Dipartimento di Scienze Politiche *Cattedra di Diritto dell'Economia*

La Cybersecurity: tra protezione giuridica e politiche multilivello.

RELATORE
Prof. Giuseppe di Gaspare

CANDIDATO
Clarissa Guerrini
Matr.075532

ANNO ACCADEMICO 2016-2017

La Cybersecurity: tra protezione giuridica e politiche multilivello.

INDICE

INTRODUZIONE

In questa tesi verrà trattato il controverso tema della *cybersecurity.* L'approccio di analisi utilizzato sarà multilivello, ovvero focalizzato sulle varie realtà internazionali. Tali "realtà" saranno gli Stati Uniti, veri protagonisti della rivoluzione 2.0, il Regno Unito, la Germania, la Francia e l'Italia.

Per fornire una visione esaustiva e una spiegazione chiara sulla sicurezza cibernetica, ho ritenuto necessario adottare una visione giuridica e una politica. La giustificazione della mia scelta risiede nella natura delle politiche nazionali, risultato di un corpo giuridico inoppugnabile. L'analisi multilivello invece deriva dalla convinzione che il *cybercrime* possa essere sconfitto solamente grazie ad un azione coordinata, attraverso un *comprehensive approach* che coinvolga tutte le potenze.

L'elaborato sarà composto da tre capitoli. Il primo capitolo servirà a chiarire e definire alcuni concetti chiave del mondo cibernetico, quali cyberspace,cybercrime e cybersecurity stessa, sottolineandone i caratteri essenziali.

Il secondo prenderà in esame l'ordinamento statunitense, inglese, tedesco e francese, per capire come i nostri maggiori Paesi Partner gestiscano questa nuova minaccia.

L'ultimo capitolo sarà incentrato sull'Italia, in particolare sul suo cammino dalla prima legge sulla sicurezza informatica (legge n.547/1993) all'applicazione della direttiva NIS (direttiva UE 2016/1148).

Per concludere saranno paragonate le differenti strategie nazionali adottate.

Alla fine della tesi verrà presentato un breve approfondimento sulla situazione attuale, per sottolineare la crescente importanza della cybersecurity e verificarne l'impatto nella prassi.

Capitolo 1. Introduzione alla *Cybersecurity*

La radice di "cibernetica", termine che troveremo spesso in questa tesi, deriva dall' antica parola greca *kybernetes* (κυβερνήτης) che significa "dirigere"(controllo) o "navigare". Il controllo può essere inteso in due modi: costringere a comportarsi in un certo modo, o fornire informazioni soggettive che consentano di regolare il proprio comportamento[1].

La distinzione tra le due definizioni di "controllo", ovvero coercizione o consiglio, non è scontata; allo stesso modo definire il *Cyberspace*, sia dal punto di vista fisico che teorico, non è semplice.[2]

1.1. La "doppia faccia" del *Cyberspace*

Lo "Spazio cibernetico" (*Cyberspace*) è definito come l'ambiente composto da infrastrutture computerizzate, inclusi hardware, software, dati e utenti, e dalle relazioni logiche tra loro. Inoltre esso comprende Internet, reti di comunicazione, sistemi attuatori di processi e dispositivi mobili dotati di una connessione di rete.[3]

Il termine "*cyberspace*" fu coniato dallo scrittore di fantascienza Gibson, che utilizzò il termine nel romanzo "Neuromancer"(1984). Da allora il mondo cibernetico cominciò a esercitare la sua influenza.[4]

La teoria precedette le prove empiriche sulla sua esistenza, sottolineandone i caratteri di illimitatezza e immaterialità.[5] La concezione di uno spazio immateriale e incommensurabile si sviluppò con il cloud computing (gestione dei dati, gestione delle informazioni, condivisione di file), dando vita alla c.d."virtualizzazione". Con la virtualizzazione il dominio di Internet fu incontrastato: da mezzo di interazione, condivisione di idee e informazioni, diventò anche il motore di nuove modalità di coinvolgimento politico,sociale, di scambio economico e commerciale. Le reti si fecero sempre più interconesse, i costi sempre più bassi, e il *cyberspace* crebbe.

La rivoluzione virtuale continua a trasferire una mole crescente di dati, database, piattaforme, infrastrutture e software dal computer dell'utente a data server più efficienti [6]; questo spostamento agisce a scapito della sicurezza e della privacy dell'*user.*[7]

Dunque, oltre a favorire e incrementare l'interazione tra individui, aziende e istituzioni per finalità

[1]Wiener N. (1965), *Cybernetics:or the Control and Communication in the Animal and the Machine*, 2nd ed. MIT Press
[2]Singer P.W., Friendman A. (2014), *Cybersecurity: What Everyone Needs to Know* ,OUP USA
[3]Italian Presidency of the Council of Ministers (2012), *Il linguaggio degli organismi informativi. Glossario intelligence*, Sistema di informazione per la sicurezza della repubblica, Quaderni di Intelligence Gnosis
[4]Gibson W. (1984), *Neuromancer*, Ace. C'è qualche similitudine con il racconto di Forster E. M. (1928), *The Machine Stops*
[5]Barlow J. P. (1996), *A Declaration of the Independence of Cyberspace*, Davos, Switzerland; Cohen J. E. (2007), *Cyberspace As/And Space*, Columbia Law Review n° 107, pp. 210-256
[6]De Capitani di Vimercati S., Foresti S., e Samarati P. (2012), *Managing and accessing data in the cloud: Privacy risks and approaches*, In Proc. of the 7th International Conference on Risks and Security of Internet and Systems
[7]Anche l'UE definisce la giurisdizione USA inadeguata per la protezione dati. Vedi Rotenberg M. and Jacobs D., *Privacy, Security, and Human Dignity in the Digital Age: Updating the Law of Information Privacy. The New Framework of the European Union*, Harvard Journal of Law & Public Policy n° 36, pp. 637-641.

sociali, economiche e finanziarie, l'evoluzione digitale della società ha creato nuove opportunità per attività criminali di vario tipo. Da un lato compaiono crimini completamente nuovi, quali le frodi finanziarie online e l'abuso di credenziali, dall'altro quelle tradizionali possono essere perpetrate con strumenti nuovi e pervasivi. Così i singoli o i gruppi criminosi ottengono mediante il Web guadagni illeciti.

È la doppia faccia del *cyberspace,* dove i benefici nascondono sempre delle minacce. Tali minacce sfruttano le vulnerabilità delle applicazioni e dei sistemi informatici, progettati e realizzati seguendo criteri di usabilità e resilienza, senza considerare la sicurezza.[8]

1.2. Dalla criminalità tradizionale al *Cyber-crime*

Il *cyber crime* può essere definito come un insieme di violazioni perpetrate tramite il *cyber space*.

Esso si distingue dalla criminalità tradizionale per l'assenza di confini fisici e limiti geografici, che disorientano la "vittima". Quest'ultima non può reagire, data l'incapacità di percepire l'attacco "fisicamente".

I trend principali del "crimine cibernetico" sono furto e manipolazione di dati sensibili, business della contraffazione, criptovalute e riciclaggio; questi rappresentano attacchi sofisticati e multiscopo[9].

*Furto e manipolazione di dati sensibili***:**

I dati sensibili rappresentano un bene sempre più sfruttato dai cyber-criminali. La crescita dei servizi cloud e dalla Internet of Things intensifica la raccolta, l'elaborazione e l'archiviazione di dati digitalizzati. Tutto ciò aumenta il livello di rischio connesso alle intrusioni, che vanno dal tradizionale schema di frode (e.g. relativamente a carte di credito o credenziali bancarie), alle attività di estorsione o di cyber-spionaggio industriale/governativo). I dati sono ripuliti e rivenduti in blocchi in base alle esigenze degli acquirenti, dopo essere stati acquistati in modalità "crime as a service". Aumenta il trend delle intrusioni nelle infrastrutture critiche, come quelle di logistica e trasporti, al fine di facilitare attività criminali tradizionali. Sono proprio le aziende a facilitare tali intrusioni, tramite l'utilizzo di sistemi automatizzati gestiti da remoto.

Business della contraffazione:

Il Surface Web e il Deep Web contengono molteplici mercati illegali. Al loro interno sono dislocati prodotti contraffatti online, mirati alle necessità prossime e future dei consumatori. Questi mercati illegali sono sempre più sofisticati, rendendo difficile distinguerli da quelli legali. Diminuendo la

[8]Laboratorio Nazionale di Cyber Security (2015), *Il Futuro della Cyber Security in Italia*, Consorzio Interuniversitario Nazionale per l'Informatica

[9]Presidenza del Consiglio dei Ministri (2013), *Quadro strategico nazionale per la sicurezza dello spazio cibernetico*. Mazzucchelli C. (2013), *Internet e nuove tecnologie: non tutto è quello che sembra*, Delos Digital srl, 24 dicembre

capacità di riconoscimento, aumenterà la contraffazione e la vendita online di prodotti di consumo quotidiano.

Criptovalute e riciclaggio:

Le criptovalute (Bitcoin) rappresentano un sistema di pagamento in via di estensione.

La loro origine è riscontrabile nell'utilizzo crescente che ne fanno le aziende, con servizi e-commerce e con la diffusione di Bitcoin-Bancomat. I Bitcoin espongono gli utilizzatori al rischio di violazione dei propri e-wallet e degli "exchange", entità che provvedono alla conversione della criptovaluta in moneta "fiat".

Tutto ciò consente scambi monetari protetti da pseudonimato e esterni ai controlli dei circuiti finanziari, rendendo possibile una maggiore espansione del commercio illegale.

Un tipo di commercio illegale è il commercio online di materiale e prestazioni professionali "crime as a service". Questo può essere anche offline, ad esempio tramite il supporto di attività di contrabbando o traffico di droga[10]

Oltre alle attività criminose a scopo di lucro, nel cyber spazio vengono svolte operazioni di cyber-spionaggio per danneggiare apparati governativi, civili e militari, e imprese private.

Gli Stati più avanzati stanno disponendo anche di unità offensive e difensive per la *cyber-war*, benchè, data l'importanza delle relazioni internazionali, atti di questo genere risultano improbabili.

Negli ultimi tempi stiamo assistendo all'utilizzo dello spazio cibernetico da parte di organizzazioni terroristiche; la rete viene sfruttata per finalità propagandistiche, addestramento, autofinanziamento e pianificazione. La capacità di questi gruppi di rappresentare un pericolo reale è destinata a crescere nel medio-lungo termine, di pari passo con le loro competenze.

Considerando la mole delle cyber-minacce e il loro continuo sviluppo, le singole misure protettive non bastano più. Occorrono vere e proprie strategie difensive, di *cybersecurity,* sostenute da un apposito corpo legislativo.

1.3. Le origini della *Cybersecurity*

La Cybersecurity è la condizione in cui il cyberspazio è protetto rispetto ad eventi volontari o accidentali. Consiste nell'adozione di procedure di autenticazione, gestione degli accessi, analisi dei rischi, rilevamento e risposta ad incidenti/attacchi, mitigazione degli impatti, recupero di componenti soggetti ad attacco, formazione ed educazione di personale, verifica e valorizzazione dei sistemi di informazione e comunicazione[11].

[10] Parodi C. (1997), *La frode informatica: presente e futuro delle applicazioni criminali nell'uso del software, in Criminalità informatica*, Sarzana Di S. Ippolito F. (a cura di), in Diritto e procedura penale. Pica G. (2000)*, Computer crimes e uso fraudolento delle nuove tecnologie*, Seminario di studi, Roma 15 dicembre. Lorusso S.(2011), *L'insicurezza dell'era digitale, Tra cybercrimes e nuove frontiere dell'investigazione*, Milano.

[11]Presidenza del Consiglio dei Ministri (2012), *Il linguaggio degli organismi informativi. Glossario intelligence*, Sistema di informazione per la sicurezza della repubblica, Quaderni di Intelligence Gnosis

L'obiettivo della " sicurezza informatica", è la difesa delle infrastrutture critiche nazionali (reti elettriche, idriche, informatiche,...), delle organizzazioni governative, delle aziende e dei singoli cittadini.[12]

Per raggiungerlo vengono progettati e realizzati "Piani strategici nazionali".

I Piani Strategici richiedono una relazione stretta tra pubblico, privato e mondo della ricerca, attivando misure successive di contrasto al *cyber crime* e azioni di prevenzione, quali sensibilizzazione e coordinamento. Per gestire il rischio in modo adeguato, è necessario progettare un efficace processo di gestione del rischio, prima individuando ciò che potrebbe andare male (identificazione del rischio), poi valutando quali rischi dovrebbero essere affrontati (analisi e valutazione dei rischi) ed attuando la risposta adeguata.

GESTIONE DEL RISCHIO

RISK ASSESSMENT	*RISK TREATMENT*
Identificazione Analisi Valutazione	Prevenzione Detenzione Risposta Copertura

Tale processo di gestione del rischio viene utilizzato come paradigma per l'istituzione di un'efficace strategia nazionale di sicurezza informatica e rappresenta uno degli elementi imprescindibili di *Cybersecurity.*

1.4. 8 elementiper la *Cybersecurity*

La frequenza e la persistenza dei rischi informatici richiede alle entità pubbliche e private di adattarsi al panorama operativo e di minaccia e di rispettare certi requisiti legali e normativi.

Esistono otto elementi fondamentali, non vincolanti e di alto livello, che consentono alle aziende di progettare e implementare la propria strategia e framework operativo in materia di cybersecurity. Tali elementi sono stati individuati dai Paesi membri del G7 e sono: un *Framework* di *Cybersecurity,* una *Governance,* un *Risk Assessment,* un effettivo *Monitoring,* una capacita di *Response* e *Recovery,* un sistema di *Information Sharing* e un continuo *Learning* della minaccia.[13] Questi sono sfruttati anche dalle autorità pubbliche per guidare la regolamentazione e la vigilanza del settore.

[12] European Union Agency for Network and Information Security (2012), *National Cyber Security Strategy. Practical Guidebook*, p. 8

[13]Banca D'Italia (2016), *G7 Fundamental elements of Cybersecurity for the financial sector,* Report

1. Cybersecurity Strategy and Framework.

Il fine ultimo delle strategie di cybersecurity è di identificare, capire e ridurre il rischio informatico. Tutto ciò è possibile attraverso un processo integrato e globale. Gli enti coivolti devono risalire alla natura, alla dimensione, alla complessità, alla cultura e al profilo del rischio. Data la vulnerabilità del contesto è necessario il supporto di una giurisdizione in materia.

2. Governance.

Una governance effettiva garantisce un sistema chiaro e articolato di responsabilità, incrementa la comunicazione tra unità operative, l'informazione tecnlogica, i rischi e le attività di controllo relative.

3. Risk and Control Assessment.

Idealmente, gli enti dovrebbero valutare i *cyber-risk* interni, rappresentati da persone, processi e tecnologie, ed evidenziando i dati che supportano ogni funzione, attività di produzione e servizio. Dovrebbero identificare e valutare l'esistenza ed effettività dei controlli o mitigare il rischio tramite la sua condivisione o il trasferimento.

4. Monitoring.

Un effettivo monitoraggio aiuta gli enti a sviluppare una certa "tolleranza" al rischio, tramite una risposta tempestiva o rimediando alle debolezze del sistema. I protocolli di analisi e controllo forniscono un essenziale meccanismo di assicurazione, la cui effettività dipende dalla natura del rischio e dall'ambiente di controllo. Tali meccanismi sono invece indipendenti dal personale responsabile per l'implementazione del *cybersecurity program*.

Attraverso gli esami on-site e altri meccanismi di supervisione (analisi comparate, esercizi tra pubblico e privato), gli enti pubblici possono comprendere le vulnerabilità e l'ampiezza delle minacce, così come quelli privati possono risalire al profilo e alle capacità del rischio.

5. Response.

Gli enti dovrebbero implementare le politiche contro eventuali incidenti e inserire ulteriori controlli per garantire una risposta effettiva. Tali controlli devono chiaramente indicare i responsabili del decision-making, definire le procedure e stabilire forme di comunicazione tra stakeholders interni ed esterni.

6. Recovery.

Una volta assicurata la stabilità e l'integrità delle operazioni, proprie ed effettive misure devono essere adottate dando la priorità alle aree critiche dell'economia. Mantenere fiducia nelle aziende significa un sistema di mutua assistenza pubblico-privato e stabilire e testare i piani per attività essenziali e i processi chiave (ad esempio il finanzamento) di recupero.

7. Information Sharing.

Condividere informazioni tecniche, come gli indicatori della minaccia o dettagli sulle vulnerabilità, porta gli enti a tenersi aggiornati e imparare i metodi all'avanguardia usati degli hackers. Data l'importanza di tale punto, le aziende e le autorità pubbliche devono identificare ed eliminare ogni impedimento allo scambio d'informazioni.

8. Continuous Learning.

Le minacce cibernetiche e le vulnerabilità si evolvono rapidamente, così come devono fare le pratiche per combatterli. Le strategie di cybersecurity e i frameworks necessitano di una periodica revisione e capacità di adattarsi al cambiamento. Lo sviluppo di settori come l'energia e le telecomunicazioni deve essere considerato parte di questo processo di revisione.

Ogni Stato presenterà poi una personale strategia, adeguata alle proprie peculiarità. Il primo passo resta comunque l'individuazione della minaccia e la consapevolezza della sua natura. Successivamente si potrà procedere per migliorare i propri livelli di protezione.

Qualsiasi attore, statale o non, può essere carnefice o vittima, ed essere utilizzato come base di attacco. In tal caso l'interdipendenza delle reti crea una reazione a catena, che parte dall'organizzazione "compromessa" fino a mettere a repentaglio le altre organizzazioni collegate. La situazione peggiore si ha quando raggiunge i vertici statali[14].Un esempio drammatico che ha reso il mondo consapevole della pericolosità insita nei sistemi informatici, si ebbe nel 2007. La vittima fu il piccolo Stato estone, dove una serie di attacchi cibernetici ha rischiato di abbattere l'intera infrastruttura informatica del Paese[15]. L'evento ebbe un impatto dirompente anche sugli altri Paesi, soprattutto negli Stati Uniti. Circa dieci anni fa nacquero i primi documenti ufficiali per la protezione cibernetica.

Questo capitolo ha delineato il fenomeno della Cybersecurity; lo ha definito e ne ha chiarito l'origine, il ruolo e le motivazioni. L'obiettivo è diffondere tale "cultura" , determinante per realizzare efficienti politiche digitali. L'assenza di quest'ultime infatti potrebbe esporre ogni Stato a perdere posti di lavoro qualificati, ricerca universitaria e privata, produzione di know how, imprese innovative, startup e altre occasioni di crescita. Secondo il World Economic Forum, le perdite economiche causate da attacchi cyber arriveranno a tremilamiliardi di dollari nel 2020; naturalmente se gli Stati non provvedono alla propria sicurezza.[16]Il capitolo successivo sarà incentrato proprio sulle politiche digitali nazionali, prendendo in considerazione le strategie di cybersecurity adottate e implementate in USA, Regno Unito, Germania e Francia .

[14]Singer P.W., Friendman A. (2014), *Cybersecurity: What Everyone Needs to Know* ,OUP, USA
[15]Tikk E., Kaska K., Vihul K..L., *International Cyber Incidents: Legal Considerations*, Tallinn: CCD COE publications
[16]World Economic Forum (2014), *Global Risks*, Insight Report Ninth Edition

Capitolo 2. Ad ogni Paese la sua Cyber-strategy

2.1. USA*:* ultimi sviluppi con la "Strengthening U.S. Cyber Security and Capabilities"

La storia della legislazione statunitense sulla cybersecurity riflette un insieme di aree e fonti giuridiche eterogenee. Le aree spaziano dalla criminalità informatica alla sicurezza nazionale (protezione delle infrastrutture critiche), mentre le fonti comprendono sia statuti legislativi che direttive presidenziali. Le origini della Cybersecurity statunitense risalgono al 1998, quando l'ex presidente Clinton ha emesso la Decisione-Direttiva presidenziale 63 (PDD-63), relativa alla protezione dell'infrastruttura critica. La PDD63 fu preceduta dalla CFAA, legge nel 1986, che sanzionava l'accesso intenzionale e non autorizzato a un computer protetto. Il Computer Fraud and Abuse Act (CFAA) non rappresentava ancora una vera e propria "legge sulla cyberecurity", ma ha facilitato lo sviluppo del settore.[17]

Il primo progetto statunitense in materia, venne presentato dal Centro per gli studi strategici e internazionali nell'agosto 2007, dopo l'attacco all'Estonia, e dopo che un'ondata di attacchi dannosi nel cyberspazio ha colpito gli Usa. Il progetto, sotto la guida del Congresso, ha impiegato un gruppo di individui specializzati, allo scopo di individuare raccomandazioni da attuare rapidamente. L'obiettivo del governo era un notevole miglioramento della sicurezza della rete della nazione e la formulazione di raccomandazioni a lungo termine. Esso ha contribuito a creare un quadro di sicurezza nazionale, in un maggiore rispetto per la privacy e le libertà civili, e una strategia globale di sicurezza nazionale che abbraccia sia gli aspetti domestici che internazionali della sicurezza informatica[18]. Tale lavoro è stato incoraggiato dal Dipartimento della Difesa (DoD) statunitense, che un anno dopo, avviò un proprio sviluppo nel campo *cyber.*[19.]

Più recentemente, nel corso del 112simo Congresso, si è cercato di creare una legislazione completamente dedita alla *cybersecurity.* L'eredità di tale Congresso ha prodotto innumerevoli leggi in merito, di cui pochissime sono entrate in vigore. Una di esse fu il *Cybersecurity Act* nell'aprile del 2012, il cui fallimento spinse il Presidente Obama a emanare un Ordine Esecutivo, presentato il 12 febbraio 2013 con il titolo "Improving Critical Infrastructure Cybersecurity". Il fine ultimo dell'*Improving Critical Infrastructure Cybersecurity* fu quello di migliorare la sicurezza della rete,

[17] Condron S. (2007), *Getting It Right: Protecting American Critical Infrastructure in Cyberspace*, Harvard Journal of Law & Technology, n °20, cap.2, pp.403–422. Brooker B.J, Crawford J., Horowitz B.M. (2007), *A Framework for the Evaluation of State Breach Reporting Laws*, in Proceedings of IEEE Systems and Information Engineering Design Symposium. Granado N., White G. (2008), *Cybersecurity and Government Fusion Centers*, in Proceedings of the 41st Hawaii International Conference on System Sciences

[18] Langevin J.R, McCaul M., Charney T., Raduege H. (2008), *Securing Cyberspace for the 44th Presidence* ,Center for Strategic and International Studies Washington DC

[19] Glebocki, Jr, J. (2008), *DoD Computer Network Operations: Time to Hit the Send Button*, Strategy Research Project, 10 marzo

attraverso una condivisione di informazioni volontarie. Il programma comprese agenzie governative, proprietari e operatori delle infrastrutture critiche del settore privato e richiese lo sviluppo di un quadro di sicurezza della rete per assisterli nell'identificazione, valutazione e gestione del rischio informatico. L'ex Presidente vide la cybersecurity come una delle più gravi sfide per la prosperità economica della nazione e agì di conseguenza[20].

Anche sul piano militare, gli USA stanno affrontano nuove minacce alla propria sicurezza nazionale, in patria e all'estero. La gamma di attori coinvolti in una potenziale *cyberwar* non conosce limiti: hacker solitari, gruppi terroristici, nazioni. Per gli USA, le minacce esterne si incarnano nello Stato cinese, nella Russia, nella Corea del Nord e nell' Iran. La proliferazione di Internet all'interno di tali *rogue state* influenza gli eventi e l'ambiente statunitense, come ha dimostrato lo scalpore suscitato dai video dell'Isis. Tali video di "reclutamento e propaganda" hanno sconvolto l'intera comunità internazionale, rivelando la complessità e vastità dei nuovi mezzi. Alla stregua degli attori statali, vi sono attori non statali che minacciano in egual maniera attacchi dirompenti e distruttivi contro gli Stati Uniti. Questi sfruttano in particolare il furto informatico della proprietà intellettuale, al fine di ottenere un vantaggio tecnologico per scopi militari ed economici. Ciò ha messo in allerta i militari e il Pentagono, con la necessità di avere una strategia e una serie di costrutti operativi innovativi.

A causa della natura altamente automatizzata e interconnessa dell'infrastruttura critica degli Stati Uniti, non è pratico creare una barriera tra operazioni militari e civili in grado di servire gli interessi nazionali. Nel quadro di interagency, il DoD dovrebbe fungere da *lead*: ogni volta che le infrastrutture critiche di difesa sono coinvolte o quando un attacco informatico ha gravemente colpito altre infrastrutture critiche nazionali, tale ente dovrebbe attivare la fase di risposta. Per consentire questa trasformazione, la modifica della legge di Posse Comitatus (PCA) è necessaria. Il PCA vieta infatti al personale militare statunitense di partecipare direttamente alle attività di contrasto nazionali, come condurre sorveglianza, ricerche, perseguimento e sequestri, o fare degli arresti per conto delle autorità civili di contrasto. La proibizione del coinvolgimento militare diretto nell'applicazione della legge è in linea con la legge statunitense[21] e la politica che ne limita il ruolo negli affari interni, ma una sua revisione porterebbe il DoD a condurre operazioni di difesa e offensivi di cyberspazio contro tutti i bersagli necessari.[22]

[20]Flowers A., Zeadally S., Murray A. (2013), *Cybersecurity and US Legislative Efforts to address Cybercrime*, Homeland Security & Emergency Management n°10, cap.1, pp. 1–27. Martinez J.(2012), *White House Circulating Draft of Executive Order on Cybersecurity*, The Hill, September 6. Warfield D. (2012), Critical *Infrastructures: IT Security and Threats from Private Sector Ownership*, Information Security Journal: A Global Perspective, n° 21, cap.3, pp.127–136. LeClaire J. (2012), *Obama May Sign Cybersecurity Executive Order*, CIO Today, November 16

[21]Section 1385 of Title 18, United States Code (USC)

[22]Clarke R.A., Knake R.K. (2014), *Cyber War,* Tantor Media, Inc.; Rid T. (2013), *Cyber War Will Not Take Place*,

2.1.(1). Ultimi Sviluppi e "Strengthening U.S. Cyber Security and Capabilities"

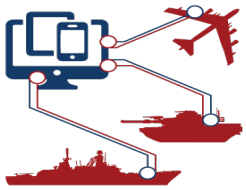
"La sicurezza informatica è una sfida politica, economica, diplomatica e militare.[23]*"*

In queste parole, Marcel Lettre non sottuvaluta la continua evoluzione della minaccia informatica, sempre più rapida e sofisticata nel corso del tempo, considerando sia la minaccia di spionaggio che la minaccia hacking alla stregua di "un continuum di attività che possono condurre ad attacchi significativi sulla infrastruttura nazionale"[24].

"La ricerca di intelligenza artificiale, di autonomia, di apprendimento profondo della macchina, di velocità e il ridimensionamento di costrutti tecnologici sono tutte le caratteristiche dell' innovazione informatica di cui il governo americano ha bisogno"[25].

Attualmente la *cyberdefense* prevede un programma dettagliato redatto del DoD, operativo a partire dal 2018; mentre sul piano giuridico, il Presidente Donald Trump ha presentato un potenziale Ordine Esecutivo, ancora sotto forma di *draft.* La bozza è stata rinominata "Strengthening U.S. Cyber Security and Capabilities".

Cyber Mission Force: 133 teams by 2018

		
Cyber Protection Teams	**National Mission Teams**	**Combat Mission Teams + Support Teams**
68 teams	**13 teams**	**27 teams+25 teams**
Defendere reti, sistemi, informazioni DoD.	Defender il territorio e gli interessi americani dagli attacchi cibernetici, che possono avere conseguenze rilevanti.	Fornire un supporto cibernetico alle operazioni militari ed piani specifici.

Oxford U.P.; Arquilla T. (2012), *Rebuttal: Cyberwar is Already Upon Us*, Foreign Policy n°192, cap. 84; Ronfeldt I. e D. (1993), *Cyberwar is Coming!*, Comparative Strategy vol.12, cap.2, pp. 141-165; Halpin E., Trevorrow P., Webb D., Wright S. (2006), *Cyberwar, Netwar and the Revolution in Military Affairs*, New York: Palgrave Macmillan; Schwartau W. (1994), *Information Warfare: Chaos on the Electronic Superhighway*, New York: Thunders Mountain Press

[23]Discorso del sottosegretario alla Difesa per l'intelligence, Marcel Lettre, durante il Forum per la Difesa Nazionale tenutosi a Simi Valley, in California, il 3 Dicembre 2016.

[24]Mercel Lettre, Former Under Segretary of Defense for Intelligent

[25]Garamone J. (2016), *Intel Undersecretary Describes Cyber Threat, Steps to Combat It*, U.S. Departement of Defence,. U.S. Cyber Command (2016), *Special Report: Department of Defense Cyber Strategy*

Sin dall'inizio della Presidenza Obama, il tema della *cyberdefense* venne affrontato nell'International Strategy For Cyberspace nel 2011. Successivamente furono individuate 4 assi di intervento per adeguarsi alle nuove minacce, sottoscritte nel Cybersecurity National Action Plan. Le quattro assi sono:

- istituzione del Chief Information Security Officer,
- incremento della collaborazione tra governo e aziende strategiche,
- rafforzamento della partnership pubblico-privato soprattutto in supporto alle PMI,
- rafforzamento della protezione delle infrastrutture critiche[26].

Data la complessità della sfida da affrontare, lo sforzo messo in campo da Washington coinvolge un numero rilevante di enti e agenzie governative. Risulta agevole suddividere i compiti tra operazioni interne ed esterne, limitando l'elenco alle agenzie di vertice che coordinano l'intero sforzo nazionale in materia cyber.

Operazioni Interne: La difesa degli assetti chiave in ambito civile, così come la protezione delle attività economiche, ricadono sotto il controllo del Department of Homeland Security (DHS) in concorso con la National Security Agency (NSA) per quanto concerne le operazioni di Information Assurance[27] Il DHS, con 240.000 dipendenti in posti di lavoro ampi nel campo dell'aviazione, della sicurezza, delle frontiere, dell'analisi cyber, è l'autorità nazionale con il compito della protezione delle infrastrutture critiche.[28] Ciò è possibile grazie all'impiego del National Cybersecurity and Communications Integration Center (NCCIC)[29] che a sua volta può fare perno sull'Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)[30] al fine di ridurre i rischi dei settori dell'economia e delle strutture nazionali più esposte alla minaccia cibernetica.

Operazioni Esterne: Le strutture militari vengono invece protette dallo US Cyber Command

[26] DoD (2016), *Cybersecurity National Action Plan*
[27] È la pratica di proteggere e gestire i rischi connessi all'uso, allo stoccaggio e alla trasmissione di sistemi di dati e di informazione. I processi di garanzia delle informazioni garantiscono in genere la seguenti funzioni per i dati e per i sistemi di informazioni associati.
[28] Official website of the Departement of the Homeland Security
[29] Il NCCIC funge da punto di riferimento per l'insieme di partner coinvolti nella protezione della cyberecurity e della comunicazione, coordinandoli e sincronizzandoli. I partner di NCCIC includono altre agenzie governative, il settore privato e le entità internazionali. Lavorando a stretto contatto con i propri partner, NCCIC analizza le informazioni sulla sicurezza in rete e le comunicazioni, condivide informazioni tempestive e funzionali e coordina gli sforzi di risposta, mitigazione e ripristino.
[30]Il team di risposta dei sistemi di controllo industriale (Cyber Emergency Response Team) (ICS-CERT) lavora per ridurre i rischi all'interno e in tutti i settori dell'infrastruttura critica, collaborando con le agenzie di contrasto e con la comunità di intelligence, coordinando gli sforzi tra governi federali, statali, locali e proprietari, operatori e fornitori. Inoltre, ICS-CERT collabora con i team di risposta informatici di emergenza (CERT) a livello internazionale e privato per condividere gli incidenti di sicurezza correlati ai sistemi di controllo e le misure di mitigazione.

(USCYBERCOM), un comando interforze attualmente subordinato allo US Strategic Command (USSTRATCOM)[31]. Sempre allo USCYBERCOM spettano anche le azioni cibernetiche da condurre verso l'esterno, tra cui rivestono particolare importanza le Offensive Cyberspace Operations (OCO – operazioni offensive in ambito cyber). Proprio allo scopo di continuare ad aumentare le capacità americane nel settore, il budget della Difesa statunitense per l'anno fiscale 2016 ha previsto che lo USCYBERCOM raggiunga i 6.000 effettivi per un totale di 133 teams operativi nelle Forze Armate. Inoltre, per il 2017, è stato presentato un budget della Difesa che prevede stanziamenti per il comparto cyber pari a 7 miliardi di dollari per migliorare ulteriormente le capacità di resilienza e l'addestramento del personale. Al momento, per quanto concerne le operazioni di spionaggio di segnali elettromagnetici (SIGINT), queste sono assegnate alla NSA che ha il compito, a livello federale, di monitorare, collezionare, processare informazioni e dati al fine di soddisfare le esigenze nazionali in materia di intelligence e contro-intelligence.[32]

Il Presidente Donald Trump ha firmato l'11 maggio 2017 un ordine esecutivo in materia, chiamato "Strengthening U.S. Cyber Security and Capabilities". Esso ribadisce l'importante ruolo svolto dal Dipartimento per la Sicurezza Nazionale (DHS) per rafforzare la sicurezza e la resilienza delle reti federali e dell'infrastruttura critica della nazione. Ogni reparto o agenzia sarà responsabile delle proprie reti, mentre il DHS guiderà questi sforzi e assicurerà un livello di sicurezza di base nel settore esecutivo civile. Tutto ciò sarà possibile grazie a una serie di azioni chiave, analizzate nel dettaglio nel sottoparagrafo seguente.[33]

2.1.(2). "Strengthening U.S. Cyber Security and Capabilities"

Lo"Strengthening U.S. Cyber Security and Capabilities" è suddiviso in tre sezioni. La prima sezione si occupa delle "Reti Federali", la seconda delle "Infrastrutture Critiche", e la terza sulla "Cybersecurity nazionale".

Sezione 1: centrata sulla gestione del rischio, chiede un rapporto dettagliato sulla modernizzazione dei sistemi informatici del governo federale. Questo rapporto sarà guidata dal Dipartimento del Commercio, il DHS, l'Office of Management and Budget (OMB), e l'Amministratore dei Servizi

[31]L' United States Strategic Command o USSTRATCOM, ha sede nella base di Air Force Base di Offatt in Nebraska. Il comando è uno dei nove comandi Usa sotto il Dipartimento della Difesa. Inoltre, è il centro di comando e controllo delle forze strategiche statunitensi e controlla le operazioni spaziali militari, le operazioni di rete informatica, le operazioni di informazione, le avvertenze strategiche e le valutazioni di intelligence nonché la pianificazione strategica globale. Il comando è responsabile sia per l'avviso precoce che per la difesa contro l'attacco missilistico e gli attacchi convenzionali a lungo raggio.

[32] Tosato F., Taufer M.(2016), *Cybersecurity, la situazione italiana e gli scenari futuri*, La relazione del Ce.S.I.

[33] Del Corno M. (2017), *La Russia fa volare le società Usa della cyber security*, il Sole 24 Ore, 17 febbraio; Homeland Security (2017), *President's Executive Order Will Strengthen Cybersecurity for Federal Networks and Critical Infrastructure,* U.S. Department of Homeland Security May 11

Generali. Vi è una forte enfasi sui sistemi condivisi / cloud. I sistemi di sicurezza nazionali devono essere conformi alle stesse raccomandazioni, ma lo sforzo di modernizzazione è separata e saranno guidati dal Segretario della Difesa e il direttore della National Intelligence.

Sezione 2: si concentra sulle infrastrutture critiche. Essa si basa sulla gestione dell'ordine esecutivo di Obama 13636 e la direttiva presidenziale 21 del 12 febbraio 2013. Ha quattro componenti:

- *Sostenere la trasparenza nel mercato.* Un rapporto esaminerà la sufficienza di politiche e pratiche federali esistenti per promuovere la conoscenza delle pratiche di gestione del rischio informatico da parte di soggetti di infrastrutture critiche,

- *Migliorare la resilienza delle infrastrutture di comunicazione di base*. Imposta un obiettivo di ridurre le minacce perpetrati da botnet. È un' importante valutazione del rischio di capacità di risposta elettrica, che coinvolge DHS, il Segretario di energia in consultazione con Stato ed enti locali, governi territoriali e le altre parti interessate,

- Un *rapporto sui rischi di sicurezza informatica,* affrontati dal Dipartimento della Difesa, e sulla c*apacità di combattimento* dell'industria della difesa, compresa la sua catena di fornitura.

Sezione 3: sulla sicurezza informatica per la Nazione, contiene sottosezioni su (a) la politica, (b) deterrenza e protezione, e (c) libertà di Internet e Governance.

"E la politica degli Stati federati a promuovere un Internet aperto, interoperabile, affidabile e sicuro che favorisce l'efficienza, l'innovazione, la comunicazione, e la prosperità economica, e rispetta la privacy, mentre la protegge contro ingerenze, frode e furto"[34]

La libertà e la governance di internet sono una risorsa che è alla base della potenza americana. Sostenere il processo multi-stakeholder risulta prezioso, per garantire l'affidabiltà e la sicurezza alle generazioni future. Nel complesso, vediamo una continuità tra questa nuova iniziativa e quelle passate. Infatti, la maggior parte dei temi e problemi individuati sono stati discussi a lungo per più di un decennio. Resta da vedere come le raccomandazioni verranno applicate nella prassi.[35] Gli investimenti di miliardi di dollari negli USA per la sicurezza informatica stanno creando una

[34] Muller M. (2017), *The Cybersecurity Executive Orders: a Tale of two Trump*, Internet Governance Project, 12 febbraio. Trump Executive Order's drafts
[35] Fonseca B., Rose J.D. (2017), *Cybersecurity in the US: Major Trends and Challenges*, 09 February

cartolarizzazione del cyberspazio. In Europa l'argomento è stato sollevato (a livello nazionale) in Germania, Francia e nel Regno Unito. In tali paesi, le strategie per affrontare la minaccia prevedono un quadro coerente con le rispettive misure nazionali di sicurezza. Inizialmente incentrate sulla mitigazione degli effetti degli attacchi informatici, peraltro con un budget di risorse insufficienti, le strategie di difesa hanno da poco cominciato a focalizzarsi sulla fase di rivelazione dei cyber criminali, radice del problema di insicurezza informatica.[36]

2.2. Regno Unito: la triade CPNI, GCHQ e NCSC

Fin dalla prima guerra mondiale, il governo britannico ha avuto ampi poteri per assicurare la sicurezza pubblica e la difesa del regno. A seguito della guerra, la legislazione sulla sicurezza, soprattutto nei casi di emergenza, è stata mantenuta.

"*.... by any persons or body of persons of such a nature and on so extensive a scale as to be calculated, by interfering with the supply and distribution of food, water, fuel, or light, or with the means of locomotion, to deprive the community, or any substantial portion of the community, of the essentials of life....*"[37]

Sebbene la legislazione possa essere cambiata nel corso degli anni, gli obiettivi fondamentali per proteggere e mantenere le infrastrutture nazionali critiche (CNI) continuano. Il quadro normativo è sostenuto dal *Civil Contingencies Act 2004 e* dalle successive implementazioni. Il lavoro del governo, in relazione al CNI, prende per lo più la forma di orientamenti non vincolanti e iniziative di buone prassi da parte del *Centre for the Protection of National Infrastructure* e il *National Cyber Security Centre* in partnership con l'industria. Il Primo Ministro ha dichiarato pubblicamente che i sistemi critici devono essere identificati, protetti e che le entità devono aver testato la capacità di risposta. Se il rischio informatico non viene gestito correttamente, il governo può intervenire "nell'interesse della sicurezza nazionale"[38].

Il suo primo documento sulla strategia britannica di sicurezza cyber, fu pubblicato nel novembre 2011. Cinque anni dopo, nel novembre 2016, è stata pubblicata la *National Cyber Security Strategy 2016* che elenca tre obiettivi chiave:

[36] Guitton C. (2013), *Cyber insecurity as a national threat: overreaction from Germany, France and the UK?,* 3 gennaio European Security, Vol. 22; Hiller J.S., Russell R.S. (2013), *The challenge and imperative of private sector cybersecurity: An international comparison*, Computer Law and Security Review

[37] Section 1(1) of the Emergency Powers Act of 1920.

[38] HM Government (2016)*, National Cyber Security Strategy*

- **Rilevamento**: per comprendere, indagare e distruggere le azioni ostili , perseguire i delinquenti e intraprendere azioni offensive nel *cyberspace*.
- **Sviluppo**: avere un'innovativa e crescente industria della sicurezza in rete, sostenuta dai programmi R&S più importanti al mondo.
- **Difesa**: avere i mezzi per difendere il Regno Unito dalle evoluzioni delle minacce informatiche e rispondere efficacemente agli incidenti. Tutto ciò per garantire che le reti, i dati e i sistemi del Paese siano protetti e resilienti.

Maggior resilienza è garantita grazie a una strategia settoriale. Infatti, l'*Office of Cyber Security and Information Assurance* (OCSIA), all'interno del *Cabinet Office,* coordina le attività svolte nell'ambito del *National Cyber Security Program* tramite i dipartimenti, le agenzie governative, le amministrazioni decentrate. Esso fornisce una direzione strategica e sorveglia i dipartimenti governativi, i quali hanno la responsabilità di garantire che nei rispettivi settori siano intraprese le adeguate misure. Infine, l'Ufficio di Gabinetto pubblica una sintesi dei piani, identificando le infrastrutture critiche all'interno dei vari settori in consultazione. L'identificazione è possibile soprattutto grazie alla cooperazione tra il *Centre for the Protection of National Infrastructure* e le organizzazioni settoriali[39]. In più il governo ha riconosciuto la necessità di lavorare attraverso organizzazioni quali gli assicuratori, i regolatori e gli investitori, per esercitare un'influenza sulle aziende e garantire la gestione del rischio informatico[40].

CPNI: Nel febbraio 2007 fu istituito il *Centre for the Protection of National Infrastructure* (CPNI) dalla fusione degli organismi predecessori: il *National Infrastructure Security Co-ordination Centre* (NISCC) e *the National Security Advice Centre* (NSAC). Il nuovo organo doveva fornire una consulenza sulla sicurezza fisica, del personale e informatica. Già NISCC esisteva per fornire consulenza alle aziende operanti nelle infrastrutture nazionali critiche, mentre NASC era un'unità all'interno di MI5, che forniva consulenza di sicurezza ad altre parti del governo. Il CPNI è al momento responsabile presso il Direttore Generale del Servizio di Sicurezza (MI5) e opera sotto il *Security Service Act* del 1989[41]. Nell'ottobre 2016, il governo ha lanciato il *National Cyber Security Center* (NCSC) come parte della sede di comunicazioni del governo, o GCHQ.

[39]Cabinet Office (2016), *Sector Resilience Plans*. Uk Cabinet Office (2012), *Cyber Security Strategy of the United Kingdom: Safety, Security and Resilience in Cyber Space*, London, UK, 5 maggio. UK Cabinet Office (2012), *The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World*, London, 5 maggio

[40]Cabinet Office (2015), *National Risk Register of Civil Emergencies*

[41]Comptroller and Auditor General (2013), *The UK Cyber-security strategy: Landscape review,* 12 febbraio

Il GCHQ: Il GCHQ è un'organizzazione britannica di intelligence e sicurezza, responsabile di fornire segnali di intelligence al governo, alle forze armate e difendere i sistemi governativi dalle minacce informatiche. La sua origine risale al 1917, per il c.d. *Zimmermann Telegraph*[42]. Tale agenzia si occupa dunque di tutte le dinamiche afferenti la *cybersecurity* e la *cyberintelligence* a beneficio sia delle istituzioni britanniche sia delle Forze Armate. Sotto il formale controllo del Joint Intelligence Committee (JIC), il GCHQ è un vero e proprio servizio che impiega oltre 6.000 persone da ambienti diversi e mantiene la Gran Bretagna sicura lavorando con i partner del Secret Service Intelligence (MI6) e MI5. La sua sede si trova a Cheltenham, con centri regionali a Scarborough, Bude, Harrogate e Manchester.[43] Il GCHQ:

- svolge un importante ruolo di supporto alle Forze Armate, collaborando con esse alla costruzione di un ambiente di comunicazione *cyber* più sicuro;
- si occupa della protezione delle industrie operanti per la Difesa (nella sede principale dell'agenzia è ospitata una cellula militare, la *Joint Cyber Unit*, con il compito di sviluppare nuove tattiche e dottrine al fine di svolgere operazioni nel *cyberspace*);
- è l'entità che si occupa di verificare e aggiornare la resilienza dell'infrastruttura cibernetica britannica, la capacità dello Stato di comunicare in maniera sicura con i propri cittadini e la protezione delle informazioni sensibili per la sovranità britannica (attraverso l'antica unità CESG, adesso NCSC)

L'agenzia dispone anche di capacità di attacco cyber che dovrebbero essere in gran parte concentrate nell'unità denominata *Joint Threat Research Intelligence Group*. Si tratta solo di capacità offensive funzionali all'attività operativa di intelligence e non di *cyberweapons* che, invece, rimangono di competenza delle Forze Armate.[44]

[42]Nel gennaio 1917 il ministro degli Esteri tedesco, Arthur Zimmermann, era preoccupato del fatto che un imminente cambiamento nella politica tedesca avrebbe potuto portare gli Stati Uniti ad aiutare gli Alleati in guerra. Era consapevole che la guerra sottomarina nell'Atlantico poteva causare l'affondamento di navi mercantili americane, spingendo gli Stati Uniti a entrare nella prima guerra mondiale a fianco degli Alleati. Così venne eleborato un piano: distrarre l'America con i problemi sul suo confine meridionale. Zimmermann inviò un telegramma all'ambasciata tedesca in America per poi trasmetterlo ad un loro ambasciatore in Messico. La speranza era che il suo messaggio persuadesse i messicani a unirsi alla guerra a fianco della Germania e bloccare il trasporto di rifornimenti americani per le potenze alleate. Nel telegramma Zimmerman promise di sostenere il Messico nella reintegrazione del Texas, Arizona e New Mexico, dopo la vittoria contro gli Alleati. Il telegramma era molto sensibile, la Germania lo aveva criptato affinchè non fosse letto da persone diverse dal destinatario. Invece fu intercettato dal Regno Unito e successivamente decifrato nella Sala 40 del Ministero della marina, la sezione dell'Ammiragliato, che aveva iniziato a produrre un intelligence per messaggi intercettati e decifrati.

[43]GCHQ Official Site, *About GCHQ,* 2017

[44] Tosato F., Taufer M. (2016), *Cybersecurity, la situazione italiana e gli scenari futuri* , La relazione del Ce.S.I.

L'NCSC: Il NCSC riunisce e sostituisce il CESG (il braccio di sicurezza delle informazioni di GCHQ), il Centro per la valutazione informatica (CCA), il Computer Emergency Response Team UK (CERT UK) e le responsabilità informatiche del CPNI. Mentre CPNI continuerà a guidare la sicurezza fisica e del personale, NCSC è ora l'autorità tecnica di *cybersecurity* leader nel Regno Unito, con la responsabilità globale del contenuto tecnico di tutti i consigli di sicurezza informatica emessi dal governo britannico. La guida rilasciata precedentemente dal CPNI, e ancora rilevante, viene archiviata sul sito NCSC.

Per le organizzazioni che dispongono di proprie reti, NCSC gestirà il partenariato di condivisione delle informazioni sulla sicurezza *cyber*. Inizialmente si concentrerà sui settori che fanno parte dell'infrastruttura nazionale critica, insieme a quelli di rilevanza economica strategica o significativa o alla fornitura di servizi pubblici chiave. NCSC offrirà un supporto limitato su un piccolo numero di organizzazioni più importanti del Regno Unito, senza offrire una linea di indagini per il grande pubblico.[45]

Dopo la Brexit, il risultato referendario che ha deliberato l'uscita del Regno Unito dall'Ue, l'Uk ha perso il ruolo di guida nel panorama europeo della sicurezza.

La sua eredità è stata raccolta senza esitazione dalle Germania.

2.3. Germania: verso la Cyber Defence Unit

A dieci anni dalla formulazione del suo precedente documento strategico, la Germania ha presentato il Libro Bianco 2016 per la sicurezza ed il futuro della Bundeswehr[46] . La pubblicazione arriva a seguito della formulazione delle nuove politiche di difesa dei maggiori Paesi europei (in documenti analoghi) e dopo il risultato referendario britannico. La tempistica del documento ed i suoi contenuti indicano che il Governo Federale Tedesco intende assumere un nuovo ruolo di leadership in Europa nel settore della Difesa[47]. Nel Libro viene ribadita la posizione tedesca, espressa alla Conferenza sulla Sicurezza di Monaco nel 2014[48]. Dalla Conferenza è scaturito il "Consenso di Monaco", artefice della "nuova edizione" del Libro Bianco: non più utilizzato per ribadire gli strumenti atti all'impiego della forza, ma portatore di una visione strategica del governo a livello internazionale. Per queste ragioni l'attuale documento strategico ha un carattere innovativo per la

[45]HM Government (2016) *National Cyber Security Strategy*
[46]The 2016 White Paper, Federal Ministry of Defence
[47]Sabatino E. (2016), Il libro bianco della Difesa tedesco: quali opportunità di cooperazione?, Istituto Affari Internazionali (IAI)
[48]2014 Munich Security Conference, MSC

politica di difesa tedesca[49].

Sul fronte interno, la Germania rappresenta inoltre uno dei Paesi più colpiti nel settore cibernetico; i dati più recenti mostrano 284 mila attacchi informatici solo nei primi tre mesi del 2017 (la Russia è stata individuata come artefice principale degli attacchi). La Germania necessita di *"... un'unità di difesa cibernetica fondamentale per la sicurezza delle infrastrutture critiche e strategiche del Paese."*[50]

BND/BSI, CERTs e BfV

La precedente struttura di *cybersecurity* e *cyberdefence* era strutturata seguendo le tradizionali competenze ministeriali.

Le operazioni SIGINT e cyber estere rientravano nelle competenze del Bundesnachrichtendienst (BND), servizio di intelligence per l'esterno della Repubblica Federale tedesca, dipendente diretamente dall'Ufficio del Cancelliere. Dal punto di vista "interno", la protezione cibernetica delle infrastrutture critiche tedesche era nelle mani del Bundesamt für Sicherheit in der Informationstechnik (BSI – Ufficio Federale per la Sicurezza Informatica), dipendente dal Ministero dell'Interno. Il BSI, autorità nazionale per la *cybersecurity*, aveva il compito di promuovere la sicurezza informatica sia a livello istituzionale sia a favore delle imprese private. Infine, una rete di Computer Emergency Response Teams (CERTs) e il Servizio di Sicurezza Interna tedesco (Bundesamt für Verfassungsschutz, BfV- Ufficio Federale per la Protezione della Costituzione) completavano l'opera.[51]

Data l'importanza crescente dell'argomento, il Ministro della difesa von der Leyen ha optato per la creazione di un apposito dipartimento.[52] Il "Dipartimento per la sicurezza informatica e cibernetica" dovrà essere reso pienamente operativo entro il 2023, ed opererà in collaborazione con il Ministero degli interni. Il bilancio dedicato alla difesa è destinato a crescere nei prossimi anni.

A tale scopo il governo tedesco pianifica lo stanziamento di un totale di 130 miliardi aggiuntivi, rispetto al livello di spesa del 2016, entro il 2030. Per l'anno 2017, a seguito dell'approvazione della sezione 14 del bilancio federale[53], gli investimenti che saranno destinati al Ministero della Difesa vedranno un aumento di 1.7 miliardi di euro rispetto al 2016[54].

---

[49]Sabatino E. (2016), Il libro bianco della Difesa tedesco: quali opportunità di cooperazione?, Istituto Affari Internazionali (IAI)

[50]Philipp Saldern, Presidente del Cyber Security Council della Germania.

[51]Federal Ministry of the Interior Bundesministerium des Innern (2012), *Cyber Security Strategy for Germany,* Berlin, Germany

[52]Abschlussbericht Aufbaustab Cyber- und Informationsraum, Bundesministerium der Verteidigung, Aprile 2016

[53]Verteidigungsausgaben sollen stark steigen, bundestag.de; Verteidigungshaushalt soll um sieben Prozent steigen, bundestag.de

[54] Sabatino E.(2016), *Il libro bianco della Difesa tedesco: quali opportunità di cooperazione?*, Istituto Affari Internazionali (IAI)

Nel caso concreto, investimenti di poco superiori al miliardo di euro sono stati utilizzati per creare una nuova struttura interforze per la *cybersecurity:* la Cyber Defense Unit.

2.3.(1). "Cyber Defence Unit"

Il 1° aprile 2017 tutte le funzioni cibernetiche sono state accentrate in una nuova struttura interforze con quartier generale a Bonn: la *Cyber defence unit*. Dal 5 aprile è entrata in azione per sovrintendere le operazioni cyber, l'infrastruttura IT, le comunicazioni militari, operative e i servizi di geolocalizzazione.

È stata inaugurata alla presenza del Ministro della Difesa della Germania, Ursula von der Leyen, con un team di 13.500 effettivi su tutto il territorio della Germania. Il comando è stato assegnato al generale Ludwig Leinhos e raggiungerà la piena operatività nel 2021.[55]

La Germania da un lato ha dato prova di mostrarsi più attiva sul terreno della sicurezza informatica strategica, dall'altro mostra uno scambio di informazioni tra Lander e amministrazioni locali pieno di ostacoli burocratici. La nuova *Cyber defence unit* è ancora in fase di perfezionamento, necessitando di altri 1000 'soldati' e 800 amministrativi.

"L'unità dovrebbe essere sempre autorizzata dal Parlamento per operare in termini offensivi", ha dichiarato Konstantin von Notz del Partito dei Verdi, lamentando scarsa trasparenza da parte del Governo sulla faccenda.[56] Restano comunque evidenti i progressi fatti nel settore, per garantire un efficacie apparato informativo.

A tal proposito è necessario ricordare la "legge sulla sicurezza IT", pubblicata nella Gazzetta Ufficiale federale il 24 luglio 2015 e entrata in vigore il giorno successivo. Questa legge mira a migliorare il livello di sicurezza IT di alcune società, a proteggere i cittadini online, e ottenere ammende amministrative fino al valore di 100.000 euro (in caso di grave violazione). La norma non ha ottenuto grande visibilità a livello europeo a causa della discussa Direttiva NIS, che non era ancora stata approvata.

Sul piano nazionale ha invece operato una vera e propria rivoluzione: ha modificato diverse altre leggi, tra cui la legge sulla telecomunicazione (TKG) e la legge Telemedia (TMG). Pertanto, dal 25 luglio 2015, i fornitori di servizi di telecomunicazione e i fornitori di servizi della società dell'informazione[57](essenzialmente fornitori di contenuti e hosting) devono rispondere a maggiori requisiti per quanto riguarda la protezione dell'utente Dati e dei loro sistemi IT. I fornitori di

[55] Tosato F., Taufer M.(2016), *Cybersecurity, la situazione italiana e gli scenari futuri*, La relazione del Ce.S.I.

[56]Agenzia Nova(2017), "Speciale Ict: cyber security, la Germania attiva l'unità di cyber difesa nazionale", 13 aprile

[57]Ai sensi del diritto tedesco / UE, un "servizio della società dell'informazione" è un qualsiasi servizio normalmente previsto per remunerazione a distanza, tramite mezzi elettronici e su richiesta individuale di un destinatario dei servizi. Comprende, ad esempio, operazioni bancarie online e acquisti online.

telecomunicazioni sono inoltre soggetti a obblighi di notifica estesi.[58]

2.4. Francia: l'ANSSI per un approccio pubblico-privato.

"Garantire la *sécurité des systèmes d'information* (SSI) con una tecnologia francese alla stregua del Pentagono statunitense". Il Libro bianco sulla difesa e la sicurezza nazionale 2008 ha lanciato questa sfida, identificando l'SSI come fondamentale per la resilienza della Francia. A tal fine, è stata avviata la cooperazione tra governo e industria, per vedere l'emergere di soluzioni valide[59]. Inizialmente, la *Direction Générale de la Sécurité Extérieure* (DGSE), il servizio di intelligence francese per la sicurezza esterna (dipendente dal Ministero della Difesa), era l'unica entità francese in grado di condurre operazioni cyber di tipo offensivo a livello strategico. La sua importanza crebbe dopo la pubblicazione del Libro Bianco 2008 e, ancor di più, nell'edizione 2013. Successivamente, la necessità di creare un approccio integrato pubblico-privato, portò alla nascita dell' *Agence Nationale de la Sécurité des Systèmes d'Information* (ANSSI).

L'ANSSI: L'ANSSI è l'autorità nazionale per la sicurezza e la difesa dei sistemi informatici ed ha il compito di individuare, contenere e rispondere ad attacchi cibernetici. Sviluppa costantemente dottrine operative, disponendo di 500 agenti (aumentati a 600 alla fine del 2016). Al momento è sottoposta al Segretariato Generale della Difesa e della Sicurezza Nazionale e dipendente direttamente dal Primo Ministro[60]. Le competenze dell'ANSSI comprendono tutta la sfera dell'infrastruttura civile e statale francese, ad eccezione delle Forze Armate. Il comparto militare è invece sotto la Direzione Generale degli Armamenti (DGA), che dispone di un apposito comando cyber (COCYBER). La collaborazione tra le due strutture, l'ANSSI e il DGA, è totale. Lo dimostra la presenza del Centro di Analisi per la Lotta Informatica Difensiva (CALID) delle Forze Armate nella medesima struttura dell' ANSSI. In un momento in cui il dominio cyber è essenziale per il sostegno dell'autonomia politica e strategica del Paese, l'Agenzia ha ampliato le capacità di difesa e resilienza *cyber* francese.[61]

[58]Federal Office for Information Security (2016), *25 years of the BSI: more security, thanks to trasparency,* Security in Focus, BSI Magazine

[59]D'Elia D.(2014), *La cybersécurité: de la représentation d'un bien public à la nécessité d'une offre souveraine* ,*Sécurité et stratégie*, vol.19, pp. 72-80.

[60]ANSSI, Agence nationale de la sécurité des systèmes d'information, Official Website France:Secrétariat général de la défense et de la sécurité nationale *Défense et Sécurité des Systèmes D'information: Stratégie de la France,* 2012 Paris; France:Secrétariat général de la défense et de la sécurité nationale *Information Systems Defence and Security: France's Strategy,* Paris, 2012

[61]Tosato F., Taufer M. (2016), *Cybersecurity, la situazione italiana e gli scenari futuri*, La relazione del Ce.S.I.

2.4.(1). Cybercom

Cybercom è la nuova unità militare specializzata nel *cyberwarfare*. È stata istituita per incrementare la capacità di attacco e difesa informatica del paese. La struttura arriverà ad impiegare, entro il 2019, 2.600 esperti di sicurezza cibernetica, e avrà un finanziamento iniziale di 2,1 miliardi di euro. Il Capo di Stato maggiore della Difesa francese lo gestirà direttamente; questa decisione risente della nuova dottrina cibernetica, secondo cui un cyberattacco potrebbe essere considerato un atto di guerra. La risposta dovrà dunque essere appropriata

"Le nostre capacità di risposta devono permettere di danneggiare i sistemi e le reti dei nostri nemici. Sospendendo i servizi o neutralizzandoli definitivamente". [62]

Tali misure derivano dal terrore di ripetere in Francia quanto accaduto nelle ultime presidenziali Usa. Le presidenziali francesi hanno avuto luogo il 23 aprile e il 7 maggio del 2017 e fino all'ultimo si è temuto tentativi di interferenze informatiche. Di conseguenza sono state poste una serie di contromisure per scongiurare rischi di hacking o di disinformazione, di cui si è occupata l'Agenzia Nazionale per la Cybersecurity (ANSSI). Tuttavia, le sue capacità limitate hanno posto seri dubbi sul risultato. Da qui nasce l'esigenza di un centro più grande e meglio finanziato, che in futuro garantisca al 100% la sicurezza informatica del paese. Il Cybercom venne presentato lo scorso ottobre, e rappresenta l'evoluzione della strategia di cybersecurity della Francia.[63] L'evoluzione era già cominciata con il Cyber Defence Pact per il triennio 2014-2016, per cui la Francia ha continuato a investire e a espandere queste capacità. Infine, con la strategia per la Sicurezza digitale, "la digitalizzazione" della società francese ha accelerato, con una crescita senza sosta dei servizi, prodotti e impieghi. La transizione digitale, favorendo l'innovazione e la crescita, è diventata una questione nazionale. Per scongiurare il *cybercrime*, lo spionaggio, la propaganda, il sabotaggio e l'eccessiva esposizione di dati personali, l'unica soluzione è stata una risposta collettiva e coordinata, basata su obiettivi strategici. Gli obiettivi strategici francesi sono divisi in 5 aree[64]:

1. interessi fondamentali, difesa e sicurezza dei sistemi e delle infrastrutture critiche dello stato, crisi di cybersecurity di grandi dimensioni;

2. digital trust, privacy, dati personali e cybermalevolence;

[62]Citazione del Ministro della Difesa francese, Jean-Yves Le Drian

[63]L'esistenza del Cybercom fu rivelata dal premier Manuel Valls in occasione della conferenza dell'ANSSI

[64]Valls M., *Stratégie nationale pour la sécurité du numérique.* "La stratégie nationale pour la sécurité du numérique" è elaborata dall'insieme dei ministri, sottoscritta dal Segretario Generale della difesa e della sicurezza nazionale, e approvata dal Primo Ministro, ai sensi del *7° de l'article R*1132-3 du code de la défense*

3. aumento della consapevolezza, formazione iniziale ed educazione continua;

4. ambiente del business della tecnologia digitale, politica industriale, export e internazionalizzazione;

5. autonomia digitale strategica e stabilità del cyberspazio.

La legislazione vigente, sia nel caso della Francia che della Germania, dovrà adattarsi alla nuova legislazione UE, in vigore dal 2018, i cui capisaldi sono: la *Network and Information Security Directive (NIS Directive)*, il *General Data Protection Regulation (GDPR)* e il *Payment Services Directive 2 (PSD 2).*

- La direttiva NIS è la base della politica legislativa dell'Unione europea in materia di sicurezza, stabilendo gli obblighi di sicurezza della rete per gli operatori di servizi essenziali (selezionati dai singoli Stati membri) e dei fornitori di servizi digitali. Gli Stati membri dell'UE avranno tempo fino al 10 maggio 2018 per adottarla e attuarla.

- Il GDPR rappresenta una grande revisione della legislazione europea in materia di protezione dei dati. Le sue disposizioni fondamentali impongono obblighi di sicurezza direttamente ai controllori e ai processori dei dati personali e introducono obblighi di segnalazione alla violazione dei dati personali. Poiché è un regolamento, il GDPR avrà effetto diretto nei Paesi Membri il 25 maggio 2018.

- Il PSD 2, infine, è una direttiva europea specifica del settore che impone i requisiti di sicurezza della rete per i fornitori di servizi di pagamento (PSP), incluse le banche. La direttiva deve essere attuata dagli Stati membri entro il 13 gennaio 2018. Le organizzazioni interessate saranno obbligate a denunciare i casi di sicurezza ai regolatori. Se un incidente di sicurezza potrebbe influenzare gli interessi finanziari di un cliente, è anche necessario notificare a questi clienti.

La Francia, attraverso la pianificazione militare *Act 2013*[65] e la strategia di *Digital Government* adottata nell'ottobre 2015[66], ha fatto progressi nella lotta alla criminalità informatica. Pertanto non avrà difficoltà nella trasposizione della direttiva NIS, operazione affidata all' ANSSI.

[65]Il governo ha approvato l'articolo 22 della legge n. 2013-1168 del 18 dicembre 2013 (la "legge di programmazione militare") che prevede diversi obblighi applicabili a operatori di grande importanza ("VIO") comparabili a quelli imposti dalla direttiva NIS riguardo agli operatori di infrastrutture critiche.

[66]Il giorno 16 ottobre 2015 il Primo Ministro francese illustrò la strategia nazionale di sicurezza digitale. Ribadì la determinazione del governo a continuare gli sforzi per affrontare le minacce provenienti dal cyberspazio e sottolineò una strategia di " equilibrio tra le considerazioni di sicurezza e il dinamismo economico".

In tutti i principali Paesi partner dell'Italia "l'amministrazione *cyber"* sta passando da un contesto di collaborazione tra diversi dicasteri all'individuazione di un'autorità centrale.Tale autorità sarà responsabile della cybersecurity e farà parte del mondo dell'intelligence o della sicurezza interna. Sono le ripercussioni in termini di sicurezza politica, economica e militare di incidenti cyber di rilievo (vedi "Approfondimento" p.34) che hanno portato a questa scelta.

Anche in Italia è in corso questa trasformazione, nonostante un approccio iniziale completamente diverso.

Capitolo 3.La risposta italiana

La prima legge italiana in materia di "sicurezza informatica" risale a 24 anni fa. La legge n.547/1993 inserisce disposizioni per l'individuazione del *Cybercrime,* analizzando in maniera piuttosto ampia l'argomento. Questa peculiarità rappresenta il problema fondamentale della legge, che va ad analizzare quattro "macro-aree" senza definirne in modo chiaro i contorni. Le aree prese in esame sono la frode informatica, la falsificazione, la lesione dell'integrità sistemica e dei dati e la violazione della riservatezza delle comunicazioni. Il settore "militare", la *cyberdefence*, non venne considerato rilevante. Il 23 novembre 2001, con la redazione della Convenzione di Budapest sul *Cybercrime,* verrà modificata la legge preesistente. La convenzione entrerà in vigore in Italia 7 anni dopo, con la l.n.48/2008. Il quadro giuridico si complica, rendendone difficile l'interpretazione e, di conseguenza, la prassi. Al momento le innovazioni tecnologiche, la crescente interdipendenza tra le infrastrutture critiche e l'ingerenza sempre maggiore del Web nella vita quotidiana hanno posto lo Stato italiano in una posizione scomoda, tra vantaggi e pericoli sempre nuovi.
La *Cybersecurity* non può più limitarsi a leggi generiche e astratte; è stato necessario stabilire un piano d'azione. In questo contesto nasce Il Quadro Strategico per la Sicurezza dello spazio Cibernetico.

3.1. Quadro Strategico Nazionale per la Sicurezza dello spazio Cibernetico

Il "Quadro Strategico Nazionale per la Sicurezza nello spazio Cibernetico" è un documento elaborato dal Tavolo Tecnico Cyber (TTC), istituito il 3 aprile 2013, che opera presso il Dipartimento Informazioni per la Sicurezza.[67]
Come precedentemente sottolineato, assume un'importanza crescente con lo sviluppo del *cybercrime*, in quanto fissa gli indirizzi strategici per combatterlo.
Tali indirizzi sono[68]:

[67]Presidenza del Consiglio dei Ministri (2013), *Quadro Strategico Nazionale per la Sicurezza nello Spazio Cibernetico*
[68]Ibidem

1) Un approccio integrato per migliorare capacità tecnologiche, operative e di analisi degli attori istituzionali. In modo che questi possano mettere a punto azioni idonee contro i rischi di una minaccia multidimensionale.	**4)** Un maggiore coinvolgimento del mondo della ricerca e delle università, promozione e la diffusione della sicurezza cibernetica tra i cittadini e all'interno delle istituzioni, per accrescere la consapevolezza del cyber-risk
2) La garanzia di business continuity, compliance con standard e protocolli di sicurezza internazionale per potenziare la capacità di difesa delle Infrastrutture Critiche Nazionali e degli attori strategici	**5)** Il rispetto delle normative nazionali e internazionali, per rafforzare la capacità di contrasto alle attività e ai contenuti illegali online.
3) Di preservare la proprietà intellettuale e la capacità tecnologica innovativa dell'Italia tramite l'incentivazione della cooperazione tra istituzioni e imprese nazionali.	**6)** Che l'Italia si impegni a mantenere un approccio integrato, nell'ambito della c*ybersecurity*, con gli altri Paesi, nelle organizzazione di cui è parte.

Raggiungere questi obiettivi richiede delle specifiche linee d'azione, le quali sono definite nel "Piano Strategico Nazionale per la Sicurezza dello spazioCibernetico" e coordinate dal CIRS. Il piano d'azione prevede:

- Lo sviluppo delle capacità del Sistema di Informazione per la sicurezza della Repubblica, delle Forze Armate e delle Autorità preposte alla Protezione e alla Difesa Civile.
- L'Incremento delle capacità di monitoraggio e analisi preventiva, tramite lo sviluppo delle capacità di pianificazione e condotta delle operazioni militari.
- L'identificazione di un'Autorità nazionale NIS (Network and Information Security) che cooperi con le omologhe Autorità degli altri Paesi membri dell'UE e con la Commissione Europea.
- Il potenziamento delle partnership pubblico-privato, soprattutto per la condivisione delle informazioni, che sarà agevolata dalla creazione di tavoli istituzionali congiunti con operatori del settore, l'organizzazione di periodiche esercitazioni, l'obbligatorietà della segnalazione di incidenti informatici e la definizione di procedure operative per lo scambio informativo.
- La definizione di un linguaggio di riferimento unico, chiaro e condiviso, predisponendo questionari atti ad individuare il livello di competenza e consapevolezza di tutti gli attori coinvolti.

- Realizzare campagne di formazione, addestramento, informazione e sensibilizzazione a beneficio del personale della Pubblica Amministrazione.
- Migliorare e sperimentazione degli strumenti di simulazione, addestramento e training on the job e introdurre moduli di formazione nelle scuole di ogni grado per promuovere la cultura del Cybersecurity.
- Rafforzare dei rapporti di cooperazione e collaborazione con le Organizzazioni internazionali delle quali l'Italia è parte, con i Paesi alleati e con le Nazioni amiche, soprattutto tramite regole comuni a livello globale e una capacità di resilienza cibernetica comune a livello europeo.
- Sviluppo di un capacity-building con i Paesi "Strategici" a livello bilaterale.
- Realizzazione della piena operatività del CERT nazionale, sulla base del modello cooperativo pubblico-privato, tramite azioni di sensibilizzazione, e di una piattaforma di coordinamento tecnico e funzionale tra tutti i CERT.
- Piena operatività del CERT-PA, come punto di riferimento delle pubbliche amministrazioni. (anche livello europeo ed internazionale).
- Creare un CERT della Difesa che segue le evoluzioni tecnico-funzionali e procedurali del NCIRC.
- Garantire la continua efficacia delle misure di sicurezza cibernetica, adattando la legislazione all'evoluzione digitale.
- Individuazione di standard per la sicurezza di prodotti e sistemi che implementano protocolli di sicurezza.
- Definizione di piani per la sicurezza di reti e sistemi tramite la cooperazione con il comparto industriale. In particolare, predisporre servizi pubblici di assistenza e collaborazione a supporto delle piccole e medie imprese, creare una supply chain virtuosa con il ricorso a meccanismi di audit, sui sistemi e sui fornitori per incentivare la verifica di affidabilità.
- Potenziamento le attività di R&S per settori strategici delle F.A.
- Coerenza tra le comunicazioni strategiche e le attività condotte nell'ambiente cibernetico, attraverso strategie di dissuasione nei confronti di potenziali avversari.
- Attribuzione di adeguate risorse umane, finanziamento per innovazioni tecnologiche e logistiche ai settori strategici delle P.A.

- Implementazione di un sistema integrato di Information Risk Management nazionale per realizzare una struttura di prevenzione, di identificazione per potenziali rischi e di produzione di politiche di riferimento per la gestione del rischio[69].

Ogni indirizzo presuppone un'organizzazione minuziosa dal punto di vista nazionale e un approccio sinergico con la comunità internazionale.

A tale scopo agisce l'Unione Europea, che in un biennio ha rafforzato la legislazione in materia *cyber,* imponendo innovazioni rilevanti agli Stati membri.

3.2. La Direttiva "Network and Information Security"

Il 6 luglio 2015 è stata approvata la Direttiva NIS (Network and Information Security), la quale elenca i requisiti minimi di Sicurezza Informatica all'interno dei Paesi Membri dell'Unione.

Il comunicato stampa emesso dal Parlamento Europeo recita:

"Il 6 luglio i deputati hanno approvato la Direttiva per la sicurezza delle reti e dell'informazione, che definisce un approccio comune dell'UE in materia di sicurezza informatica. Essa elenca i settori critici come l'energia, i trasporti e il settore bancario in cui le imprese dovranno assicurare di essere in grado di resistere ad un attacco informatico. Esse saranno obbligate a segnalare gravi incidenti di sicurezza alle Autorità nazionali, mentre i fornitori di servizi digitali come Amazon e Google dovranno notificare loro eventuali attacchi importanti. Inoltre, la direttiva mira a rafforzare la cooperazione in materia di sicurezza informatica tra i Paesi dell'UE."[70]

Gli Stati membri avranno 21 mesi di tempo per adeguarsi alla direttiva NIS e 6 mesi supplementari per identificare gli operatori dietro le infrastrutture critiche nazionali, di cui ogni Stato sarà responsabile.

Il pilastro della direttiva NIS è la condivisione delle informazioni all'interno dell'UE. Perciò le organizzazioni saranno obbligate a segnalare gravi incidenti informatici ai CSIRT (Computer Security Internet Response Team) nazionali. La collaborazione tra gli Stati sarò facilitata dall'ENISA, l'Agenzia europea per la sicurezza delle reti e dell'informazione.[71]

Il governo italiano ha recepito la Direttiva Nis con il Decreto Legislativo del 17 febbraio 2017.

Quest'ultimo sostituirà il decreto del Presidente del Consiglio dei Ministri del 24 gennaio 2013, grazie a cui era nato il "Quadro Strategico Nazionale".

Il nuovo decreto prevede di "ricondurre a sistema e unitarietà le diverse competenze coinvolte nella gestione della crisi", dal momento che il quadro legislativo preesistente suddivideva le varie

[69]Presidenza del Consiglio dei Ministri (2013), *Quadro Strategico Nazionale per la Sicurezza nello Spazio Cibernetico*
[70]GUUE, "direttiva UE 2016/1148", Parlamento Europeo e Consiglio
[71]Ibidem

funzioni di cyber sicurezza tra molteplici soggetti istituzionali.

Con la direttiva 2016/1148 viene alla luce un'esigenza di "semplificazione e razionalizzazione nell'architettura istituzionale", per ragioni di maggiore trasparenza ed efficienza.[72]

3.3. Decreto del Presidente del Consiglio dei Ministri, 17 febbraio 2017

Il D.p.C datato 17 febbraio 2017 rappresenta un importante traguardo per l'Italia.

Il giorno seguente alla sua approvazione, si svolse a Palazzo Chigi una riunione del Cisr, nel corso della quale è stato approvato un programma nazionale per la sicurezza cibernetica e rafforzato il suo ruolo.

Il nuovo programma si articola in diverse fasi, e coinvolge un numero limitato di attori: il CIRS, il DIS, il NSC e il Presidente del Consiglio. Questi sono chiamati a svolgere mansioni delicate e fondamentali per la *Cybersecurity.*

CIRS: Il Comitato Interministeriale per la Sicurezza della Repubblica è presieduto dal Presidente del Consiglio, dai ministri degli Affari Esteri, dell'Interno, della Difesa, della Giustizia, dell'Economia, delle Finanze, dello Sviluppo Economico, per la Semplificazione e la Pubblica Amministrazione.Con la nuova direttiva europea, al Cirs spetterà il ruolo principale: emanare direttive per innalzare il livello di sicurezza informatica. Nel suo lavoro sarà supportato da un organismo collegiale di coordinamento, detto Cisr tecnico, presieduto dal direttore generale del Dis e composto dai dirigenti di vertice delle amministrazioni rappresentate.

DIS: Il direttore generale del Dis, attualmente il prefetto Alessandro Pansa, dovrà definire le linee d'azione per innalzare i livelli di sicurezza dei sistemi e delle reti. Inoltre, spetterà a lui individuare i più adeguati supporti tecnologici e valutare ed eliminare le eventuali vulnerabilità del sistema.

Con il Dis sarà integrato il Nucleo Sicurezza Cibernetica (Nsc).

NSC: Il Nucleo per la sicurezza cibernetica svolge la funzione fondamentale di raccordo tra le varie dimensioni:

- coordina tutti i ministeri tra loro;
- intrattiene le relazioni tra il governo e l'Agid, l'Agenzia per l'Italia Digitale;
- costituisce un punto di riferimento nazionale per i rapporti con l'Onu, la Nato, l'Ue, altre organizzazioni internazionali ed altri Stati.

[72]GU Serie Generale n.87 del 13-4-2017, "Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali". (17A02655) Decreto del Presidente del Consiglio dei Ministri 17 febbraio 2017

Ciò è possibile perché il Nsc riceve dall'estero le segnalazioni di eventi cibernetici e dirama gli allarmi alle amministrazioni e agli operatori privati. Si muove inoltre in campo preventivo, promuovendo la pianificazione della risposta ed elaborando, in raccordo con il Mise e l'Agid, le simulazioni di eventi di natura cibernetica. Queste misure permettono di valutandone dimensioni, intensità e natura delle potenziali minacce, per fornire alle singole amministrazioni competenti in via ordinaria di fronteggiare l'attacco.

Il Nsc non è più alle dipendenze dell'Ufficio del Consigliere militare di Palazzo Chigi. Essendo stato integrato nel Dis, può informare tempestivamente il Presidente del Consiglio e il Cirs tramite il direttore generale del Dis, e redigere appositi report sullo stato di attuazione delle misure di coordinamento da trasmettere al 'Cisr tecnico'.

Infine al *Presidente del Consiglio dei ministri* è affidata l'alta direzione e la responsabilità generale della politica dell'informazione per la sicurezza. Egli svolge le proprie funzioni coordinando le politiche dell'informazione per la sicurezza; impartendo direttive e, sentito il Cisr, emanando le disposizioni necessarie per l'organizzazione e il funzionamento del Sistema.[73]

Nonostante la rilevanza di tali misure, lo scenario italiano sulla sicurezza informatica si è rivelato critico. Tale affermazione deriva dall'analisi svolta dal Rapporto Clusit 2017, che delinea le numerose sfide che l'Italia deve ancora affrontare.

3.4. Rapporto Clusit 2017

Il Rapporto Clusit è il risultato della cooperazione tra centinaia di esperti dell'Associazione per la Sicurezza Informatica Italiana con enti nazionali pubblici e privati. [74]

Secondo il rapporto Clusit sulla sicurezza ICT dell'anno 2017, il 2016 è stato un anno critico per la sicurezza informatica italiana. L'Italia figura nella Top Ten dei Paesi più colpiti al mondo dalle minacce cyber, nello specifico al nono posto nel ranking mondiale della Kaspersky Lab.[75] L'elevata quantità di attacchi subiti e il numero considerevole di vittime colpite dipendono dal volume degli scambi economici nazionali e nel know-how nazionale in settori specifici. Infatti, nel panorama competitivo globale, molte economie emergenti sono interessate a sottrarre il patrimonio tecnologico e industriale italiano, ricorrendo ai numerosi portali messi a disposizione dalla rivoluzione 2.0 e all'espansione dell'arena digitale. [76]

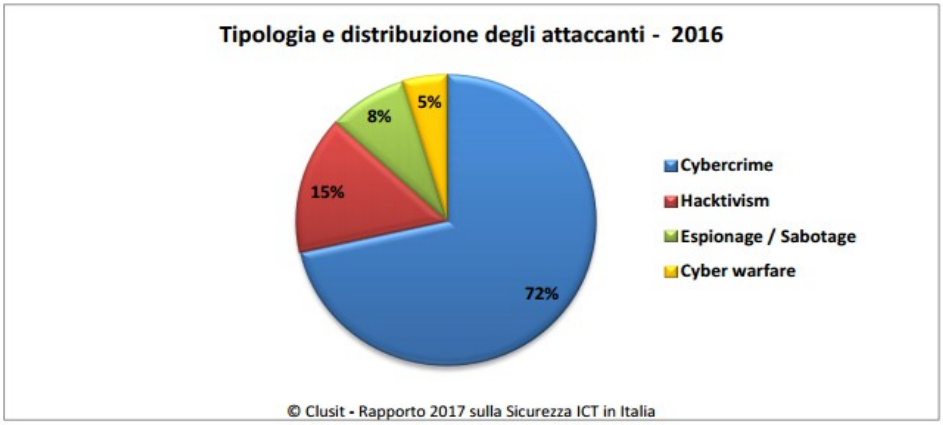
[73]GU Serie Generale n.87 del 13-4-2017, "Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali". (17A02655) Decreto del Presidente del Consiglio dei Ministri 17 febbraio 2017

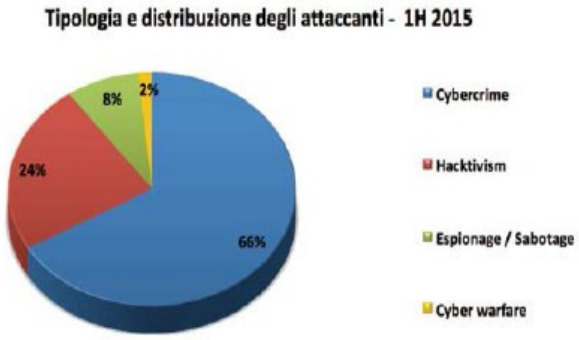
[74]Belviolandi S. (2017), *Rapporto Clusit 2017 sulla sicurezza IT e Cybercrime: l'Italia vittima dei Ransomware*, 22 febbraio

[75]Tosato F. , Taufer M. (2016), *Evoluzione del Quadro di sicurezza cibernetica nazionale in prospettiva futura*, Relazione C.e.s.i.

[76]Ibidem

Dal punto di vista quantitativo, sono stati calcolati ben 1050 mila attacchi globali, con conseguenze disastrose in ambito economico e personale.[77] Per quanto riguarda la tipologia di attacco, è interessante comparare la situazione del 2016 con l'anno precedente. Il rapporto Clusit mostra dei grafici particolarmente esplicativi:





Come è evidenziato, la maggior parte degli attacchi è classificabile come *Cybercrime* (estorsione di denaro e informazioni), su cui si concentrano gli sforzi in materia legislativa. Mentre quest'ultimo va crescendo l'*Hacktivism* diminuisce, lasciando il posto alla nuova *Cyber warfare*, la guerra delle informazioni.

[77] Clusit (2017), *Rapporto Clusit 2017 sulla sicurezza ICT in Italia*

CONCLUSIONI

Un contesto cibernetico sempre più sfidante, richiede un adeguamento progressivo delle infrastrutture di *cybersecurity* e *cyberdefense*. Dopo aver analizzato le varie scelte organizzative, sia straniere che italiane, è necessario confrontarle.

Prima di tutto, all'estero prevale una visione di "comprehensive approach", ispirata molto più alla Defense che alla Security. In tutti i principali Paesi partner dell'Italia si sta passando da un contesto di collaborazione tra diversi dicasteri, all'individuazione di un'autorità centrale responsabile della cybersecurity. Tale autorità non sarà un'istituzione qualsiasi: farà parte del mondo dell'intelligence o della sicurezza interna. Questa scelta è giustificata dalle severe ripercussioni in termini di sicurezza politica, economica e militare, causate da incidenti cyber di rilievo. Ciò ha costretto anche l'Italia a operare questa trasformazione. Con il d.p.c del 17 febbraio 2017, il ruolo del MISE come autorità nazionale di regolamentazione in materia di sicurezza e integrità delle reti di comunicazione elettronica (sancito dal DPCM 24 gennaio 2013) viene riconsiderata. Ferme restando le attuali competenze di AISE, AISI e del RIS Difesa in materia di SIGINT, il Centro Studi Internazionali prospetta la creazione di un ulteriore organismo, un terzo servizio di Intelligence e Sicurezza Cibernetica alle dipendenze del DIS, effettivamente responsabile della sicurezza e dell'integrità dell'infrastruttura cibernetica del Paese. Questa nuova entità avrebbe come scopo primario assicurare la sicurezza della rete informatica, dei software e dell'hardware in uso da parte delle varie articolazioni dello Stato e poi, in partnership con le realtà private, delle infrastrutture critiche nazionali e della supply-chain legata alla Difesa. La risposta nazionale e internazionale dovrebbe essere attivata tramite un contatto diretto con il Nucleo per la Sicurezza Cibernetica (NSC). La necessità di protezione delle infrastrutture critiche istituzionali e civili da minacce sempre più sofisticate e organizzate (schemi da operazione militare) richiede un servizio del genere. Gli strumenti tipici dell'intelligence, monitorerebbero e contrasterebbero operazioni di ricognizione cibernetica, utilizzate per la preparazione di un potenziale attacco. La stretta collaborazione con le aziende e il mondo dell'accademia sarebbe il catalizzatore, lo strumento finale per l'adozione di standard condivisi e best practices nella prevenzione del cyber spionaggio a fini economici. Tali misure migliorerebbero le capacità di resilienza nazionali.

Passando sul fronte militare delle *cyber* armi, l'Italia si basa sui principi elencati nel Libro Bianco per la Sicurezza Internazionale e la Difesa. Gli altri Paesi stanno invece sviluppando armi offensive in un'ottica di deterrenza contro potenziali aggressori, ben consapevoli che la sola prospettiva di difesa cibernetica non è sufficiente a scoraggiare la minaccia. È impossibile, dal punto di vista

tecnico ed economico, proteggere tutti i potenziali bersagli. Di conseguenza, sarebbe opportuno procedere allo stesso modo, implementando nel più breve tempo possibile il Comando Operativo Cibernetico Interforze (COCI), struttura alle dipendenze dello Stato Maggiore della Difesa (SMD), con lo scopo di proteggere le infrastrutture critiche della Difesa. Le sue funzioni sarebbero svolte In collaborazione con il nuovo servizio di Intelligence e Sicurezza Cibernetica, il COCI dovrebbe procedere allo sviluppo e l'utilizzo di *cyber-weapons* nazionali. Secondo il Ce.S.I., l'utilizzo di "armi cibernetiche" e la capacità di creare danni fisici deve restare una competenza esclusiva delle Forze Armate. Ciò mantiene il sistema di pesi e contrappesi stabilito dalla nostra Costituzione[78] .

In conclusione, rendere l'Italia un paese competitivo politicamente, economicamente e militarmente nello scenario mondiale, richiede di affinare la struttura nazionale di *cybersecurity*, in linea con quella dei principali alleati. Il decreto del 17 febbraio 2017 rappresenta il punto di partenza di questo tortuoso cammino, l'inizio dell'avventura italiana nel *cyberspace.*

[78]Tosato F. , Taufer M. (2016), *Evoluzione del Quadro di sicurezza cibernetica nazionale in prospettiva futura*, Relazione C.e.s.i.

Approfondimento: Cyber Attacco 12 Maggio 2017

Il 12 maggio 2017 sarà sempre ricordata come una data significativa per la *cybersecurity* mondiale. Quello stesso giorno, i ministri delle finanze del gruppo G7 si erano riuniti per discutere della minaccia di attacchi informatici, per individuare le vulnerabilità e valutare le misure di sicurezza. Venne inolte portata a termine la Locked Shields 2017 in Estonia, che con venticinque nazioni, 800 partecipanti e più di 2000 attacchi virtuali, rappresenta la più grande esercitazione al mondo di Cyber Defense. La simulazione è organizzata dalla Nato Cooperative Cyber Defence Centre of Excellence di Tallinn, con lo scopo di addestrare gli esperti del campo della sicurezza dei sistemi informatici nazionali. Quello stesso giorno però non si è svolta solo una simulazione; si è verificato un reale atto di pirateria informatica su scala globale.

Il virus ha un nome eloquente, Wannacry ("Voglio piangere"), e venerdì 12 maggio si è riprodotto per ben 36mila volte in tutto il mondo, dall'Europa agli Stati Uniti, arrivando fino alla Russia e a Taiwan. È un ransomware, un tipo di malware che prende in ostaggio pc e smartphone e poi chiede agli utenti il pagamento di un riscatto (ransom) in bitcoin. Il riscatto richiesto ammontava a circa 300 dollari (230 sterline)[79]. Secondo la società di sicurezza informatica Avast e il Kaspersky Lab, sono stati colpiti ben 74 Paesi. Nel mirino sono finiti i sistemi informatici di migliaia di aziende e organizzazioni, come quello del servizio sanitario nazionale del Regno Unito e della compagnia spagnola Telefonica. La propagazione del virus è stata fermata dal primo costruttore automobilistico di Francia, Renault, bloccando alcuni impianti di produzione.[80]

Come ha avuto origine? Secondo quanto affermato dal presidente di Microsoft, Brad Smith, la causa dell'attacco è il furto di dati segreti dell'Agenzia per la sicurezza nazionale (NSA) degli Stati Uniti. L'attacco sarebbe stato sferrato utilizzando EternalBlue, una cyber arma trafugata negli scorsi giorni alla Nsa dal gruppo hacker Shadow Brokers. I software di spionaggio utilizzati dalla Nsa sono stati quindi utilizzati per infettare migliaia di computer a livello globale. I ransomware sono tra i virus informatici più potenti. L'attacco di venerdi è solo l'ultima di una lunga serie di violazioni: circa un anno fa l'ospedale di Los Angeles dovette pagare quasi 20mila euro per sbloccare e-mail e altri file sottratti dal virus, mentre a San Francisco i cybercriminali tennero in ostaggio per alcuni giorni i sistemi informatici della metro, fino ad ottenere 70mila dollari per ritornare alla normalità.

Smith ha inoltre riaperto il dibattito sui servizi di intelligence dei governi. Quest'ultimi dovrebbero equilibrare il loro desiderio di tenere segreti i software d'intrusione, per condurre lo spionaggio e la

[79]Camodeca D. (2017), *Attacco Cibernetico su scala mondiale, riscatto in Bitcoin*, 13 maggio; BBC News (2017), *Cyber-attack: Europol says it was unprecedented in scale*, 13 maggio; Camodeca D. (2017), *Attacco Cibernetico su scala mondiale, riscatto in Bitcoin*, 13 maggio

[80]Il Fatto Quotidiano (2017), *Pirateria informatica, Europol: Attacco hacker senza precedenti? Serve indagine. Renault blocca fabbriche in Franci*a

guerra informatica, con la necessità di far conoscere alle aziende del settore le proprie manchevolezze. Il presidente della Microsoft ha accusato l'Nsa americana, colpevole di aver diffuso online strumenti di hacking, che sfruttano "bug" dei sistemi operativi senza informare le aziende produttrici. Questo sistema si ritorce contro tutti, permettendo agli hacker di colpire senza difese efficaci da parte delle aziende. I responsabili della National Security Agency americana si giustificano ribadendo che EternalBlue è uno strumento sviluppato per individuare potenziali criminali o stati responsabili di attacchi informatici. Inoltre, la cyberarma sfrutta una vulnerabilità presente in tutte le versioni più diffuse di Windows, ma la falla avrebbe dovuto essere risolta dalla stessa Microsoft con un update, chiamato MS17-010.I, che risale allo scorso marzo[81].

Chi è il colpevole? Symantec (Usa) e Kaspersky (Russia) adombrano l'ipotesi di un'azione nord coreana. A favore di questa tesi sono stati specificati alcuni fattori significativi.

Il primo è che "WannaCry" ha al suo interno codici ("comandi" che vengono fatti eseguire al computer infettato) che risalgono ad una precedente versione dello stesso "ransomware". Tale versione fu usata in passato da un gruppo di hacker, il "Lazarus Group", che opera proprio dalla Corea del Nord.

Il secondo fattore è che proprio con questa precedente versione di "WannaCry", il gruppo nordcoreano è riuscito a depredare 81 milioni di dollari da una banca del Bangladesh. Il Lazarus Group si è dimostrato uno dei sodalizi cybercriminali più impegnati nell'estorcere soldi alle aziende o agli enti pubblici e privati che sono riusciti a raggiungere e "infettare"[82].

Inquietante il fatto che l'azione dei pirati informatici sia avvenuta in concomitanza con il lancio di un missile balistico "di nuovo tipo" da parte del regime di Kim Song-un.

Perchè? Alcuni esperti della sicurezza informatica hanno però affermato di non essere sicuri che l'attacco fosse principalmente a scopo di lucro, rilevando che la maggior parte dei maggiori ransomware e altri tipi di campagne di estorsione di cybercrime hanno prodotto milioni di dollari di entrate agli autori degli attacchi. "Credo che questo sia stato diffuso allo scopo di causare il maggior numero possibile di danni", ha dichiarato Matthew Hickey, co-fondatore della società di consulenza informatica britannica Hacker House.

Oltre alla necessità immediata di proteggere le strutture informatiche, l'attacco ha trasformato la cybersicurezza in un argomento politico in Europa e negli Stati Uniti, la cui discussione ha coinvolto anche il ruolo svolto dai governi nazionali. Il presidente russo Vladimir Putin ha

[81]Scott M. and Wingfield N. (2017), *Hacking Attack Has Security Experts Scrambling to Contain Fallout*, The New York Times, 13 maggio; Lohr S., Alderman L. (2017), *The Fallout From a Global Cyberattack: 'A Battle We're Fighting Every*, The New York Times, 15 maggio

[82]Gerino C. (2017), *Cyber attacco, Symantec (Usa) e Kaspersky (Russia) adombrano l'ipotesi di un'azione nord coreana*, La Repubblica, 16 maggio

dichiarato che tale tema dovrebbe essere "discusso immediatamente ad un livello politico serio"[83].

Come questa tesi e gli ultimi avvenimenti hanno ampiamente dimostrato, gli attori sull'attuale fronte cyber sono numerosi, tra i più attivi sicuramente USA, Russia, Regno Unito, Nord Corea e Cina. Le dinamiche nel cyber spazio continuano a influenzare eventi nel mondo reale, compresi i rapporti tra Stati; proprio per questo si dovrebbe parlare di cyber-diplomazia e regole di comportamento nel cyber spazio. Ciò deve essere chiaro soprattutto a chi governa, per evitare un fronte politico debole contro la minaccia cyber.

In un contesto in cui l'individuazione della minaccia è sempre più complessa, individuare i colpevoli è un'impresa davvero ardua. Sono necessari esperti in materia, non solo tecnici, ma anche legali e politici. Una politica cyber è oggi un punto fermo nella strategia di un governo che guarda con preoccupazione al futuro, consapevole dei pericoli e delle conseguenze di un attacco informatico[84].

Brad Smith si è rivolto a tutti gli apparati governativi e agli sviluppatori informatici, affinchè facciano fronte comune nella lotta contro i *cyber* crimini:

"Abbiamo bisogno del settore delle tecnologie, dei clienti e dei governi per lavorare insieme e proteggerci dagli attacchi informatici contro la sicurezza. Bisogna agire di più e farlo subito".

[83]Redazione online (2017), *Nuovi cyber-attacchi in Asia. Putin accusa l'intelligence Usa*, Il Sole 24 Ore, 15 maggio
[84]Redazione Cronaca (2017), *L'attacco degli hacker, i consigli della Polizia di Stato: ecco cosa dovete fare*, Corriere della Sera, 15 maggio

ABSTRACT

INTRODUCTION

This thesis deals with the controversial issue of *Cybersecurity.* The title is "The Cybersecurity: between legalprotection and multilevel policies". Due to the magnitude of the subject, I have followed a comprehensive approach, which includes a wide range of Countries, such as the United States, the United Kingdom, Germany and France. Lastly, Italian situation will be discussed, analysing its own "cyber path" over these few years. The analytical outlook will present either a legal and a political view, as the title suggests. This choice is justified by the conviction that national policies are the direct result of a stable legal body.

The thesis is divided in three chapters and each one is formed by four paragraph.

The first chapter presents a general overview of the topic. The paragraphs are structured to underline "key words"-as cyberspace, cybercrime and cybersecurity- with the exception of the last one, which lists the cybersecurity's paramount elements.

The second chapter focuses on national cybersecurity's strategy and the related legal instruments. Each paragraph is dedicated to a different State. The first analysis will concern the U.S.A., the main character of 2.0 revolution, followed by the United Kingdom, Germany and France.

The third chapter, which is the last one, will give a detailed analysis of Italy, highlighting every step made and every goal achieved as regards the subject matter

Finally, in the conclusion a comparison between the various realities discussed will be offered.

FIRST CHAPTER

The term "Cyber" is an ancient Greek word, which means "control". The literal sense of "control" is not forgone, because it could be translated as "constraint" or "advice". This interpretative issue is reflected in the controversial definition of cyberspace, both in the practical and in the theoretical view. The "*cyberspace*" is the environment composed by computing infrastructures, such as hardware, software, data and users, and their mutual relationships. It includes also Internet and other communication networks. The practical use of the word "cyberspace" started in 1984, when it was copied by a sci-fi novel, called "Neuromancer", written by Gibson. In the theory, this term was associated with a sense of immateriality and limitlessness. The current concept developed with the "cloud computing" (data and information management and file sharing), which was the starting point of "virtualisation time". Due to the proliferation of networks and the reduction of costs, the Internet domain is growing. The digital interactions increase as the risks. On one hand new types of

crimes have appeared, on the other, the traditional ones have nowadays most sophisticated means to apply.

The *cybercrime* is the set of violations perpetrated in the cyberspace. Its main trends are theft and manipulation of sensitive data, counterfeiting business, cryptovalue and recycling. “Cybercrime” differs from the traditional one because of the absence of physical borders and geographical limits, which makes the potential “victim” disoriented. Taking the amount of attacks into accounts, single protective measures are not enough. It is fundamental a real strategy.

“*Cybersecurity*” is the condition where cyberspace is protected against voluntary or accidental malicious events. Its objective is the defence of critical national infrastructures, governmental organizations, enterprises and individual citizens, through the drawing up of “National Strategic Plans”. These require a close relationship between the public and the private sectors and the R&D programmes. In addition, the plan must include a preventive and subsequent action, composed by: an effective governance, a risk and control assessment, a monitoring and an information sharing system, a good response and recovery capability.

An efficient digital policy is a primary need in the XXI century for each Country. Its absence exposes to the risk of losing qualified jobs, university and private research, know-how production, innovative businesses, start-ups and other opportunities of economic growth. The spread of a cybersecurity culture must be the ultimate goal of every State. This being said, in the second chapter I examine the U.S.A., the U.K, Germany and France strategy as far as cybersecurity is concerned.

SECOND CHAPTER

USA: The U.S.A cybersecurity was born in 1998, when the former president Clinton delivered the Presidential Decision Directive 63 (PDD-63), which concerned the protection of the National critical infrastructures. Nevertheless, the first cybersecurity programme was presented in 2007, by the Center of International Strategic Studies, after a wave of malicious cyber-attacks against the U.S.A. The government's goal was to improve the security of the nation's network and to formulate long-term recommendations. It has helped to create a national security framework, with respect for privacy and civil rights, and a comprehensive national security strategy that embraces both national and international aspects of IT security. This job was driven by the Congress and supported by the Defense Department. Due to the legal aspects involved, the former president Obama has issued an Exectived Order on February 12, 2013, titled “Improving Critical Infrastructure Cybersecurity”. It was the response to the *Cybersecurity Act*'s failure, which happened in April 2012, and it was based on the voluntary information sharing mechanism. In addition, the U.S.A. has been facing new threats in the military field. The actors involved in a potential cyberwar could be either American or

non-American citizens. For instance, individual hackers, terrorist groups or citizens from “rogue states” such as China, Russia and North Korea. These enemies want to obtain a military and economic advantage over the U.S.A. Because of the highly automated and interconnected nature of U.S.A. critical infrastructures, it is not practical to divide military and civilian operations. In this interagency framework, DoD should activate the response phase.

At the moment, the DoD has provided a detailed strategy of cyberdefense, which will be operative since 2018. At the same time, the President Donald Trump has presented a potential Executive Order. The draft has been renamed "Strengthening U.S. Cyber Security and Capabilities".

THE UNITED KINGDOM: Since the First World War, the British government has ensured both the Kingdom defense and public security .After the war, security legislation has been maintained with few changes, basing on non-binding guidelines and good practice initiatives promoted by the *National Infrastructure Security Co-ordination Centre* (NISCC) and *the National Security Advice Centre* (NSAC), both in partnership with industry. These two institutions joined in 2007, under the name of *Centre for the Protection of National Infrastructure* (CPNI). If the centre was not able to handle computer risks, the government could intervene "in the interests of national security”.

The first document about English cybersecurity was published in November 2011. Along with this, five years later a *National Cyber Security Strategy* was drawn up. It was composed by 3 cornerstones*:* Survey, Development and Defense. Greater resilience was also guaranteed through a sectoral strategy. As a matter of fact, the Office of Cyber Security and Information Assurance (OCSIA), within the Cabinet Office, coordinated National Cyber Security Program's activities into departments, government agencies, and decentralized administrations. Sectoral organizations collaborated with the Center for the Protection of National Infrastructure. In October 2016, the government launched the National Cyber Security Center (NCSC) as part of the GCHQ, the British intelligence and security organization. The NCSC will be the leading technical authority in cybersecurity in the United Kingdom, with the global responsibility of all cybersecurity advice, which will be issued by the British government. Instead, the CPNI will be continuing to drive physical security and staffing.

GERMANY: Germany presented in 2016 the White Paper for Security and the Future of the Bundeswehr. The timing of the document's publication- just after the British referendum result- and its contents, indicate that the German Federal Government has intended to assume the European leadership in the defence sector. In addition, Germany is one of the most affected countries by the cybercrime. It is demonstrated by recent data (284,000 computer attacks only in the first three months of 2017). The previous cybersecurity and cyberdefence structures were controlled by the traditional ministerial division. The foreign cyber operations were part of the

Bundesnachrichtendienst (BND), an intelligence service for German foreign affairs, directly dependent on the Chancellor's Office, while the cybernetic protection of the German critical infrastructures was performed by the Bundesamt für Sicherheit in der Informationstechnik (BSI - Federal Office for Computer Security), dependent on the Ministry of Interior. Recently, the German Defense Minister, von der Leyen, has opted for the creation of a special department, called "Computer and Cyber Security Department". It will have to be fully operational by 2023 and will work in collaboration with the Ministry of Interior.

The budget allocated for the defence will rise in the coming years. In practice, it will be employed for the creation of the "Cyber Defense Unit". It has entered into action since 5th Aprile 2017 to oversee cyber operations, IT infrastructures, military communications, operational and geolocation services. It will be fully operational in 2021.

FRANCE: The *Direction Générale de la Sécurité Extérieure* (DGSE) was the first French intelligence service for the external security. It was the only French entity capable of conducting offensive cyber-operations at a strategic level, until the birth of the *Agence Nationale de la Sécurité des Systèmes d'Information* (ANSSI). ANSSI is the national authority for security and defence of IT systems and its tasks are to identify, contain and respond to cyberattacks. Its competences include the whole critical infrastructures' area, both the public and the private ones, with the exception of the Armed Force, which is led by the General Armaments Directorate (DGA) and its own cyber command (COCYBER). Nowadays, cyber supremacy is essential for supporting the political and strategic autonomy of the Country. The Agency has increased French cyber defence and resilience capabilities with the Cyber Defense Pact (2014-2016) and the creation of the "Cybercom", a new military unit that is specialized in cyberwarfare. As far as France and Germany are concerned, the current legislation will have to be adapted to the EU one, which will be in force from 2018. It will be based on three pillars: the *Network and Information Security Directive (NIS Directive)*, the *General Data Protection Regulation (GDPR)* and the *Payment Services Directive 2 (PSD 2).*

Even Italy has to adapt its own legislation.

THIRD CHAPTER

ITALY: 24 years ago was issued the first Italian law in the field of "computering security". The law n.547/1993 provided some dispositions to counter the cybercrime in a broader view and it was modified by the l.n.48/2008, after the Budapest's Convention about Cybercrime in 2001. However, the "virtualitation era" required an action plan with specific rules, to replace ancient and abstract general laws. Hence, in 2013 was published the first Italian "National Strategic Framework for the Cybernetic Security". The "National Strategical Framework for the Cybernetic Security" is a

document elaborated by the Cyber Technical Table on 3rd April 2013. It has been working in the Information for Security Department, fixing the final tasks to fight cybercrime. Moreover, the action lines have been defined in the "National Strategical Plan for the Cybernetic Security" and coordinated by the CIRS (Interministerial Committee for Security of the Republic).

Nevertheless, national capabilities should spread into a global dimension. As Germany and France, Italy ought to follow the European Cyberstrategy. On 6th July 2015, was approved the Network and Information Security Directive (NIS Directive), which relied on an efficient information sharing system within the EU. The member States should implement the NIS directive within 21 months. The collaboration between States has been promoting by ENISA, the European Networks and Informations Security Agency. In Italy, NIS Directive has been transposed by a Legislative Decree in February 2017. It has replaced the previous Decree of the President of the Ministers' Council, issued on 24th January 2013 (it had established the 1st National Strategical Framework).

The program described in the new Decree is divided into many phases, and involves a limited number of actors: CIRS, DIS, NSC and the President of the Council. The CIRS has to emanate guidelines to raise the level of computer security, while the DIS' General Manager has to define these in practical actions. In addition, the DIS includes the NSC, which performs the paramount role of linking the several actors involved. Finally, the President of the Council coordinates the information security policy and issues both the directives and the arrangements for the system's organization and operations. He is responsible for their management. In spite of all these measures, Italian scenario is still critical. Italy is the ninth Country in the world ranking of Kaspersky Lab, which calculates theexposure to the cyber-attacks. According to Clusit Report the most difficult year for Italy was the 2016. From a quantitative point of view, 1050,000 global attack have been perpetuated, with disastrous consequences for the state economy and citizens' lifestyle. The high amount of attacks and the considerable number of victims depend on the volume of national economic exchanges and national know-how in specific sectors. Indeed, within such a competitive panorama, some emerging economies are interested in subtracting the Italian Technological and industrial know-how. This cybernetics context is a challenge. It requieres a gradual transformation of cybersecurity and cyberdefense infrastructures into a "comprehensive approach".

Bibliografia

- Agenzia Nova (2017), *Speciale Ict: cyber security, la Germania attiva l'unità di cyber difesa nazionale*, 13 aprile
- Arquilla J. (2012), *Rebuttal: Cyberwar is Already Upon Us*, Foreign Policy 192, n°84
- Banca D'Italia (2016), *G7 Fundamental elements of Cybersecurity for the financial sector,* Report
- Barak Obama (2010)*, Executive Order 13636 – Improving Critical infrastructure Cybersecurity*. Remarks by the President on Securing Our Nation's Cyber Infrastructure, May 29.
- Barlow J. P. (1996) , *A Declaration of the Independence of Cyberspace,* Davos, Switzerland
- BBC News (2017), *Cyber-attack: Europol says it was unprecedented in scale*, 13 maggio
- Belviolandi S. (2017), *Rapporto Clusit 2017 sulla sicurezza IT e Cybercrime: l'Italia vittima dei Ransomware*, 22 febbraio
- Brooker B.J.,Crawford J.,Horowitz B.M. (2007), *A Framework for the Evaluation of State Breach Reporting Laws*, in Proceedings of IEEE Systems and Information Engineering Design Symposium
- Bundesministerium des Innern (2012), *Cyber Sicherheitsstrategie für Deutschland ,* Berlin, Germany
- Camodeca D. (2017), *Attacco Cibernetico su scala mondiale, riscatto in Bitcoin*, 13 maggio
- Clarke R.A., Knake R.K. (2014), *Cyber War,* Tantor Media
- Clusit (2017), *Rapporto Clusit 2017 sulla sicurezza ICT in Italia*, 2017
- Cohen J. E. (2007), *Cyberspace As/And Space,* Columbia Law Review 107, pp. 210-256.
- Comptroller and Auditor General (2013), *The UK Cyber-security strategy:Landscape review*, 12 febbraio
- Condron S. (2007), *Getting It Right: Protecting American Critical Infrastructure in Cyberspace,* Harvard Journal of Law & Technology, Vol.20, cap.2, pp.403–422.
- De Capitani di Vimercati, S. Foresti, Samarati P. (2012), *Managing and accessing data in the cloud: Privacy risks and approaches*. In Proc. of the 7th International Conference on Risks and Security of Internet and Systems
- DoD (2016), *Cybersecurity National Action Plan*
- Egorov O. (2017), *Hacker, la Russia sotto attacco*, RBTH, 16 maggio
- European Union Agency for Network and Information Security (2012), *National Cyber*

Security Strategy. Practical Guidebook, p8

- Federal Ministry of the Interior Bundesministerium des Innern, *Cyber Security Strategy for Germany,* Berlin, Germany;
- Federal Office for Information Security (2016), *25 years of the BSI: more security, thanks to trasparency,* Security in Focus, BSI Magazine
- Flowers A., Zeadally S., Murray A.(2013), *Cybersecurity and US Legislative Efforts to address Cybercrime,* Homeland Security & Emergency Management, vol.10, cap.1, pp.1–27.
- Fonseca B.,Rose J.D.(2017), *Cybersecurity in the US: Major Trends and Challenges*, 09 February
- Garamone J. (2016), *Intel Undersecretary Describes Cyber Threat, Steps to Combat It,* U.S. Departement of Defence
- Gerino C. (2017), *Cyber attacco, Symantec (Usa) e Kaspersky (Russia) adombrano l'ipotesi di un'azione nord coreana*, La Repubblica, 16 maggio
- Gibson W. (1984), *Neuromancer,* Ace
- Glebocki, Jr J. (2008), *DoD Computer Network Operations: Time to Hit the Send Button*,Strategy Research Project, 10 marzo
- Goldman R. (2017), *What We Know and Don't Know About the International Cyberattack*, New York Times, 13 maggio
- Granado N., White G. (2008), *Cybersecurity and Government Fusion Centers*, in Proceedings of the 41st Hawaii International Conference on System Science
- Guitton C. (2013), *Cyber insecurity as a national threat: overreaction from Germany, France and the UK?,*European Security, Vol. 22, 3 gennaio,
- Halpin E.,Trevorrow P., Webb D.,Wright S.(2006), *Cyberwar, Netwar and the Revolution in Military Affairs,* New York: Palgrave Macmillan
- Hiller J.S.,Russell R.S. (2013), *The challenge and imperative of private sector cybersecurity: An international comparison*, Computer Law and Security Review
- HM Government (2016)*, National Cyber Security Strategy 2016*
- Il Fatto Quotidiano (2017), *Pirateria informatica, Europol: Attacco hacker senza precedenti? Serve indagine. Renault blocca fabbriche in Franci*a
- Laboratorio Nazionale di Cyber Security (2015), *Il Futuro della Cyber Security in Italia*, Consorzio Interuniversitario Nazionale per l'Informatica
- Langevin J., McCaul R., Michael T., Charney S.,Raduege H. (2008), *Securing Cyberspace for the 44th Presidency,*Center for Strategic and International Studies Washington DC

- LeClaire J. (2012), *Obama May Sign Cybersecurity Executive Order*, CIO Today, November 16
- Lohr S., Alderman L. (2017), *The Fallout From a Global Cyberattack: 'A Battle We're Fighting Every*, The New York Times, 15 maggio
- Lorusso S.(2011), *L'insicurezza dell'era digitale, Tra cybercrimes e nuove frontiere dell'investigazione*, Milano
- Martinez J. (2012), *White House Circulating Draft of Executive Order on Cybersecurity*, The Hill, September 6
- Mazzucchelli C. (2013), *Internet e nuove tecnologie: non tutto è quello che sembra*, Delos Digital srl, 24 dicembre
- Muller M. (2017), *The Cybersecurity Executive Orders: a Tale of two Trump*, Internet Governance Project, 12 febbraio
- Paganini P. (2017), *Elezioni USA e francesi, la politica indifesa verso la minaccia cyber,* Head of Cybersecurity Services Grant ThorntonConsultants e Chief Security Officer CSE - CybSec Enterprise SpA, 19 Maggio,
- Parodi C. (1997), *La frode informatica: presente e futuro delle applicazioni criminali nell'uso del software, in Criminalità informatica,* Sarzana Di S. Ippolito F. (a cura di), in Diritto e procedura penale
- Pica G. (2000), *Computer crimes e uso fraudolento delle nuove tecnologie*, Seminario di studi, Roma,15 dicembre.
- Presidenza del Consiglio dei Ministri (2012)*, Il linguaggio degli organismi informativi. Glossario intelligence,* Sistema di informazione per la sicurezza della repubblica, Quaderni di Intelligence Gnosis
- Presidenza del Consiglio dei Ministri (2013), *Piano Strategico Nazionale per la Sicurezza nello Spazio Cibernetico*
- Presidenza del Consiglio dei Ministri (2013), *Quadro strategico nazionale per la sicurezza dello spazio cibernetico*
- Redazione Cronaca (2017), *L'attacco degli hacker, i consigli della Polizia di Stato: ecco cosa dovete fare*, Corriere della Sera, 15 maggio
- Redazione online (2017), *Nuovi cyber-attacchi in Asia. Putin accusa l'intelligence Usa*, Il Sole 24 Ore, 15 maggio
- Rid T.(2013), *Cyber War Will Not Take Place*, Oxford U.P.
- Rijtano R. (2017), *Ransomware, l'attacco riparte dalla Cina. In Europa scampato cyber-caos per WannaCry,* La Repubblica, 15 maggio

- Ronfeldt D.(1993), *Cyberwar is Coming!*, Comparative Strategy 12, n°2, pp.141-165
- Rotenberg M., Jacobs D., *Privacy, Security, and Human Dignity in the Digital Age: Updating the Law of Information Privacy: the New Framework of the European Union*, Harvard Journal of Law & Public Policy 36, pp. 637-641.
- Sabatino E.(2016), *Il libro bianco della Difesa tedesco: quali opportunità di cooperazione?*, Istituto Affari Internazionali (IAI)
- Schwartau W. (1994), *Information Warfare: Chaos on the Electronic Superhighway,* New York: Thunders Mountain Press
- Scott M. and Wingfield N. (2017), *Hacking Attack Has Security Experts Scrambling to Contain Fallout*, The New York Times, 13 maggio
- Section 1385 of Title 18, United States Code (USC)
- Singer P.W., Friendman A.(2014), *Cybersecurity: What Everyone Needs to Know*,OUP USA
- Spadaro E.(2017), *Cyber, maxi attacco hacker mondiale: tra i paesi colpiti anche l'Italia. Un ransomware blocca i pc richiedendo un vero e proprio riscatto elettronico*, Difesa e Sicurezza Nazionale/Internazionale, 12 maggio
- Tikk E. , Kaska K., Vihul K. L., *International Cyber Incidents: Legal Considerations*, Tallinn: CCD COE publications
- Tosato F.,Taufer M.(2016), *Cybersecurity, la situazione italiana e gli scenari futuri*, La relazione del Ce.S.I.
- U.S. Department of Defence (2016), *Cyber Strategy*
- Uk Cabinet Office (2012), *Cyber Security Strategy of the United Kingdom: Safety, Security and Resilience in Cyber Space*, London, UK, 5 maggio 2012;
- UK Cabinet Office (2012), *The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World*, London, 5 maggio
- UK Cabinet Office (2015) , *National Risk Register of Civil Emergencies,* London UK
- UK Cabinet Office (2016), *Sector Resilience Plans,* London, UK
- Warfield D. (2012), *Critical Infrastructures: IT Security and Threats from Private Sector Ownership*, Information Security Journal: A Global Perspective, vol.21, cap.3, pp.127–136.
- Wiener N. (1965), *Cybernetics: or the Control and Communication in the Animal and the Machine,* 2nd ed. MIT Press
- World Economic Forum: Global Risks (2014), Insight Report Ninth Edition