione della mancanza, in seno al Department of Homeland Security (DHS) di un efficace sistema di analisi predittiva delle minacce derivanti dal cyber spazio. [6]

CamminoDiritto.it
ISSN 2421-7123

Una soluzione a tutte queste problematiche potrebbe essere raggiunta con la predisposizione di un nuovo documento strategico nazionale con la finalità di sintetizzare ed armonizzare l'insieme di direttive e di strategie fino ad oggi prodotte, descrivendo in modo semplice, puntuale e completo l'attuale condizione dell'architettura strategica nazionale americana in materia.

Solo attraverso questi ulteriori accorgimenti il nuovo documento strategico nazionale americano potrà far fronte alle minacce derivanti dal cyber spazio in modo concreto ed efficace. [7]

È possibile affermare che i principi cardine estrapolabili dalle politiche di cyber security, tanto in ambito europeo tanto in ambito internazionale, pongono in evidenza un approccio comune delle principali questioni strategica in piena armonia con la globalità del fenomeno. È auspicabile che ciascuno stato interessato dell'eurozona e non fondi il proprio quadro strategico nazionale in coerenza con i principi sopra enucleati.

2. Modello Italiano-Francese-Tedesco a confronto

Bisogna ben tener presente che un paragone del nostro sistema di cybersecurity con l'impianto francese e quello Tedesco appare quasi ridicolo, considerato che la Francia e la Germania sono tra i principali partner in materia di cybersecurity nel continente europeo.

Entrambe le potenze richiamate possono contare già da diversi anni su una robusta struttura atta alla difesa dalle minacce provenienti dal cyber spazio.

Il cyberspazio e le relative questioni di cybersicurezza e di cyber strategy sono un elemento chiave nel mondo odierno, sia per il settore privato quanto per il settore pubblico. Nell'ultimo decennio hanno acquisito maggiore importanza, soprattutto con il perdurante crescere degli attacchi informatici condotti da gruppi o enti avversi al blocco Occidentale su tutta Russia e Cina.

Questi attacchi in numerose occasioni hanno determinato pesanti conseguenze, si pensi che nell'ultimo decennio si è arrivati ad una media di 106 attacchi ogni mese. In Italia si è assistito ad un aumento vertiginoso degli attacchi cyber verso aziende o enti. [8]

Dato da notare è come una buona parte di questi attacchi sfrutti quelle che sono le criticità dei sistemi di rete e delle infrastrutture critiche prese di mira. [9]

CamminoDiritto.it
ISSN 2421-7123

Per quanto concerne la prospettazione delle principali politiche di governance in materia di cybersecurity tra i principali attori del panorama europeo vi è quello francese. [10]

In Francia il contesto della cyber sicurezza vede i suoi primi sviluppi intorno al 2008, allorquando venne creata un'agenzia destinata alla sicurezza cibernetica, a seguito della presentazione del c.d. "Libro Bianco sulla difesa e la sicurezza nazionale del 2008" durante il periodo di presidenza di Sarkozy. [11]

Sulla base di tali scelte giace la necessità di identificare i rischi maggiori per le infrastrutture prese in considerazione nonché la necessità di dotarsi di una idonea capacità di rilevazione e contrasto di tali minacce.

Sulla base di tali prospettazioni nacque la c.d. "A.N.S.S.I. – Agence Nationale de la Securitè des Systemes d'Information" ovverosia un'autorità pubblica posta sotto il controllo diretto del governo francese ed in diretto raccordo con il Segretario Generale per la Difesa e sicurezza Nazionale alla quale vennero specificatamente riservate funzioni in materia di cybersecurity. [12]

L'Agenzia in questione è struttura in cinque differenti divisioni con l'aggiunta di un'unità di anticipazione (C.A.C.) ed ha quale finalità lo svolgimento di una serie di attività sia di tipo normativo sia di tipo operativo, a partire dalla emissione di norme e regolamenti con contestuale verifica della loro applicazione a terminare con operazioni di verifica e di monitoraggio dei meccanismi di allerta e rapid response.

Alla stessa agenzia viene devoluto l'importante compito di rilasciare certificati di sicurezza per i principali prodotti e fornitori di servizi ICT.

L'agenzia in questione, a partire dal 2013, ha visto accrescere la propria rilevanza vedendo aumentare poteri e prerogative soprattutto in relazione agli operatori considerati di vitale importanza, ovverosia coloro i quali che, in caso di attacco, se fossero messi totalmente o parzialmente fuori uso, comporterebbero un potenziale danno economico. Di non secondaria importanza anche l'implementazione dell'apposito CSIRT nazionale ad opera dell'A.N.S.S.I. con il fine di monitorare e difendere i sistemi francesi da attacchi informatici, nonché fornire servizi di training ed awareness.

Uno dei documenti indubbiamente di maggiore significato è rappresentato dalla "Strategia nazionale francese per la sicurezza digitale" annunciata nel 16 ottobre del 2015 dal primo ministro francese Valls e funzionalmente realizzata per supportare la transizione digitale della società francese. [13]

CamminoDiritto.it
ISSN 2421-7123

Indubbio che questo documento abbia rappresentato un primo segnale all'interno dell'eurozona che pone la Francia senza precedenti come leader nella promozione di una "road map" per l'autonomia strategica digitale.

La strategia de quo, secondo quanto stabilito in essa, è guidata dalla A.N.S.S.I. e rappresenta uno dei principali strumenti idonei ad approntare un adeguata risposta ai problemi legati all'era digitale; questo perché la transizione digitale sicuramente favorisce l'innovazione e la crescita ma al contempo comporta numerosi rischi per lo Stato, nonché per i principali attori coinvolti nel cyber spazio.

Fenomeni come lo spionaggio, la criminalità informatica, la propaganda etc. richiedono una risposta collettiva e coordinata sulla base di alcune priorità strategiche quali: la difesa e la tutela degli interessi e delle libertà fondamentali; maggiore fiducia digitale; maggiore sensibilizzazione ed informazione.

Facendo un passo indietro all'adozione del Libro Bianco, appare opportuno sottolineare come già in quel documento, rasentandosi la pericolosità dei rischi provenienti dal cyber spazio, si evidenziasse l'impatto che tali minacce avrebbero avuto sulla vita di un'intera nazione, atteso che l'odierna società appare fortemente e strettamente interdipendente ai processi IT in ragione del maggiore e sempre crescente uso di tali tecnologie.

È possibile affermare che con il ''Libro Bianco'' del 2008 sia stato realizzato un invito rivolto allo stato francese a sviluppare capacità di prevenzione e risposta in relazione agli attacchi informatici, facendo di ciò una delle priorità della sicurezza nazionale. Nel campo della prevenzione viene auspicata altresì l'utilizzazione di prodotti e reti ad alta sicurezza, nonché la realizzazione di un vero e proprio bacino di competenze al servizio delle p.a. e degli operatori. e l'A.N.S.S.I. è stata realizzata in linea con questo libro Bianco.

Con decreto istitutivo dell'associazione de quo è stato istituito un vero e proprio comitato strategico per la sicurezza nazionale al fine di realizzare una vera e propria strategia. (che verrà poi ad essere realizzata nel 2015).

Parallelamente alla realizzazione dell'A.N.S.S.I. viene istituto anche un osservatorio di sicurezza informatica di zona, il c.d. "OzSSI", per ogni area di difesa e sicurezza sul territorio nazionale. Lo scopo è quello di diffondere a livello nazionale una maggiore consapevolezza al fine di migliorare la sicurezza informatica. [14]

Doveroso specificare che, prima della realizzazione di una prima vera e propria strategia

CamminoDiritto.it
ISSN 2421-7123

per la sicurezza informatica nazionale, nel 2013 è stato pubblicato un nuovo Libro Bianco al fine di evidenziare come in quegli anni gli attacchi informatici contro le reti ed i sistemi informativi di numerose imprese francesi del settore pubblico e privato fossero in aumento. Con la realizzazione di questo nuovo documento, a partire da quel momento, lo stato francese non si sarebbe più soltanto limitato a provvedere alle proprie esigenze di cybersecurity ma piuttosto anche quelle degli operatori di vitale importanza, il cui danneggiamento avrebbe avuto un forte impatto economico e militare sulla vita della Nazione.

Questo "potenziamento/aggiornamento" della sicurezza informatica francese ha stabilito che le reti ed i sistemi informativi più critici, riferiti a questi operatori, avrebbero dovuto: rispettare gli standard di sicurezza definiti dall'ANSSI, disporre di solidi meccanismi di rilevamento e prevenzione delle minacce; disporre di un adeguato meccanismo di segnalazione e reporting. [15]

Quanto prospettato in tale documento di aggiornamento del 2013 è stato poi recepito nella legge di programmazione militare, L.n.1168 del 2013 adottata il 19 dicembre. La legge de quo ha seguito e si è adattata agli orientamenti fissati dall'aggiornato Libro Bianco.

Questo meccanismo ha consentito agli operatori nazionali "vitali" dei settori pubblico e privato di proteggersi nel migliore dei modi ed ha stabilito, in capo all'A.N.S.S.I. ed altri enti dello stato, importanti funzioni di supporto nell'ottica di un rafforzamento della sicurezza interna, attribuendo infine nuove prerogative in materia in capo al Presidente del Consiglio dei ministri francese.

E' opportuno evidenziare una rapida disamina delle politiche di governance in materia di cyber sicurezza del governo tedesco; in Germania già nel 1991 è stato fondato il B.S.I. (Bundesamt fur Sicherheit in der Informationstechnik) ovverosia l'ufficio federale per la sicurezza informatica. [16]

L'ufficio in questione nasce come autorità dedicata alla sicurezza informatica dei soli apparati federali. A differenza del modello francese il ruolo del B.S.I. ha assunto connotati di tipo prettamente operativo, in particolar modo con riferimento alla protezione delle reti e delle strutture informatiche nazionali tedesche, affidando al Consiglio per la cybersecurity (Cyber – Sicherheitstrat) l'importante compito di delineare un vero e proprio piano strategico del governo tedesco.

Il B.S.I., a seguito dell'aggiornamento della Direttiva Nis-1 di cui si è approfondito a dovere nel capitolo precedente, è stato incaricato della prevenzione di minacce alla sicurezza dei sistemi IT, del rilascio dei certificati di sicurezza nonché dello sviluppo dei

CamminoDiritto.it
ISSN 2421-7123

relativi standard minimi.

Altro potenziamento che ha interessato l'ufficio in questione si è avuto nel 2015 con l'adozione dell'IT Security Act, unitamente ad una specifica regolamentazione riferita alle infrastrutture critiche. [17]

Con l'introduzione del security act 2.0, la cui adozione si è avuto nel maggio dell'anno corrente, il B.S.I. è stato dotato di ulteriori poteri, questa volta di tipo "pro attivi", ai fini della individuazione dei rischi e delle vulnerabilità, connessi alle principali infrastrutture critiche, procedendo con la valutazione di elementi come la sicurezza dei sistemi informatici di infrastrutture, dei servizi digitali e del settore pubblico.

Volendo attualizzare il discorso appare opportuno sottolineare che la Germania il 14 giugno dell'anno corrente ha adottato la sua prima Strategia di sicurezza nazionale. Il primo documento di questo tipo fu adottato dal paese solo dopo la Seconda guerra mondiale.

Il documento è stato definito dagli esponenti del governo come un grande cambiamento ed ha quale obiettivo quello di integrare la pianificazione militare con altre questioni di sicurezza. L'idea posta alla base della strategia è quella di considerare anzitutto tutte le minacce interne ed esterne alla sicurezza della Germania. [18]

Il documento identifica tutta una serie di aree da intendersi come delle vere e proprie sfide "centrali" per la sicurezza del paese, quali: la difesa nazionale e dell'Alleanza atlantica; la protezione civile; protezione della tecnologia e delle infrastrutture critiche; sicurezza informatica e spaziale; sicurezza alimentare e prevenzione pandemica e climatica.

Ponendo l'attenzione sul documento in questione è possibile leggere che l'obiettivo del governo federale tedesco è quello di rafforzare la sicurezza lungo tre assi specifici: la capacità di difesa, di resilienza e di sostenibilità. [19]

Nel testo vengono citati il "Climate Adaptation Act" ed una versione rivisitata della "Strategia nazionale per la biodiversità". La strategia in questo punto verte sull'impegno del governo tedesco nel recepimento di regolamenti vincolanti, in ossequio al diritto internazionale, al fine di affrontare le future pandemie o eventi catastrofici.

Uno dei punti più controversi della strategia in materia di cybersecurity concerne il c.d. "hack-back" ovverosia la pratica di condurre attacchi informatici infiltrandosi nei sistemi di rete degli aggressori, quindi in buona sostanza una vera e propria politica del

CamminoDiritto.it
ISSN 2421-7123

contrattacco. Lo scopo del contrattacco è quello di eliminare i dati intercettati o disabilitare l'infrastruttura attraverso la quale il nemico sta agendo. [20]

Ad onore del vero la politica dell'hack-back era stata in primo momento escluso nell'accordo di colazione del 2021 per poi trovare successivo ingresso a seguito del suscitato interesse ad opera del ministro federale dell'interno Nancy Faeser. Occorre sottolineare che nella strategia manca completamente il riferimento ad una riforma strutturale dei processi decisionali, non si è riusciti, in altri termini, a realizzare un Consiglio di Sicurezza nazionale con finalità di coordinamento dell'azione governativa. [21]

E' possibile in tal senso affermare che i nostri baricentri di riferimento in materia di cyber sicurezza stiano tendendo ad un rapido sviluppo ed evoluzione, il fatto che siano nati così tardi rispetto a quelli istituti dai partner francesi e tedeschi denota in assoluto la necessità di continuare ad investire in un contesto che sta assumendo con il passare degli anni un ruolo sempre più cruciale nello scacchiere internazionale il tutto nell'ottica della realizzazione di un sistema uniforme e coeso.

3. Esperienza anglosassone in materia di Cybersecurity

Per quel che concerne il Regno Unito appare opportuno sottolineare che l'apporto alla particolare questione della cyber sicurezza è molto simile rispetto a quello statunitense.

Il Regno Unito, ormai ex membro dell'Unione europea, diversamente che dagli altri paesi dell'eurozona e sotto l'impulso dei paesi nato, ha istituito il suo primo centro di sicurezza cibernetica a Londra nel 2009. Si è cercato di adottare un approccio piuttosto accentrato nella formulazione di strategie e di programmi soprattutto a seguito del lancio del National Cyber Security Programme. [22]

Nel 2013 il Regno Unito ha reso pubblico che per lo sviluppo di capacità da impiegare nel dominio cibernetico andava annoverata anche la capacità di attacco. Invero, le ultime operazioni offensive in tale contesto risalgono appena al 2007.

Sempre nell'anno 2013, con la finalità di coordinare le operazioni di cyber warfare, venne creato il Joint Forces Cyber Group composto da due unità cibernetiche, sotto la direzione congiunta del Ministero della Difesa e dal Government Communication Headqarter. [23]

Nel 2015 la Strategic Defence and Security Review ha sottolineato che la minaccia cibernetica rientra tra le principali minacce che il paese è chiamato ad affrontare in futuro

CamminoDiritto.it
ISSN 2421-7123

e per la quale l'apparato governativo deve essere messo nelle condizioni di approntare una idonea e preventiva risposta. [24]

Nell'anno 2016 venne formulata la National Cyber Security Strategy incentrata su tre pilastri principali. Primo tra questi è l'obiettivo di assicurare la difesa e la resilienza dei networks britannici, nonché delle principali attività economiche, dei dati dei cittadini e delle pubbliche istituzioni. Altro obiettivo ha ad oggetto lo sviluppo di una vera e propria industria della sicurezza cibernetica di modo da assicurare lo sviluppo di sistemi di difesa all'avanguardia. Conclusivamente ritroviamo, tra gli obiettivi, la capacità di deterrenza di modo da rendere il Paese un difficile bersaglio di attacco.

Nell'alveo di tale ultimo obiettivo la strategia delinea il principio di Active Cyber Defence (a.c.d.) ovverosia la capacità di rafforzare il network ed il sistema di difesa, prospettandosi la possibilità di mettere in atto operazioni cyber offensive per finalità di mera deterrenza, talvolta anche in assenza di un vero e proprio attacco, anche se nel rispetto della legislazione nazionale e non in materia. [25]

Il documento getta poi le basi per la realizzazione di un National Cyber Security Centre (N.c.s.c.) quale organo centrale deputato alla sicurezza cibernetica a livello nazionale con ruolo primario sotto il profilo del coordinamento delle politiche di settore; in diretto contatto con i ministeri e le agenzie a cui è devoluta la realizzazione e l'attuazione dei programmi di sicurezza cibernetica.

L'organo in questione, sancisce il documento, è coordinato dal prima citato G.c.h.q. il quale, in possesso di informazioni di sicurezza riservate, dà la possibilità al centro di avere uno screening della situazione completo.

Il N.c.s.c. coordina anche le azioni del Cyber Security Operations Centre ovverosia un centro di difesa e risposta ad attacchi cibernetici rivolti alle infrastrutture ed ai sistemi del Ministero della Difesa. Con la strategia in questione sono stati stanziati ulteriori finanziamenti pari ad un ammontare di 1,9 miliardi di sterline, nel quinquennio 2016-2021, incrementandosi di un ulteriore 55% rispetto al finanziamento reso nel periodo precedente; alcuni di questi finanziamenti sono poi stati utilizzati per la realizzazione di ulteriori due centri per l'innovazione cyber da impiegarsi in procurement innovativo e "secure by design". [26]

Si cerca, oltretutto, di stimolare lo sfruttamento delle conoscenze in ottica multipiano tra aziende, università ed istituzioni. La strategia, infine, sottolinea l'importanza di operare a livello internazionale nel contrasto agli attacchi promuovendo collaborazione anche attraverso framework collaborativi ad hoc. A tal proposito, insieme ad Australia, Canada,

CamminoDiritto.it
ISSN 2421-7123

Nuova Zelanda e Stati Uniti, Londra fa parte del Five Eyes network che costituisce la più stretta partnership internazionale in materia di intelligence. [27]

La Gran Bretagna rappresenta, forse l'unico tra i paesi un tempo europei, più evoluti in materia in considerazione della forte influenza esercitata dai paesi U.S.A., ma soprattutto la prima nazione ad erogare importanti fondi in materia di cyber sicurezza, in ragione della prematura consapevolezza di quanto il dominio digitale fosse importante per la tutela della politica e dell'economia dell'intera nazione. [28]

Già a partire dagli anni 2000, dunque, il Regno unito predisponeva già di un adeguato sistema di controllo e di gestione del rischio da minaccia cibernetica, poi nel 2009 venne lanciata la prima vera e propria strategia nazionale di cybersecurity. Dalla strategia in questione è data evincersi la consapevolezza del Regno Unito in ordine alla necessità di predisporre importanti finanziamenti per obiettivi di cyber sicurezza. Viene maturata molto presto la consapevolezza che importanti finanziamenti avrebbero consentito di trarre vantaggio da sistemi di intelligence di alto livello e da altre elevate capacità di sicurezza.

Nel 2015 il governo britannico decide di trasformare questa strategia nazionale in una strategia nazionale quinquennale per la sicurezza informatica, arrivandosi ad un nuovo modo di pensare alla gestione degli incidenti informatici. La nuova strategia ha consentito la realizzazione dell'Active Cyber Defence ed ha posto le condizioni per un diverso partenariato con il settore privato ma ciò ha poi trovato una nuova sede nel National Cyber Security Center (N.C.S.C.) il quale è lo stesso centro nazionale a fornire, in caso di minacce, consigli e linee guida su come mitigare molti dei rischi previsti.

A partire dal 2016 in poi si sono registrati numerosi sviluppi e solo recentemente il governo britannico ha lanciato la sua strategia di sicurezza 2022-2030, la "Building a Cyber resilient public sector", attraverso la quale si cerca di soffermare l'attenzione sul settore pubblico. Stando ad una serie di reports le organizzazioni governative sono prese principalmente di mira dagli incidenti informatici; pertanto, si è deciso di intervenire prevalentemente in quel settore nei prossimi anni.

Sono stati investiti, per il funzionamento di questa strategia, ulteriori 40 milioni di sterline. L'obiettivo prospettato è quello di realizzare una più efficiente resilienza informatica in tutte le organizzazioni governative del paese. [29]

4. Cyber-security nei paesi N.A.T.O. e cooperazione N.A.T.O – U.E.

CamminoDiritto.it
ISSN 2421-7123

Per comprendere l'approccio Nato alle dinamiche di cyber security e cyber defence appare opportuno sottolineare che l'approccio dell'Alleanza Atlantica verso la cyber defence si è evoluto significativamente solo negli ultimi anni con la consapevolezza crescente che un attacco cibernetico avesse il potenziale di causare danni imparagonabili alle strutture essenziali di un paese. Addirittura, riconoscendosi ciò, si è affermato che la cyber defence doveva diventare un caso di difesa collettiva di cui all'art.5 del Trattato di Washington. [30]

La Nato negli ultimi anni ha adottato politiche e piani d'azione istituendo comitati, agenzie e centri operativi con l'obiettivo di integrare il dominio cibernetico.

La strategia dello US Cyber Command si basa sulla persistenza delle operazioni, mantenendo l'iniziativa tramite una campagna articolata senza soluzione di continuità tra azioni difensive e offensive. Il Regno Unito ha adottato un approccio simile a quello americano e già dal 2013, come analizzato nel paragrafo precedente, ha reso pubblico che lo sviluppo di capacità da impiegare nel dominio cibernetico a livello nazionale includeva anche quelle offensive. [31]

Il vertice di Varsavia ha portato anche alla firma del primo Cyber Defence Pledge volto a istituire una piattaforma comune per migliorare le capacità nazionali di difesa e resilienza rispetto ad un attacco cibernetico. [32] Si tratta di un focus in linea con l'elevata importanza attribuita agli attacchi cibernetici, giudicati sempre più frequenti, complessi e distruttivi, al punto da poter attivare l'articolo 57, tanto che nel comunicato del vertice di Bruxelles del 2018 viene esplicitamente affermato che la difesa cibernetica è parte della difesa collettiva Nato.

Di fronte a questa situazione che ha visto anche il moltiplicarsi di attacchi cibernetici durante la prima ondata di Covid-19, a giugno 2020 il North Atlantic Council ha riaffermato che i Paesi membri sono: "determined to employ the full range of capabilities, including cyber, to deter, defend against and counter the full spectrum of cyber threats." (determinati ad aumentare capacità di deterrenza e di difesa nonché dell'intero spettro di questioni relative al cyber spazio). [33]

Da notare come la Nato si dichiari pronta ad usare non solo capacità cyber ma anche aeree, marittime o terrestri, per rispondere ad un attacco cibernetico, considerando quindi tutti i domini operativi in modo integrato ai fini della deterrenza e difesa in linea con l'integrazione del Cyber Operation Centre nella struttura di comando Nato come deciso durante il vertice di Bruxelles.

Il vertice di Londra del 2019 ha dato nuovo slancio politico-strategico alle attività Nato

CamminoDiritto.it
ISSN 2421-7123

nel campo cibernetico assieme a quello spaziale, nella consapevolezza della competizione geopolitica a tutto campo con Cina e Russia nel quadro di un "multipolarismo aggressivo". Non a caso nel 2020 il rapporto del Gruppo di Riflessione sulla Nato in prospettiva 2030 ha attribuito grande importanza alle Emerging and Disruptive Technologies (Edt) intese sia come settore sul quale investire maggiormente sia come sfide, tra cui rientrano prioritariamente proprio quelle relative alla cyber defence, in primis l'Artificial Intelligence (Ai). [34]

Già nel 2016 la Nato ha riconosciuto il cyberspace come dominio operativo nel quale l'Alleanza deve essere in grado di operare altrettanto efficacemente che in quelli terrestre, marittimo ed aereo.

Gli alleati mantengono in ogni caso la leadership politico-militare anche nel campo cibernetico e le strutture Nato servono, in primo luogo, come sostegno al processo decisionale. A livello operativo, nel 2019 all'interno del Allied Command Operations (Aco) è stato creato un Cyberspace Operations Centre (Cyoc) responsabile delle operazioni cyber Nato, a supporto dei comandi operativi soprattutto nel monitorare il cyberspace e coordinare le operazioni in questo dominio con quelle in campo terrestre, navale o aereo. [35]

Il Cyoc potrebbe aprire la strada alla futura costituzione di un Comando Nato per le operazioni cibernetiche al pari dei comandi operanti nel domino aereo, marittimo e terrestre. [36]

A livello tecnico la Nato Communications and Information Agency (Ncia), istituita nel 2012, fornisce molte delle capacità necessarie alle strutture dell'Alleanza in termini di cyber defence. [37]

Infine, al di fuori del comando militare integrato alleato, il Cooperative Cyber Defence Center of Excellence (CCDCoE), inaugurato già nel 2008 in Estonia (a seguito dell'interruzione che ha destabilizzato un'intera nazione, di cui parleremo più approfonditamente nel paragrafo successivo), prepara studi e report su temi di interesse per la difesa cibernetica e ospita esercitazioni periodiche come il LockedShield dal 2010.

Il riconoscimento Nato del dominio operativo cibernetico sta influenzando anche lo sviluppo delle dottrine e capacità militari alleate, nonché l'addestramento del personale da parte del Paesi membri in modo da aumentare la difesa e resilienza su questo fronte.

Il Cyoc è l'attore chiave al riguardo mentre l'Act considera il dominio cibernetico nel

CamminoDiritto.it
ISSN 2421-7123

quadro più ampio della trasformazione militare e dell'innovazione tecnologica in una prospettiva di medio-lungo periodo.

Gli stati, a loro volta, utilizzano la piattaforma del Cyber Defence Pledge per valutare autonomamente nel tempo i progressi sullo sviluppo delle capacità nazionali di difesa cibernetica anche attraverso il rapporto finale sull'attuazione degli impegni presi e per scambiarsi informazioni e buone prassi al riguardo.

Un ruolo importante è giocato ovviamente anche dal Nato Defence Planning Process (Ndpp), la procedura principale omnicomprensiva e di lungo periodo, con cui i Paesi membri concordano gli obiettivi nazionali di sviluppo delle rispettive forze armate in modo da contribuire anche agli impegni Nato di difesa collettiva e gestione delle crisi. [38]

Nel quadro del Ndpp, dal 2012 sono stati inseriti degli obiettivi di sviluppo di capacità di cyber defence, i cui progressi vengono valutati periodicamente.

Per le caratteristiche intrinseche del domino cibernetico ove l'innovazione tecnologica è guidata principalmente da aziende private che spesso non operano nel campo militare, la cooperazione tra la Nato e la controparte industriale, compresa quella civile a vario titolo coinvolta nella gestione delle infrastrutture critiche, è estremamente importante.[39]

Su questa base le istituzioni dell'Alleanza e dell'Unione hanno scambiato informazioni su strategie, politiche, standard e attività di addestramento relative alla difesa cibernetica, ed hanno partecipato alle rispettive esercitazioni – la suddetta Cyber Coalition Nato e la Cyber Europe dal lato UE.

Nel 2016 le due organizzazioni hanno firmato un documento, il "Technical Arrangement on Cyber Defence", che governa lo scambio di informazioni non classificate a beneficio della capacità di entrambe di avere un quadro più completo della situazione e di proteggere i rispettivi network.

La cooperazione Nato-Ue sulla cyber defence è oggetto di incontri regolari durante i quali ci si aggiorna reciprocamente anche sulle rispettive attività settoriali; i progressi di tale partenariato sono stati riconosciuti nel 2019 dallo stesso Stoltenberg. Al di là della stretta cooperazione con l'Ue, la Nato è aperta a cooperare con l'Onu, l'Osce, e stati terzi che condividano lo stesso approccio alleato alla cyber defence.

5. Problematiche connesse alla cyber sicurezza, il caso Estonia 2007

CamminoDiritto.it
ISSN 2421-7123

Nel maggio del 2007 l'Estonia ha subito uno dei più importanti attacchi cibernetici della storia fin ora registrati. L'attacco in questione nel giro di poche ore ha compromesso numerosi servizi, sia di natura istituzionale che non, gettando nel panico un'intera nazione. [40]L'evento che ha dato il via a questo attacco digitale sarebbe in realtà alquanto inusuale, atteso che tutto è partito dalla decisione del governo estone di rimuovere la statua del Soldato di Bronzo nel centro di Tallinn, capitale del paese.

Il monumento era stato lì costruito dai sovietici per commemorare i loro caduti in guerra. Per i cittadini estoni la statua rappresentava il simbolo di un'occupazione opprimente. [41]

L'attacco cibernetico, che in definitiva non è stato possibile ricondurre con assoluta certezza al governo russo, ha causato il collasso dell'intero sistema bancario, di numerosi servizi governativi, di alcune società e del sistema mediatico, finendo con l'isolare completamente il paese dal resto del mondo. Sulla base di successivi reportage è stato possibile calcolare, in quegli anni, un traffico notturno in entrata in Estonia di circa 20.000 pacchetti di dati al secondo.

Nei momenti in cui si è consumato l'attacco la soglia appena richiamata è giunta fino ai 4 milioni di pacchetti al secondo. Per comprendere le dimensioni del fenomeno si immagini che, a livello globale quasi 1 milione di computer si è improvvisamente spostato su una serie di siti Estoni, da quello del Ministero degli Esteri alle principali banche del paese.

A questo punto appare spontaneo chiedersi come sia stato possibile realizzare un attacco di simile portata in così poco tempo. La risposta è piuttosto semplice: sulla base di una serie di report risulta che l'attacco in questione sarebbe strato strutturato su più fronti. [42]

La presenza di operatori più che esperti e l'utilizzo di vari software avrebbe permesso l'abbattimento di tutte le frontiere della nazione. Nel frattempo, si è sviluppato anche il c.d. "Manuale di Tallin" sul diritto internazionale applicabile alla guerra informatica.

Il manuale si è mosso nel senso di fornire un regolamento comune nel cyber spazio in ossequio ai principi del diritto internazionale.

L'esperienza estone ha avuto un notevole impatto nella corsa alla cyber security del paese. Nel 2008 venne istituto il Centro di Eccellenza per la difesa informatica cooperativa della NATO (CCDEOE) a Tallin. [43]

Il Centro è essenzialmente un "think tank" militare che opera per la creazione di soluzioni di difesa informatica attraverso un'analisi multinazionale e interdisciplinare di vari

CamminoDiritto.it
ISSN 2421-7123

problemi informatici.

A partire dal 2018 il centro de quo è responsabile dell'identificazione e del coordinamento delle soluzioni di istruzione e formazione nella difesa informatica per tutti gli organismi della NATO in tutta l'Alleanza.

Oggi il CCDCOE comprende 25 Stati e altri sono in attesa di aderire, inclusi i Paesi partner della NATO Giappone e Australia. Il Centro è noto soprattutto per aver elaborato il Manuale di Tallinn, cui si è accennato poc'anzi.

Seppur non vincolante, è il più autorevole e completo del suo genere ed è continuamente sviluppato dal CCDCOE con il contributo di quasi 50 Stati.

Il caso dell'Estonia ha sicuramente dimostrato come nel XXI secolo i confini geografici non sono più da considerarsi un limite per gli Stati geograficamente più "piccoli" e ha evidenziato come il dominio del cyber space, seppur con le sue insidie portate a galla dall'attacco del 2007, con una volontà politica a lungo raggio, possa creare occasioni e opportunità di crescita al fine di ottenere uno status di "potenza" digitale.

6. Considerazioni conclusive e prospettive future della cyber-security.

Da tale disamina si è avuto modo di notare come, negli ultimi decenni, i casi di attacchi cyber sono aumentati considerevolmente al punto da rappresentare una vera e propria minaccia per la difesa di ciascuno stato.

Al fine di contenere e talvolta prevenire questi attacchi, a livello internazionale sono state portate avanti numerose iniziative volte talvolta ad una regolamentazione delle azioni lecite che possono essere effettuate nello spazio cibernetico. [44]

Tra le questioni più problematiche vi rientra sicuramente quella della difficoltà in ordine alla identificazione degli autori degli attacchi di volta in volta realizzati; talvolta, in secondo luogo, la veloce innovazione tecnologica che ha interessato il settore impone l'utilizzo di importanti e costanti investimenti nelle tecnologie dedicate al contrasto implicando pertanto l'utilizzo di personale qualificato. [45]

La necessità di dotare l'Alleanza atlantica di equipaggiamenti all'avanguardia tecnologica ha portato, già nel 2014, alla costituzione di specifiche partnership con le industrie del settore cibernetico. La cooperazione Nato-Ue ha inserito già nel 2016 la dimensione cyber

CamminoDiritto.it
ISSN 2421-7123

tra le aree prioritarie in cui collaborare.

L'analisi così prospettata, tra le politiche di governance in materia di cyber security, ha condotto alla individuazione di differenti approcci verso la difesa cibernetica e ci dimostra quanto ci sia ancora da "lavorare" nella realizzazione di regole e procedure uniformi e condivise.

Una prima importante differenza concerne proprio il tipo di politica adottato da questi paesi. E' possibile affermare che vi è una sostanziale divisione tra paesi che prevedono la possibilità di effettuare solo azioni di prevenzione o difesa, da altri che invece mirano a sviluppare la capacità di portare a termine operazioni offensive, anche in assenza di una vera e propria minaccia cibernetica.

Tra i paesi ove è possibile riscontrare una politica della deterrenza vi rientra sicuramente la Germania che intende la deterrenza cibernetica come la capacità di uno stato di rispondere adeguatamente e tempestivamente ad un attacco cyber realizzando il c.d. "hack-back".

È fondamentale sottolineare come, per la stessa Germania ed altri paesi che utilizzino questo tipo di politica, una governance di questo tipo mal si adatti alla necessaria velocità di reazione per limitare o evitare che si realizzino i danni di un attacco cibernetico.

Appare ovvio pensare che in un sistema come la Germania, ove si richiede in alcuni casi la preventiva approvazione parlamentare, ciò potrebbe causa l'incapacità dello Stato di proteggere i suoi interessi primari proprio in ragione della considerazione che servono azioni rapide e mirate.

Paesi come Inghilterra e la Francia, invece, sono tendenzialmente portati all'utilizzo di una politica diversa, appunto di matrice offensiva. [46]

Per quanto i paesi, anche all'interno della stessa Euro-zona, presentino tali sostanziali differenze, è possibile ugualmente procedere alla seguente schematizzazione delle esigenze condivise: la necessità di avere un quadro regolamentare a livello NATO ed internazionale; una migliore integrazione della componente cyber nelle strutture nazionali; una collaborazione meglio strutturata e più strategica con le imprese e con il mondo della ricerca; un maggior numero di investimenti nell'aggiornamento delle capacità legate al mondo cyber; un rafforzamento della formazione specialistica del personale volto alla protezione della minaccia cyber; ed una maggiore sensibilizzazione degli operatori all'interno delle strutture critiche essenziali ma più in genere della

CamminoDiritto.it
ISSN 2421-7123

popolazione, nell'utilizzo del cyber spazio.

Per quanto il 2023 e gli anni a venire serbano qualcosa che nessuno è in grado di prevedere, c'è da aspettarsi che le principali organizzazioni governative tenderanno alla realizzazione di migliori strategie di controllo di cloud; le identità e gli end-point saranno molto più al sicuro. Con il termine della pandemia, dalla durata di ben due anni, ci si prospettava un graduale ritorno alla normalità che di fatto non si è avuto a causa di tutte le conseguenze che il conflitto russo-ucraino ha portato con sé.

Nell'ambito della cyber sicurezza il recente conflitto ha determinato l'inizio della guerra cibernetica.

Si è già avuto modo di apprendere negli scorsi anni come le minacce più gravi e sofisticate sono state spesso realizzate da piccoli gruppi criminali, quindi tendenzialmente attacchi semplici seppure di grande impatto.

Gruppi sempre più numerosi di giovani hacker, rappresentanti della c.d. "criminalità disorganizzata", hanno creato numerosi danni riuscendo ad introdursi in decine di aziende ben strutturate e riconosciute sfruttando la rete di contatti aziendali.

Appare evidente come nel 2023 l'autenticazione a più fattori, la presenza di sessioni in rete di breve durata ed i privilegi di alcuni "account" fortemente ridimensionati devono assurgere a diventare la base dello standard della sicurezza aziendale.

Al pari si ritiene altresì che l'attività di monitoraggio debba svilupparsi nel senso di divenire più dettagliata, abbandonandosi l'idea di realizzare gruppi isolati cui vengono devolute tali funzioni.

Nel 2023 il mercato della cyber sicurezza deve sapersi adattare più che mai al modello di utilizzo dei prodotti di cyber security. Acquistare più prodotti dallo stesso "vendor" non appare più una soluzione prospettabile. Il futuro sembra prevedere un numero sempre maggiore di collaborazioni tra rivenditori, assicurandosi di convesso un maggior valore ed una maggiore affidabilità dei prodotti relativi allo stack della sicurezza. Altro aspetto da non sottovalutare concerne proprio il trattamento dei dati personali. [47]

Appare indiscutibile l'importanza dei dati, così come appare di tutta evidenza che tra normative varie, un aumento del richiesto livello di competenza degli analisti, un aumento degli attacchi informatici, questi dati siano sottoposti a rischi sempre maggiori; pertanto, si auspica la realizzazione di un sistema di "data retention" più semplice e funzionale. [48]

CamminoDiritto.it
ISSN 2421-7123

L'anno appena trascorso ci ha insegnato che nemmeno le più grandi organizzazioni (Microsoft, Samsung, Uber, etc.) sono immuni dagli attacchi cyber ed appare, a tal proposito, inverosimile ritenere che possa trattarsi semplicemente di giovani hacker riunitisi sulla rete.

Si ritiene piuttosto possa trattarsi di organizzazioni criminali informatiche sponsorizzate da specifici Stati o Nazioni; pertanto, l'approccio del c.d. "Zero Trust" si configura quale approccio migliore da adottarsi per gli anni a venire. [49]

Conclusivamente, alla luce di tale disamina è possibile auspicarsi che, in ragione della eccesiva imprevedibilità della minaccia cibernetica, i principali attori nazionali coinvolti si adoperino nel migliore dei modi al fine di garantire un'adeguata risposta a ciò che il futuro del cyber spazio ha in serbo; ed è proprio in tale ottica che il legislatore europeo sembra essersi mosso negli ultimi anni, attraverso la predisposizione di strumenti nel suo scacchiere, quali ad esempio la Direttiva NIS, la Direttiva nis-2 ed il Regolamento D.O.R.A., che sortiranno i primi effetti da qui a qualche anno.

CamminoDiritto.it
ISSN 2421-7123

Note e riferimenti bibliografici

[1] Per maggiori informazioni, si consulti il seguente documento in lingua inglese {https/URL}

[2] Stuxnet è un virus informatico che qualcuno suppone creato e diffuso dal governo statunitense seppure mai confermato (nell'ambito dell'operazione "Giochi Olimpici" che consisteva in un'"ondata" di "attacchi digitali" contro l'Iran[3]) in collaborazione col governo israeliano. Lo scopo del software era il sabotaggio dell'impianto di arricchimento di Natanz. In particolare, il virus doveva disabilitare le centrifughe dell'impianto impedendo la rilevazione dei malfunzionamenti e della presenza del virus stesso. Nel documentario diretto da Alex Gibney, Zero Days, viene per la prima volta rivelato che il virus Stuxnet faceva parte di un progetto ben più ampio di attacchi informatici a obiettivi sensibili presenti in Iran (chiamato "Nitro Zeus"). Stuxnet colpiva i PLC componenti hardware programmabili via software fondamentali per l'automazione degli impianti, in particolare quelli adibiti al controllo delle centrifughe (utilizzate per separare materiali nucleari come l'uranio arricchito). La caratteristica che ha colpito gli esperti fin dall'inizio fu il livello di sofisticatezza di questo software che dimostrava che chi aveva scritto il programma conosceva fin nei dettagli l'ambiente informatico in uso nell'impianto. Questo malware fra l'altro faceva leva su quattro vulnerabilità di Windows ancora inedite (0-day) all'epoca per poi propagarsi verso il software Step7 della Siemens, informazioni che secondo alcuni specialisti del settore varrebbero sul mercato nero almeno un quarto di milione di dollari ciascuna. In seguito all'infezione del virus nel centro di arricchimento il programma si è diffuso al di fuori dello stabilimento (tramite un PC portatile infetto) a causa di un errore di programmazione presente nel virus stesso dato che Stuxnet poteva essere eseguito anche su più sistemi dotati di sistema SCADA e PLC, colpendo principalmente le aziende (e quindi anche le relative nazioni tra cui il Giappone, gli USA ed in Europa)) da cui provenivano le attrezzature per il programma atomico iraniano venendo così scoperto e finendo poi sotto i riflettori dei media di tutto il mondo. L'architettura di Stuxnet è estremamente complessa ma in estrema sintesi il virus è composto da tre grandi moduli: un worm che danneggia i PLC e permette al software di autoreplicarsi su altre macchine, un collegamento che mette in esecuzione le copie create dal worm e un rootkit che nasconde il virus rendendolo non individuabile. L'inizio del contagio da parte di Stuxnet è probabilmente avvenuto all'interno del sistema industriale stesso tramite una chiavetta USB infetta in mano a un ignaro ingegnere iraniano: il virus si è poi propagato in rete cercando il software industriale Step7 (realizzato dalla Siemens per controllare i PLC dell'impianto), modificandone il codice in modo da danneggiare il sistema facendo credere all'operatore che tutto funzionasse correttamente.

[3] Sulla base dei pilastri prima considerati è possibile affermare che le attuali 15 Cyber-strategie attualmente già formalizzate dai paesi dell'eurozona basano il loro pensiero strategico principalmente sui seguenti elementi: Creazione di regole comuni; Sviluppo dei rapporti diplomatici nell'ottica del rafforzamento e creazione di partnership internazionali; creazione e rafforzamento di un sistema di information sharing e incident response; creare figure professionali ad hoc ed infine aumentare la consapevolezza dei cittadini sul cyber spazio;

[4] Si consulti per ulteriori informazioni, il seguente documento in lingua

{https/URL}

[5] Per far fronte all'incombente minaccia, che ha registrato una crescita del 782% tra il 2006 ed il 2012, il governo degli USA si è impegnato nel tempo, al fine di delineare e dare attuazione ad una serie di documenti strategici operativi, con la finalità principale di fissare principi cardine dell'azione del governo in materia di cyber sicurezza; costituire specifiche strutture governative, nonché definire ruoli e responsabilità all'interno di queste strutture per fronteggiare la minaccia;

[6] Il Dipartimento per la sicurezza interna degli Stati Uniti (DHS) è il dipartimento esecutivo federale degli Stati Uniti responsabile della sicurezza pubblica , più o meno paragonabile ai ministeri degli interni o degli interni di altri paesi. Le sue missioni dichiarate riguardano l'antiterrorismo , la sicurezza delle frontiere , l'immigrazione e le dogane, la sicurezza informatica e la prevenzione e la gestione dei disastri. Ha iniziato ad operare nel 2003, formatosi a seguito dell'Homeland Security Act del 2002 emanato in risposta agli attacchi dell'11 settembre . Con

CamminoDiritto.it
ISSN 2421-7123

oltre 240.000 dipendenti, il DHS è il terzo dipartimento di gabinetto più grande dopo i dipartimenti della difesa e degli affari dei veterani . La politica di sicurezza interna è coordinata alla Casa Bianca dall'Homeland Security Council . Altre agenzie con importanti responsabilità in materia di sicurezza nazionale includono i Dipartimenti della Salute e dei Servizi Umani , della Giustizia e dell'Energia .

[7] Appare opportuno che il documento strategico definisca con chiarezza ed in modo univoco: i costi e le risorse necessarie per una sua attuazione concreta; i ruoli e le responsabilità assegnati a ciascun attore nella gestione della minaccia; la metodica attraverso la quale valutare i risultati raggiunti nell'implementazione della nuova strategia; la priorità ed il posizionamento di una nuova strategia all'interno del quadro strategico americano e l'eventuale suo collegamento, in chiave di raccordo, con gli altri documenti;

[8] Come già noto, per far fronte alle continue incursioni il Governo italiano, con il D.L. 14 giugno 2021, ha istituto l'A.C.N. con il compito di tutelare i nostri interessi nel mondo cibernetico. Il compito dell'agenzia è quello di implementare la strategia nazionale in tema di cybersecurity e perseguire il conseguimento dell'autonomia di questa, anche tramite collaborazioni con ambienti di ricerca o comunque universitari; parallelamente la stessa sarà tenuta allo sviluppo di forti linee di partenariato con i principali paesi europei al fine di arrivare ad una condivisione delle strategie relative al cyberspazio. Gli enti privati, in particolare, rivestono un ruolo molto importante in questa lotta, atteso che sono direttamente interessati dall'odierna rivoluzione digitale ed atteso che il settore privato è forse il settore più frequentemente bersagliato da questi attacchi di matrice cibernetica;

[9] Volendo prospettare una stima totale degli attacchi subiti e dei rispettivi destinatari è possibile affermare che il 35% degli attacchi ha avuto ad oggetto due settori nevralgici quali la P.A. e la sanità; il resto degli attacchi ha avuto ad oggetto imprese del settore manifatturiero ed a seguire quello finanziario. Non sono state risparmiate in assoluto neanche le società "I.C.T.", providers di servizi digitali e gli E-commerce. Il settore pubblico per antonomasia è il bersaglio principale; da considerarsi, in subordine, la crescente importanza del privato. Nel 2021 gli attacchi critici a livello mondiale sono stati circa il 32% di tutti gli attacchi realizzati. Il 47% di questi ha rasentato un alto livello di pericolosità. Per quel che concerne le principali tecniche di attacco i malware rappresentano lo strumento più utilizzato.

[10] Si consulti per maggiori approfondimenti il documento di cui al sito seguente: {https/URL}

[11] Il quarto Libro Bianco dal 1972 riduce ulteriormente la Difesa francese dopo la cura dimagrante imposta nel 2008 dalla riforma varata da Nicolas Sarkozy che ha tagliato 54 mila unità tra il 2009 e il 2015, dei quali 45 mila già attuati. Nei prossimi anni verranno ridotti gli effettivi di altre 23.500 unità entro il 2019, cioè oltre il 10 per cento dei militari in servizio, quest'anno 218 mila più 67 mila civili. Le Forze Terrestri perderanno 7 mila effettivi e una delle 8 brigate che compongono la Forza Operativa (73 mila unità in riduzione a 66mila) rinunciando anche a 50 dei 250 carri amati Leclerc. La "Force de frappe", l'arsenale nucleare, non verrà ridimensionato. Le Forze Aeree vedranno ridotti i jet da combattimento (i Rafale saranno in tutto 225 invece di 286), limitati a 50 i velivoli cargo e tagliati da 140 a 115 gli elicotteri multiruolo (ma arriveranno i velivoli teleguidati statunitensi) mentre la Marina non subirà decurtazioni. Si tratta di un serio ridimensionamento delle ambizioni militari che dimezza la forza impiegabile in un conflitto prolungato per almeno un anno da 30 mila a 15 mila unità (ma con un preavviso di sei mesi) e da 70 a 45 aerei da combattimento pur mantenendo una forza di 7 mila uomini di pronto impiego dispiegabili in tre diversi teatri operativi. Parigi manterrà la capacità di inviare 2.300 militari a 3 mila chilometri in una settimana. Rispetto al Libro Bianco 2008, che ridimensionava la presenza francese in Africa, il documento dell'amministrazione Hollande rimette il Continente Nero al centro degli interessi strategici francesi anche in virtù delle crisi in Libia, Malì e Costa d'Avorio. In Africa i francesi schierano stabilmente circa 5 mila militari a un costo di 400 milioni di euro annui. Secondo il commento del quotidiano Le Monde la Francia assillata dal cruccio del deficit" prepara le guerre di domani con ambizioni ridotte", e pur senza voler ridimensionare il proprio status di media potenza si trova costretta ad" essere realista sui propri mezzi". L'idea di fondo, spiega ancora il giornale, è di snellire alcuni ambiti ma mantenere comunque la presenza in tutti i campi, dallo spazio all'armamento pesante, e tutelare i programmi di sviluppo con prospettive di crescita a lungo termine. Un'impostazione ben più morbida di quella auspicata dal ministero dell'Economia che ha fatto tirare un sospiro di sollievo al ministro della Difesa, Jean-Yves Le Drian, capace di scongiurare una riduzione del budget del settore, almeno per il momento.

[12] L' Agenzia Nazionale per la Sicurezza dei Sistemi Informativi (ANSSI) è un servizio francese creato con decreto nluglio 2009 . Questo servizio di competenza nazionale è annesso al Segretariato Generale per la Difesa e la

CamminoDiritto.it
ISSN 2421-7123

Sicurezza Nazionale (SGDSN), l'autorità incaricata di assistere il Presidente del Consiglio dei Ministri nell'esercizio delle sue responsabilità in materia di difesa e sicurezza nazionale. L'ANSSI sostituisce il Dipartimento centrale per la sicurezza dei sistemi informativi , istituito con decreto luglio 2001. Il suo budget ammonta a 136 milioni di euro, di cui 30 milioni di euro dedicati al libro paga nel 2014 e alla sua forza lavoro, a 350 persone nel 2013, 500 agenti a fine 2015 e un obiettivo di 600 agenti a fine 2017. In definitiva è prevista una forza lavoro di 750 agenti. Vincent Strubel, ingegnere minerario generale, è stato nominato direttore generale dell'ANSSI il 4 gennaio 2023, succedendo a Guillaume Poupard .

[13] Nell'ottobre 2015 è stata annunciata la Strategia nazionale per la sicurezza digitale (Stratégie nationale pour la sécurité du numérique), diretta a sostenere la transizione digitale della società francese. La Strategia è caratterizzata da cinque obiettivi: garantire la sovranità della Francia e assicurare la sicurezza delle sue infrastrutture critiche nel caso di un grande attacco informatico. Questo obiettivo è perseguito rafforzando le capacità scientifiche, tecniche e industriali necessarie e la sicurezza delle infrastrutture vitali; proteggere i cittadini e le imprese e combattere la criminalità informatica. In questa direzione è promosso il percorso "identité numérique" allo scopo di rafforzare la fiducia degli utenti nella loro vita digitale, limitando il rischio di uno sfruttamento indesiderato dei loro dati, e creare altresì un dispositivo nazionale di assistenza alle vittime di atti di cyber-violenza; sensibilizzare i ragazzi sulla sicurezza digitale e sui comportamenti responsabili nel cyberspazio a partire dall'età scolastica. Anche l'istruzione superiore e la formazione continua devono comprendere una sezione dedicata alla sécurité numérique; Sviluppare un ecosistema favorevole alla ricerca e all'innovazione e rendere la sicurezza digitale un fattore di competitività. La Francia sostiene lo sviluppo dell'economia e la promozione internazionale dei suoi prodotti e servizi digitali e garantisce la disponibilità di prodotti e servizi digitali con livelli di fiducia e sicurezza adeguati agli usi e alle minacce informatiche; promuovere la cooperazione con gli Stati membri volontari in modo da favorire un'autonomia strategica digitale europea (Autonomie stratégique numérique européenne), giocando un ruolo attivo nella promozione di un cyberspazio sicuro, stabile e aperto.

[14] Istituito sotto l'egida dell'ANSSI, lo scopo di questo osservatorio è quello di migliorare la conoscenza di Internet francese studiando le tecnologie fondamentali per il suo corretto funzionamento. Fino a poco tempo fa, nonostante l'importanza data a questo tema, non esisteva un organismo deputato a studiare i rischi di fallimento di Internet a livello nazionale. A livello tecnico, la resilienza e la solidità di Internet possono essere caratterizzate da una serie di indicatori tecnici misurabili. Alcuni di questi sono presi direttamente dalle regole ingegneristiche chiamate best practice, cioè, definite dalla comunità. Uno degli obiettivi dell'osservatorio è aumentare la comprensione collettiva dell'Internet francese per arrivare a una visione coerente e il più completa possibile. Ciò consentirà di identificare le interazioni e le dipendenze tra i vari attori interessati. La missione dell'Osservatorio francese sulla resilienza di Internet è anche quella di identificare e misurare indicatori di resilienza rilevanti e rappresentativi e di rendere pubblici i loro risultati. Inoltre, coinvolge gli attori Internet francesi nelle sue attività al fine di aumentarne l'efficacia e incoraggiare la piena adozione delle migliori pratiche.

[15] Si veda per maggiori approfondimenti www.altalex.com

[16] Il BSI è stato fondato nel 1991 con la legge sull'Ufficio federale per la sicurezza informatica (BSIG) ed è nato dall'Ufficio centrale per la sicurezza informatica (ZSI). La sua autorità precedente era il Central Office for Ciphering (ZfCh) che era affiliato al Federal Intelligence Service (BND) . Il matematico Otto Leiberich , al Servizio segreto federale dal 1957 e lì da ultimo a capo dello ZfCh e dal 1° giugno 1989 ZSI, è stato il primo presidente del BSI. Dopo la partenza di Otto Leiberich, Dirk Henze è stato nominato nuovo presidente di BSI con effetto dal 1° gennaio 1993. Gli successe Udo Helmbrecht nel marzo 2003. Successivamente Michael Hange è entrato in carica come presidente il 16 ottobre 2009 e si è ritirato l'11 dicembre 2015. Dal 18 febbraio 2016 al 18 ottobre 2022, l'ex presidente dell'organizzazione di lobby legata alla Russia Cyber-Sicherheitsrat Deutschland e. V. Arne Schönbohm l'autorità. L' ufficio è classificato nel gruppo salariale B 8 della scala salariale federale B. Porta il titolo ufficiale di Presidente. Nel periodo precedente alla sua nomina, la sua nomina è stata criticata. Claudia Plattner è Presidente del BSI dal 1° luglio 2023. A metà del 2017 il BSI ha istituito un centro di competenza per raggruppare le attività del BSI nel campo dell'intelligenza artificiale e dell'apprendimento automatico. Dopo l'accordo di coalizione delle parti nel governo federale nel febbraio 2018 l'area di competenza dell'Ufficio federale è stata ampliata. Ha rilevato la consulenza per le piccole e medie imprese ed è stata ampliata come autorità nazionale per la sicurezza informatica. Ciò include la certificazione centrale e la standardizzazione

CamminoDiritto.it
ISSN 2421-7123

per la sicurezza informatica e informatica. Inoltre, il BSI riceve compiti aggiuntivi nell'area della protezione dei consumatori digitali. Per la cooperazione con gli stati federali il BSI ha istituito un sistema di collegamento nazionale con contatti nelle città di Amburgo, Wiesbaden, Bonn, Stoccarda, Berlino e Dresda. Nel 2017 BSI ha istituito un ufficio di collegamento a Wiesbaden. Il 5 febbraio 2019 il BSI ha aperto ad Amburgo un ufficio di collegamento per la regione settentrionale. Con la sua presenza ad Amburgo l'autorità per la sicurezza informatica sta ampliando la sua gamma di informazioni e supporto per aziende, autorità, comuni e altre istituzioni nel nord della Germania. L'ufficio di collegamento funge da punto di contatto per autorità, aziende e altre istituzioni negli stati federali di Brema, Amburgo, Meclemburgo-Pomerania occidentale, Bassa Sassonia, Sassonia-Anhalt e Schleswig-Holstein per questioni relative al BSI e al tema della sicurezza informatica. Da dicembre 2019 esiste un secondo ufficio per 200 dipendenti a Freital vicino a Dresda. Ciò dovrebbe migliorare l'accessibilità delle VdB. Nello stesso anno il Comitato del bilancio del Bundestag tedesco ha deciso di istituire un'altra filiale a Saarbrücken con 30 posti. Nel settembre 2022, BSI ha annunciato l'introduzione di un'etichetta di sicurezza IT per la maggior parte dei prodotti IoT e smart home. Da allora le aziende possono richiederlo al BSI che presenta le proprietà di sicurezza dei prodotti in un modo facilmente comprensibile per i consumatori.

[17] Con la firma da parte del Presidente federale e la pubblicazione nella **Gazzetta ufficiale federale** : è entrata in vigore la seconda legge sull'aumento della sicurezza dei sistemi informatici (legge tedesca sulla sicurezza informatica 2.0). Il Consiglio federale ha approvato la legge il 7 maggio 2021. La legge era stata approvata dal Bundestag tedesco il 23 aprile 2021. Il BSI ha così acquisito nuove competenze che rafforzano notevolmente la sua attività di autorità federale per la sicurezza informatica. Il German IT Security Act 2.0 rafforza il BSI nelle seguenti aree: **Rilevamento e difesa:** il BSI ha ricevuto maggiori autorità nel rilevamento delle vulnerabilità della sicurezza e nella difesa dagli attacchi informatici. In qualità di principale centro di competenza della Germania per la sicurezza delle informazioni, il BSI può quindi plasmare la digitalizzazione sicura e, tra le altre cose, stabilire standard minimi vincolanti per le autorità federali e monitorarli in modo più efficace; **Sicurezza informatica nelle reti mobili:** la legge contiene un regolamento sul divieto dell'uso di componenti critici per proteggere l'ordine pubblico o la sicurezza in Germania. Gli operatori di rete devono inoltre soddisfare specifici requisiti di sicurezza di alto livello e i componenti critici devono essere certificati. Tra le altre cose, la legge garantisce la sicurezza delle informazioni nelle reti mobili 5G; **Protezione dei consumatori:** il BSI diventerà l'organo consultivo indipendente e neutrale per i consumatori in materia di sicurezza informatica a livello federale. Ciò significa che la protezione dei consumatori è ora una funzione del BSI. L'introduzione dell'IT Security Mark uniforme per i cittadini ha lo scopo di rendere la sicurezza informatica più trasparente in futuro e di chiarire quali prodotti sono già conformi a specifici standard di sicurezza informatica; **Sicurezza per le imprese:** le infrastrutture critiche sono state ampliate per includere il settore della gestione dei rifiuti urbani. Inoltre, anche altre società di particolare interesse pubblico (ad esempio, produttori di armi o società di particolare importanza economica) dovranno implementare in futuro determinate misure di sicurezza informatica e saranno incluse negli scambi di informazioni riservate con BSI; **Autorità nazionale di certificazione della sicurezza informatica:** ai sensi dell'articolo 9a (1), il BSI è l'autorità nazionale di certificazione della sicurezza informatica (NCCA) ai sensi dell'articolo 58, paragrafo 1, del regolamento (UE) 2019/881, noto anche come legge sulla sicurezza informatica (CSA). L'NCCA è responsabile in particolare della supervisione e dell'applicazione delle norme nell'ambito dei sistemi europei di certificazione della sicurezza informatica. Le attività di vigilanza e certificazione devono essere mantenute rigorosamente discrete e svolte in autonomia. Per loro stessa natura, la sicurezza delle informazioni e la digitalizzazione vanno di pari passo. Sono due facce della stessa medaglia, e del BSI. Con il German IT Security Act 2.0 il Bundestag tedesco e il Consiglio federale hanno completato un aggiornamento chiaro e urgente della sicurezza delle informazioni in Germania. Affinché la transizione digitale abbia successo in modo sicuro il BSI deve funzionare come una forte autorità federale per la sicurezza informatica. Fornire consigli, informazioni e avvertimenti diventerà sempre più importante in futuro.

[18] Oltre alle minacce di natura meramente militare vi si includono anche gli attacchi informatici o possibili attacchi alle infrastrutture critiche. La nuova strategia, soprattutto a seguito del recente conflitto bellico che ha interessato Russia e Ucraina, mira ad assurgere a vero e proprio punto di svolta storico cercando di garantire quella sicurezza politica ed economica di cui il paese necessita.

[19] Per quel che concerne la capacità di difesa si mira ad una spesa nel limite massimo di almeno il 2% del PIL interno per questioni di cyber sicurezza, obiettivo che fin ora non è stato raggiunto nonostante i precedenti impegni presi dal paese con la NATO. Si specifica che il raggiungimento di questo obiettivo sarà graduale e pluriannuale predisponendosi almeno nella fase iniziale uno speciale fondo per la “Bunderswehr” e ricavandosi il restante, per il tramite dell’adozione di una sostanziale politica del risparmio delle finanze pubbliche, senza che ciò vada fortemente ad impattare sul bilancio federale complessivo. Il documento pone altresì la sua attenzione

sull'ampliamento delle capacità in campo militare nell'area della cybersecurity e del cyber spazio, predisponendosi al contempo un rafforzamento dell'industria europea degli armamenti. Il secondo asse, quello della resilienza, pone l'attenzione su una più efficace protezione delle infrastrutture critiche. Si specifica che alcune aree, come quella del trasporto, della sanità, delle energie, devono essere al meglio protette dai rischi informatici. Il testo afferma che il B.S.I. deve essere ampliato, così come le riserve nazionali nei principali settori di cui si è sopra parlato. Con riguardo all'ultimo aspetto della strategia, quello della "Sostenibilità", sembra che il documento vi attribuisca un rilievo minore rispetto agli altri due elementi;

[20] L'hack-back consiste in una strategia di cybersicurezza adottata da alcuni paesi, tra i quali ritroviamo la Germania, in virtù della quale si mira ad una offensiva, dunque a dei veri e propri attacchi informatici in chiave difensiva, talvolta anche in assenza di specifici attacchi ad opera di nemici, La Germania teme possibili azioni di cyber warfare contro le sue infrastrutture critiche. Lo ha affermato il capo del servizio d'intelligence interno tedesco (BfV) Hans-Georg Maaßen, in un'intervista all'emittente RBB. A riguardo ha sottolineato che il paese europeo dovrebbe essere pronto con misure antisabotaggio. "Ciò significa che dovremmo implementare malware in tutte le nostre infrastrutture critiche – ha aggiunto -. In modo, poi, da poterlo attivare in un momento X, se dovesse sorgere una disputa politica". A sostegno della sua tesi, il direttore della BfV ha ricordato l'attacco cibernetico a una centrale elettrica ucraina nel dicembre 2015 spiegando che i cyber aggressori aveva tentato un'aggressione alla Germania nello stesso periodo. Perciò anche se tutte le autorità delle infrastrutture critiche sono consapevoli della minaccia, non si possono escludere azioni future. "Perché molto, se non quasi tutto – ha proseguito – è connesso oggi a Internet". Il direttore della BfV Maaßen: Serve un quadro legale che autorizzi l'hack-back. Obiettivo: cancellare i dati prima che cadano nelle mani di hacker ostili, Infine, Maaßen ha ribadito la sua richiesta di un quadro legale in Germania per il cosiddetto hack-back, l'hacking di ritorno contro azioni di cyber warfare. Questo consentirebbe a una vittima innanzitutto di identificare i presunti hacker responsabili dell'aggressione informatica, poi di prendere contromisure e recuperare o distruggere i dati rubati. "Quando vediamo i dati che scorrono dai computer tedeschi dobbiamo assicurarci che vengano cancellati prima ancora di raggiungere l'hacker – ha concluso -. Questo è un obiettivo importante che vogliamo raggiungere".

[21] Nel documento, oltretutto, la Russia viene ad oggi considerata come la più grande minaccia per la pace e alla sicurezza nella regione euro-atlantica per il prossimo futuro partendosi dall'innesto generato dal conflitto in Ucraina. Molto particolare la presa di posizione, nel documento in relazione alla Cina. Quest'ultima nazione è vista come un partner più che una concorrente e/o rivale di sistema. In definitiva, la strategia pur gettando le basi per una tendenziale spinta del governo tedesco verso la sfida digitale, appare comunque lacunosa sono diverse questioni che appaiono centrali in questo preciso momento storico

[22] Si consulti per maggiori informazioni il seguente documento in lingua {https/URL}

[23] Nell'agosto 2010 l'allora segretario alla Difesa , Liam Fox , ha chiesto a Lord Levene , ex capo degli appalti della difesa , di presiedere il gruppo direttivo per la riforma della difesa. Il compito del gruppo era quello di rivedere in modo indipendente la difesa e la struttura e la gestione del Ministero della Difesa . Il gruppo ha riferito nel giugno 2011, con una raccomandazione chiave che prevedeva la creazione di un Joint Forces Command (JFC) per gestire e fornire specifiche capacità congiunte e per assumere un ruolo guida nello sviluppo di una guerra congiunta, imparando dalle lezioni e dalla sperimentazione per consigliare su come i militari dovrebbero condurre operazioni congiunte in futuro. Il rapporto sulla riforma della difesa ha anche formulato le seguenti raccomandazioni: Il Joint Forces Command dovrebbe essere guidato da un ufficiale militare a quattro stelle che avrebbe la responsabilità di comandare e generare le capacità congiunte assegnate al comando e stabilire il quadro per gli abilitatori congiunti che risiedono nei singoli servizi. Un certo numero di organizzazioni militari attualmente gestite centralmente all'interno del MOD dovrebbero passare al Joint Forces Command, tra cui il Directorate Special Forces , l' Accademia della Difesa e il Development Concepts and Doctrine Center . Il quartier generale congiunto permanente (PJHQ) dovrebbe risiedere all'interno del comando interforze, ma riferire per scopi operativi direttamente al capo di stato maggiore della difesa . Nell'attuare il Joint Forces Command, il MOD dovrebbe esaminare in dettaglio le capacità e le funzioni congiunte o potenzialmente congiunte tra i servizi armati (Royal Navy , Army e Royal Air Force), per determinare quali potrebbero essere razionalizzate, il vantaggio di ulteriori organizzazioni congiunte, quali organizzazioni dovrebbero trasferire al Joint Forces Command e quali dovrebbero essere trasferite a un servizio principale;

[24] La National Security Strategy and Strategic Defense and Security Review 2015 è stata pubblicata dal governo britannico durante il secondo ministero Cameron il 23 novembre 2015 per delineare la strategia di difesa del Regno Unito fino al 2025. Ha identificato le principali minacce per il Regno Unito e le capacità necessarie per affrontarle. Il National Security Risk Assessment 2015 ha rilevato che le minacce affrontate dal Regno Unito, compresi i suoi territori d'oltremare e gli interessi d'oltremare, sono "aumentate in scala, diversità e complessità" dal 2010. Ha

CamminoDiritto.it
ISSN 2421-7123

evidenziato quattro minacce particolari che potrebbero essere le priorità per la sicurezza del Regno Unito nel prossimo decennio: La crescente minaccia rappresentata dal terrorismo, dall'estremismo e dall'instabilità. La recrudescenza delle minacce statali; e intensificando la concorrenza statale più ampia. L'impatto della tecnologia, in particolare le minacce informatiche; e più ampi sviluppi tecnologici. L'erosione dell'ordine internazionale basato su regole, che rende più difficile creare consenso e affrontare le minacce globali.

[25] Secondo la revisione effettuata dal National Accounting Office l'obiettivo della ACD è tra i pochi obiettivi che al febbraio 2019 erano stati implementati fino a quel momento senza subire ritardi. Per maggiori informazioni si veda National Audit Office, Progress of the 2016–2021 National Cyber Security Programme, HC1988, session 2017-2019, marzo 2019, {https/URL}

[26] Il Royal United Services Institute (RUSI , Rusi) è un think tank per la difesa e la sicurezza con sede a Londra , nel Regno Unito. Fu fondata nel 1831 dal duca di Wellington, Sir Arthur Wellesley . L'istituto è stato registrato come Royal United Service Institute for Defence and Security Studies e precedentemente noto come Royal United Services Institute for Defence Studies. L'attuale presidente della RUSI è il duca di Kent e il suo direttore generale è Karin von Hippel . RUSI è stata fondata nel 1831, diventando così il più antico think tank di difesa e sicurezza del mondo su iniziativa del Duca di Wellington . Il suo obiettivo originale era studiare la scienza navale e militare. Il duca di Wellington ha guidato l'istituzione della RUSI in una lettera allo United Service Journal di Colbourn sostenendo che dovrebbe essere formato "un Museo dei servizi uniti" gestito interamente da ufficiali navali e militari e sotto il patrocinio del monarca, allora re Giorgio IV , e dei comandanti in capo delle forze armate. Una simile istituzione dimostrerebbe che le due professioni sono entrate negli elenchi della scienza e sono pronte a contendersi gli onori tam Artibus quam Armis («tanto con le arti quanto con le armi»). Successivamente il comandante Henry Downes, Royal Navy, riunì un gruppo con l'obiettivo di formare un comitato d'azione al quale il primo ADC di King George fu incaricato di trasmettere "la cortese e alta approvazione di Sua Maestà dell'impresa e dei principi su cui si propone di condurla", che sono stati dichiarati adatti a "una società strettamente scientifica e professionale, e non un club". La morte del re ritardò le cose ma il duca di Clarence espresse la sua disponibilità a diventare un mecenate così, incoraggiato dal potente sostegno del duca di Wellington, il primo aiutante di campo , Sir Herbert Taylor , ripresenta il progetto a Guglielmo IV(l'ex duca di Clarence), e ha potuto assicurare al comitato che "poteva procedere sotto i graziosi auspici di Sua Maestà". Il 25 giugno 1831 il comitato si riunì. La presidenza fu assunta dal maggiore generale Sir Howard Douglas , nella sua persona un simbolo dello "United Service": un soldato che era il massimo esperto di artiglieria navale. La decisione di istituire l'istituzione fu presa dal futuro feldmaresciallo visconte Hardinge e appoggiata dal futuro contrammiraglio Sir Francis Beaufort , il famoso idrografo. Il primo nome adottato fu il Museo Navale e Militare: questo fu modificato nel 1839 in United Service Institution e nel 1860 in Royal United Service Institution da un atto costitutivo reale . Nel 2004 il nome è stato cambiato in theRoyal United Services Institute for Defence and Security Studies. I borsisti della RUSI possono utilizzare l'abbreviazione post-nominale di cinque lettere, FRUSI

[27] I **Cinque Occhi** (Five Eyes in inglese, acronimo: **FVEY**) è un'alleanza di sorveglianza che comprende Australia, Canada, Nuova Zelanda, Regno Unito e Stati Uniti. Questi paesi fanno parte dell'accordo UKUSA, un trattato di cooperazione congiunta in materia di intelligence dei segnali. Le sue origini possono essere fatte risalire al periodo successivo alla Seconda Guerra Mondiale, quando gli Alleati sottoscrissero la Carta Atlantica con l'intento di definire i loro obiettivi per un mondo postbellico. Nel corso della guerra fredda, FVEY sviluppò il sistema di sorveglianza ECHELON per monitorare le comunicazioni dell'ex Unione Sovietica e del blocco orientale divenuto poi un mezzo per monitorare le comunicazioni private in tutto il mondo. Alla fine degli anni '90 il disvelamento pubblico dell'esistenza di ECHELON innescò un grande dibattito in seno al Parlamento europeo e, in misura minore, al Congresso degli Stati Uniti. I Cinque Occhi hanno ulteriormente ampliato le proprie capacità di sorveglianza nel corso della "guerra al terrore", ponendo molta enfasi sul monitoraggio del World Wide Web. L'ex consulente della NSA Edward Snowden ha descritto i **Cinque Occhi** come "un'organizzazione di intelligence sovranazionale che non risponde alle leggi conosciute dei propri paesi". I documenti fatti trapelare da Snowden nel 2013 hanno rivelato che i Cinque Occhi hanno spiato persone e condiviso le informazioni raccolte al fine di eludere le normative nazionali restrittive sulla sorveglianza dei cittadini. Nonostante le continue polemiche sui suoi metodi l'alleanza dei Cinque Occhi rimane una più complete coalizioni di spionaggio della storia.

[28] Si veda per maggiori approfondimenti www.altalex.com

[29]Si consulti

{https/URL}

CamminoDiritto.it
ISSN 2421-7123

[30] L'articolo 5 è il più famoso del Trattato Nord Atlantico, perché è quello che stabilisce che:

"Le parti convengono che un attacco armato contro una o più di esse in Europa o nell'America settentrionale sarà considerato come un attacco diretto contro tutte le parti". Questo significa, nella sua forma più semplice, che tutti gli alleati sono obbligati a soccorrere uno stato membro che sia stato attaccato. In realtà però l'articolo 5 è molto più lungo di così, e pone tutta una serie di condizioni e cautele, alcune delle quali sono poi specificate e descritte successivamente, nell'articolo 6. Non c'è nessun automatismo nell'articolo 5 del trattato NATO, e anzi è previsto che gli stati membri valutino con attenzione la natura dell'«attacco armato» e decidano di conseguenza quale sia la migliore «azione» da intraprendere in risposta. Ciò significa che l'articolo 5 non prevede necessariamente una risposta di tipo militare ma che tutto dipende dalle circostanze e dalla valutazione degli alleati. Quando viene invocato l'articolo 5, gli alleati tendenzialmente devono verificare che quello che è avvenuto sia effettivamente un attacco armato contro un paese alleato e sia effettivamente un attacco ostile e poi decidere la risposta da dare, se militare o di altro tipo. Secondo l'articolo 5 gli stati possono agire anche «individualmente» in difesa di un alleato attaccato ma ogni risposta da parte della NATO nel suo complesso deve essere decisa dal Consiglio Nord Atlantico. Su come dovrebbero essere prese queste decisioni ci sono alcune incertezze anche tra gli esperti legali. La stessa NATO, sia sul suo sito sia sui suoi documenti ufficiali, parla indifferentemente di «unanimità» (una decisione viene presa con l'accordo positivo di tutte le parti) o di «consenso» (una decisione viene presa anche se alcune delle parti sono neutrali, o hanno delle rimostranze ma non le esprimono con un'esplicita posizione contraria). Altrove si legge che le decisioni sono prese sulla base di una posizione che sia «accettabile per tutti» e che alcuni membri possono «accettare di non essere d'accordo». Non è chiaro, però, cosa succederebbe se un paese decidesse di mettere un veto deciso e netto. Il punto è che finora questo non è mai successo: in circa 70 anni di storia della NATO le decisioni sono sempre state prese senza eccezionali controversie e praticamente sempre all'unanimità, o comunque senza eccessive contrarietà. La NATO non si è mai trovata a dover prendere decisioni estremamente gravi come potrebbe essere un intervento militare contro la Russia, e anche per questo non è del tutto chiaro cosa succederebbe in circostanze del genere.

Finora l'articolo 5 del trattato è stato invocato una volta sola dagli Stati Uniti a seguito dell'attacco terroristico dell'11 settembre 2001 contro New York e Washington la cui risposta fu l'invasione dell'Afghanistan per rovesciare il regime dei talebani, accusati di dare rifugio ad al Qaida, organizzazione responsabile degli attentati. Questa singola occasione mostra piuttosto chiaramente come l'attivazione dell'articolo 5 non soltanto sia oggetto di consultazioni e deliberazioni, ma anche che queste deliberazioni richiedono un certo tempo.

[31] In realtà nel Regno Unito già il vertice dei capi di stato e di governo del 2008 aveva adottato una prima Policy on Cyber Defence che ha compiuto un salto in avanti nel summit del 2014 con la Enhanced Nato Policy on Cyber Defence;

[32] Si veda per maggiori informazioni {https/URL}

[33]Si veda per maggiori informazioni {https/URL}

[34] Si consulti il seguente documento per maggiori informazioni {https/URL}

[35] Un centro operativo di sicurezza (SOC) è responsabile della protezione di un'organizzazione dalle minacce informatiche. Gli analisti SOC eseguono il monitoraggio 24 ore su 24 della rete di un'organizzazione e indagano su eventuali potenziali incidenti di sicurezza. Se viene rilevato un attacco informatico gli analisti SOC sono responsabili di adottare tutte le misure necessarie per porvi rimedio. Comprende i tre elementi costitutivi per la gestione e il miglioramento della posizione di sicurezza di un'organizzazione: persone, processi e tecnologia. In tal modo la governance e la conformità forniscono un quadro, legando insieme questi elementi costitutivi. Un SOC all'interno di un edificio o di una struttura è una posizione centrale da cui il personale supervisiona il sito utilizzando la tecnologia di elaborazione dei dati. In genere un SOC è attrezzato per il monitoraggio degli accessi e il controllo dell'illuminazione, degli allarmi e delle barriere dei veicoli.

[36] Il comando alleato per le operazioni (ACO) è uno dei due comandi strategici dell'Organizzazione del Trattato del Nord Atlantico (NATO), l'altro è il comando alleato per la trasformazione (ACT). Il quartier generale e il comandante dell'ACO sono rispettivamente il quartier generale supremo delle potenze alleate in Europa (SHAPE) e il comandante supremo alleato in Europa (SACEUR).

[37] L' Agenzia per le comunicazioni e l'informazione della NATO (Agenzia NCI) è l'hub tecnologico e informatico

CamminoDiritto.it
ISSN 2421-7123

della NATO. L'Agenzia fornisce la tecnologia C4ISR (comando, controllo, comunicazioni e computer, intelligence, sorveglianza e ricognizione; fare riferimento alla terminologia di comando e controllo) inclusa la difesa informatica e missilistica. L'Agenzia NCI, guidata dal Direttore Generale, ha sede a Bruxelles, in Belgio. L'Agenzia è il braccio esecutivo dell'Organizzazione per la comunicazione e l'informazione della NATO (NCIO). Il NCIO è gestito da un Consiglio di vigilanza dell'agenzia (ASB) composto da rappresentanti di ogni Stato membro della NATO. L'ASB sovrintende al lavoro del NCIO. Dopo essersi consultato con il Segretario Generale della NATO, l'ASB del NCIO nomina il Direttore Generale dell'Agenzia. Tutti i 31 stati della NATO sono membri del NCIO. L'ASB, che riferisce al Consiglio Nord Atlantico (NAC), emette direttive e prende decisioni politiche generali per consentire al NCIO di svolgere il proprio lavoro. Le sue decisioni su questioni fondamentali come la politica, la finanza, l'organizzazione e lo stabilimento richiedono l'accordo unanime di tutti i paesi membri. Al vertice di Lisbona del novembre 2010, i capi di Stato e di governo della NATO hanno concordato di riformare le 14 agenzie NATO esistenti situate in sette Stati membri. In particolare, gli alleati hanno concordato di razionalizzare le agenzie in tre grandi temi programmatici: appalti, supporto, comunicazioni e informazioni. La riforma mira a migliorare l'efficienza e l'efficacia nella fornitura di capacità e servizi per ottenere una maggiore sinergia tra funzioni simili e per aumentare la trasparenza e la responsabilità. Nell'ambito del processo di riforma l'Agenzia NCI è stata creata il 1° luglio 2012 dalla fusione dell'Organizzazione NATO C3, dell'Agenzia dei servizi di comunicazione e dei sistemi informativi della NATO (NCSA), dell'Agenzia di consultazione, comando e controllo della NATO (NC3A), dell'Agenzia di gestione del sistema di comando e controllo aereo della NATO (NACMA) e del Servizio di tecnologia dell'informazione e della comunicazione della sede della NATO (ICTM).

[38] Nel febbraio 2023 i ministri della Difesa della NATO hanno approvato la Guida politica per la pianificazione della difesa 2023, forse preannunciando il cambiamento più significativo nella pianificazione della difesa dalla fine della guerra fredda. Informato dal miglior pensiero politico e militare, tra cui l'ultimo Concetto strategico, il Concetto per la deterrenza e la difesa dell'area euro-atlantica e il Concetto di Capstone per la lotta alla guerra della NATO, ACT attende con impazienza un anno entusiasmante e stimolante. L'orientamento politico 2023 rappresenta il culmine della prima fase del ciclo di pianificazione della difesa. I Comandi strategici, con il Comando alleato per la trasformazione in testa, sono già profondamente immersi nel lavoro necessario per tradurre la guida delle Nazioni nei requisiti minimi di capacità che descriveranno il pool di forze e capacità richieste dall'Alleanza per raggiungere il suo livello di ambizione. La combinazione di un esigente livello di ambizione, un'ampia gamma di concetti nuovi e in via di sviluppo e una spinta rafforzata per allineare più strettamente la pianificazione delle operazioni e della difesa significa che molte sfide saranno acute nel prossimo anno. Lavorando a stretto contatto con il Comando alleato per le operazioni e altre entità della NATO, il Comando alleato per la trasformazione dovrà abbracciare l'ignoto, rimanere flessibile e preservare lo spazio di manovra per soddisfare le elevate aspettative delle Nazioni. Il processo di pianificazione della difesa della NATO non è lineare, c'è di più che il Comando alleato per la trasformazione farà nel 2023. Sono in corso i preparativi per il processo di targeting che inizierà nel 2024 e si concluderà nel 2025 con l'obiettivo di fornire un risultato coerente e trasparente. Allo stesso modo le nostre squadre a Mons sosterranno lo Staff internazionale nell'autunno del 2023 mentre iniziano il processo impegnativo ma importante di revisione dei risultati dell'ultimo ciclo. Ciò comporterà a turno incontri bilaterali con ciascuno degli alleati e offrirà naturalmente l'opportunità di abbracciare le conversazioni aperte e sincere necessarie per fornire le capacità necessarie per consentire i tre compiti fondamentali dell'Alleanza: deterrenza e difesa; prevenzione e gestione delle crisi; e sicurezza cooperativa.

[39] A tal fine già nel 2014 l'Alleanza aveva lanciato la Nato Industry Cyber Partnership (Nicp), che prevede tra l'altro la partecipazione dei rappresentanti industriali al Cyber Defence Workshop annuale volto allo scambio con gli alleati di informazioni altamente tecniche sulle minacce, le vulnerabilità e le possibili soluzioni

[40] Si veda per maggiori approfondimenti www.altalex.com;

[41] Si consulti www.wikipedia.org per maggiori informazioni;

[42] A seguito di tale catastrofe il governo estone si è ben presto affrettato ad incolpare la Russia, accusandola di essere direttamente coinvolta. Solo successivamente si sono fatti dei passi indietro attesa l'assoluta mancanza di prove fornite alla base di queste accuse. In risposta a tali attacchi la NATO ha altresì condotto una propria valutazione interna inerente alla sicurezza informatica ed alle difese infrastrutturali. La valutazione ha condotto alla elaborazione di un rapporto inviato ai ministri della difesa alleati nell'ottobre del 2007. Il rapporto in questione ha delineato le leggi internazionali che sono considerate applicabili al regno informatico

CamminoDiritto.it
ISSN 2421-7123

[43] The NATO Cooperative Cyber Defence Centre of Excellence is a multinational and interdisciplinary cyber defence hub, per maggiori informazioni si veda {https/URL}

[44] Si veda per maggiori approfondimenti www.altalex.com

[45] L'eccessiva pervasività di questi attacchi cibernetici ha portato la Nato a dichiarare il cyber spazio come dominio operativo già dal 2016, compiendo numerosi passi avanti nell'approccio a questo tipo di minaccia. Addirittura, si è visto come questi attacchi possano realizzare l'attivazione della clausola di difesa di cui all'art.5 del Trattato dell'Atlantico del Nord, in ragione della circostanza che la componente cibernetica rappresenterà sempre più parte integrante dei conflitti.

[46] Per le capitali appena richiamate, difesa e deterrenza cyber equivale ad assicurare non solo adeguate capacità di reazione in caso di attacco cibernetico ma anche di adeguata possibilità di azione preventiva ai danni di potenziali avversari. Nel 2016, a titolo meramente esemplificativo, il Regno Unito ha condotto e portato a termine con successo un attacco cibernetico ai danni dell'Isis;

[47] Si veda per maggiori informazioni: www.altalex.com

[48] La "data retention" consiste nel periodo di conservazione dei dati personali – che il titolare del trattamento determina in ottemperanza al principio di minimizzazione – necessario per raggiungere le finalità connesse ad un determinato trattamento. Pertanto, dando per scontato che il dato personale sia stato acquisito lecitamente e che le finalità del trattamento siano altrettanto lecite, bisogna in questo caso stabilire l'intervallo temporale all'interno del quale il trattamento di tale dato possa essere opportunamente motivato. I principali punti di riferimento, a proposito della conservazione dei dati dei dipendenti, sono costituiti: dall'art. 5 GDPR il quale introduce il concetto di "scadenza" della finalità del trattamento; dall'art. 13 GDPR il quale prevede che nell'informativa debbano essere riportati il tempo di conservazione o i criteri per la definizione dello stesso. Pertanto, è lo stesso legislatore ad introdurre un certo margine di flessibilità, potendo il titolare del trattamento indicare un termine fisso (es. 10 anni) o criteri per il calcolo di tale termine (es. i termini di prescrizione legale o – nel caso delle strutture sanitarie – l'assenza di termini di conservazione della cartella clinica). A tali criteri potrebbero affiancarsi quelli previsti da Provvedimenti del Garante Privacy su temi specifici (es. videosorveglianza, marketing e profilazione del consumatore).

[49] La sicurezza zero-trust ha sostituito i vecchi presupposti secondo cui le risorse all'interno del perimetro della rete aziendale devono essere ritenute attendibili e considera la fiducia come una vulnerabilità, dal momento che gli utenti di una rete "attendibile" potevano spostarsi all'interno della rete o causare l'esfiltrazione di tutti i dati ai quali avevano legittimamente accesso. In un'architettura zero-trust non viene effettuato alcun tentativo di creare una rete attendibile. Invece il concetto di fiducia viene completamente eliminato. Una volta determinata la superficie protetta, il modo in cui il traffico di rete attraversa la superficie, sapere quali utenti stanno accedendo alle risorse protette, catalogare le applicazioni utilizzate e i metodi di connettività diventano i cardini della creazione e dell'applicazione di policy di accesso sicure per i dati protetti. Dopo aver compreso queste dipendenze è possibile implementare i controlli in prossimità della superficie protetta per creare un microperimetro, in genere utilizzando un firewall di nuova generazione (NGFW), chiamato gateway di segmentazione, che consente solo il traffico noto proveniente da utenti e applicazioni legittimi. Il NGFW offre visibilità sul traffico e applica il controllo dell'accesso basato sul metodo Kipling definendo la policy di accesso in base a chi, cosa, quando, dove, perché e come. Ciò aiuta a determinare quale traffico può passare attraverso il microperimetro, impedendo l'accesso a utenti e applicazioni non autorizzati e mantenendo all'interno i dati sensibili. Poiché la forza lavoro è distribuita e remota il modello zero-trust non dipende da alcuna posizione specifica. Le risorse e gli utenti possono risiedere ovunque: on-premise, in uno o più cloud o nell'edge, nelle case dei dipendenti come su dispositivi IoT.

Bibliografia:

-Porcedda Maria Grazia; Cybersecurity, Privacy and Data Protection in EU Law: A Law, Policy and Tecnology

CamminoDiritto.it
ISSN 2421-7123

Analysis, Milano, 2023.

-Laselli Michele, Caria Giovanni Battista; Cybersecurity & Cyberwarfare. Diritto, tecnologia e sicurezza, Roma, 2023.

-Ursi Riccardo; La sicurezza nel cyberspazio, Milano, 2023.

-Vinciguerra Calogero; Intelligence e sicurezza del cyberspazio, Lecce, 2022.

- Brooks Charles J., Craig Jr. Philip A.; Practical Industrial Cybersecurity. ICS, INDUSTRY 4.0, AND LLoT, 2022.

-Casadei Thomas e Pietropaoli Stefano; Diritto e tecnologie informatiche. Questioni di informatica giuridica, prospettive istituzionali e sfide sociali, Padova, 2021.

-Contaldo Alfonso, Mula Davide; Cybersecurity Law. Disciplina italiana ed europea della sicurezza cibernetica anche alla luce delle norme tecniche, Pisa, 2020.

-Sandro Marrone ed Ester Sabatino., La difesa cibernetica nei Paesi NATO: modelli

a confronto, 2020.

-Mollo Francesca; Protezione dei dati personali e profili assicurativi, Padova, 2020.

-Martina Petrucci Marta Cogode; Il cybersecurity act: i vantaggi del nuovo regolamento europeo di certificazione della cyber-sicurezza per le tecnologie dell'informazione e della comunicazione, 2019.

- Paolo Giudice Andrea Piazza Giovanni Reccia Nunzia Ciardi, Corrado Giustozzi;

Rapporto Clusit 2019, 2019.

- Sica Salvatore, Codiglione Giorgio Giannone**;** Security and Hate Speech. Personal

Safety and Data Security in the Age of Social Media, Bologna, 2018.

- Baldoni R., Montanari L., "Italian Security Report. Un framework nazionale per la

Cyber Security", Cyber Intelligence and Information Security Center, Sapienza

Università di Roma, febbraio 2018.

- Marotta A., Martinelli F., Nanni S., Orlando A., Yautsiukhin A.;"Cyber-insurance

survey", Computer Science Review, Volume 24, pgg. 35-61, maggio 2017.

- Ulrik Franke; "The cyber insurance market in Sweden", Computer & Security,

Volume 68, pgg. 130 -144, luglio 2017.

-Sica Salvatore, D'Antonio Virgilio, Riccio Giovanni Maria; La nuova disciplina europea sulla privacy, Padova, 2016.

-Sica Salvatore, Zenozencovich Vincenzo; Manuale di diritto dell'informazione e della comunicazione, Padova, 2015.

-J.A. Green. Cyber Warfare. A multidisciplinary analysis, Routledge, New York,

2015.

- Zichao Yang, John C.S. Lui; "Security adoption and influence of cyber-insurance

markets in heterogeneous networks", Performance Evaluation, Volume 74, 2011.

- Y.Y. Haimes. On the definition of resilience in systems, Risk Analysis. 2009, pp.

CamminoDiritto.it
ISSN 2421-7123

498– 501.

- Baroni L., “Le polizze per i rischi tecnologici”, Assicurazioni a cura di Pellino P.,

Pellino R., pgg. 343 ss., Sorgi, Torino, 2008.

- Bohme R., Kataria G., “Models and Measures for Correlation in Cyber-Insurance”,

Workshop on the Economics of Information Security (WEIS), University of Cambridge, UK, 2006.

---

* Il simbolo {https/URL} sostituisce i link visualizzabili sulla pagina:
https://rivista.camminodiritto.it/articolo.asp?id=11188