Sen. Gen. Luigi RAMPONI

Con il patrocinio della
F I N M E C C A N I C A SpA
CONSORSIO STABILE MILES-S.I.
e con la collaborazione di
BOOZ&CO.

C Y B E R S P A C E

E LA SFIDA ALLA

SICUREZZA NAZIONALE

Atti del convegno promosso dal
Centro Studi Difesa e Sicurezza
A Roma il 29 Marzo 2011

A cura di:
Giuseppe CORDOVA
Salvatore SCURO
Grafica:
Mario CORDOVA

Edizione Ce. Stu. Di. S.
Via Damiata, 1 – 00192 ROMA
Tel/fax 06 3227255 – email: segreteria@cestudis.it
Sito internet: http//www.cestudis.it

Sen. Gen. Luigi RAMPONI
Presidente del Ce.Stu.Di.S.

APERTURA DEI LAVORI DEL CONVEGNO

Buongiorno a tutti. Mi scuso per il ritardo con il quale do inizio ai lavori del convegno: mi sono recato all'ingresso della sala, per rivolgermi alle molte persone ancora in fila per entrare e scusarmi, doverosamente con loro, sia per la lunga attesa a cui vengono sottoposti, sia perché non tutti potranno accedere visto che la sala oltre ad avere tutti i posti esauriti ha anche alcuni auditori in piedi.

Prima di dare inizio ai lavori del convegno devo far presente che, a causa della situazione nazionale ed internazionale molto tesa, alcuni dei relatori che avevano dato la loro adesione a questa iniziativa, ed in particolare dei Dicasteri degli Interni e degli Esteri, per i molti impegni che in questo momento devono fronteggiare e che si possono facilmente immaginare, non potranno essere presenti. Mi riferisco al Ministro Roberto Maroni, al Ministro Ignazio La Russa, al Sottosegretari Vincenzo Scotti che trovasi a NewYork ed al Prefetto Antonio Manganelli, Capo della Polizia.

Il Centro Studi Difesa e Sicurezza ha sempre tenuto presente il potenziale sviluppo della cibernetica al punto che già tre anni fa aveva organizzato un convegno sul tema: "*Terrorismo e contro terrorismo nella cyber war"* che riguardava la componente cibernetica in rapporto con il terrorismo, sia in termini di utilizzo da parte loro delle reti per le attività operative, sia come possibilità di attacco alle nostre reti cibernetiche.

Oggi, ho riproposto questo secondo convegno sulla problematica perché nel frattempo, come al Ce.Stu.Di.S per altro si prevedeva, l'argomento è diventato di grandissima attualità al punto che si debba vedere questa ***area della cyber space come la quinta dimensione - nella quale si può portare gli attacchi e ci si deve difendere - aggiungendo questa dimensione tra le tradizionali: terra, mare, cielo e spazio***.

La cyber space è quindi diventata la quinta dimensione e si sta vivendo una esperienza davvero eccezionale, epocale (come lo è stata, quaranta anni fa, quella dello spazio) perché negli Stati di avanzata tecnologia, si sono realizzate rete di interconnessione di informatica e di telecomunicazione, che praticamente reggono le sorti della guida e del funzionamento di tutto quanto riguarda lo Stato, la Società e costituisce, sempre più, una parte importante della nostra vita quotidiana.

Di contro, in questo contesto, la cyber space denuncia anche una grossa vulnerabilità nei confronti:

- della criminalità, perchè questa se ne può avvalere, come "moderno grimaldello", per sottrarre denaro, per truffare cittadini ed organismi vari;
- del terrorismo che può avvalersene per tutto lo spettro delle loro attività: dal reclutamento al finanziamento, dalla propaganda all'attacco informatico vero e proprio;
- dell'intelligence che cerca di permeare queste strutture - sia che trattasi di organismi Statali o di organizzazioni non governative, del tipo Wikileaks - per violarne i segreti custoditi.

Al di là di queste tre minacce vi è, soprattutto, la minaccia di guerra: ***la cyber war***.

Le prossime guerre tra Stati non verranno più iniziate dalle Forze Armate, ma saranno concentrate su un massiccio utilizzo di attacchi informatici per sabotare preventivamente la capacità di risposta o di offesa degli avversari e per arrecare pesanti danni, non virtuali ma materiali.

Lo spazio cibernetico è, dunque, un nuovo fondamentale campo di battaglia e di competizione geopolitica del XXI secolo.

Appurata questa realtà, è indispensabile un impegno per fronteggiare tale minaccia, ricordando che gli attori che possono avvalersi dello strumento informatico per azioni ostili, vanno dall'hacker individuale che agisce a scopo di lucro, fino all'apparato governativo che persegue obiettivi di geopolitica o di propaganda.

Il discorso, analogamente, vale per lo spettro dei possibili bersagli: dai conti correnti dei singoli cittadini alla sicurezza dei gangli vitali dello Stato.

Un attacco informatico, quindi può provenire pressoché da chiunque e per qualunque fine ed ha infiniti potenziali obiettivi: da chiunque contro chiunque.

Tutto ciò rende necessario mettere a punto delle difese e, siccome parlo di cyber war, significa mettere a punto delle difese nelle quali occorre anche essere capaci di poter colpire preventivamente l'avversario, per evitare che colpisca noi: è questa la grande attualità di questo convegno ed anche della problematica che lo riguarda.

Bisogna mettere a punto una strategia che non è la strategia tradizionale dove vi erano dei punti fermi e su questi punti si costruiva il concetto d'azione, di difesa o di attacco, nei confronti dell'avversario (anche in quella nucleare vi erano dei punti fermi).La eterogeneità, la complessità e la continua evoluzione dell'***ambiente cyber*** impone, per entrare in questo nuovo ordine di idee, una adeguata strategia di contrasto, basata su altri parametri.

Un altro aspetto interessante, è rappresentato dal fatto che lo scontro cibernetico può eliminare grosse differenze di potenziale: uno Stato molto forte, in termini di armamenti convenzionali e nucleari, può essere paralizzato da uno Stato piccolo dalla aggressiva capacità cyber.

Lo cyber space, quindi, può eliminare il divario di potenza avendo la possibilità di vulnerare o paralizzare le strutture critiche del rivale "superpotente" - annullando così il gap militare o, addirittura, rendendo impossibile la sua utilizzazione – divenendo, a sua volta, uno strumento di deterrenza.

Tutto ciò ribadisce il concetto precedentemente espresso e cioè: ***la cyber è una minaccia che può provenire da chiunque contro chiunque.***

I Governi ed i Parlamenti nazionali possono e debbono svolgere un ruolo fondamentale, una volta individuata la minaccia di attacchi cibernetici, definendo e votando leggi adeguate, stipulando e ratificando accordi internazionali, garantendo che il sistema di leggi e di altre misure siano correttamente applicate, in ambito nazionale.

In riferimento alla situazione nazionale, l'Italia:

- ha fino ad oggi adottato misure di prevenzione e di protezione, delle strutture e degli assetti pubblici e privati, in termini omologhi a quelli messi in atto dai principali parters europei;
- ha una diffusa predisposizione ed una organizzazione, nel quadro di difesa contro attacchi cibernetici, di sistemi di protezione, nell'ambito dei diversi assetti pubblici e privati, in avanzata via di realizzazione ;
- ha una struttura nel quadro della capacità offensiva, di competenza della Difesa, che viene sviluppata in ambito e nel contesto della Nato.

Vi è, tuttavia, una urgente necessità di indirizzo e di coordinamento unitario ed in tale quadro il Governo ed il Parlamento possono e devono svolgere un ruolo fondamentale.

Il convegno, quindi, anche sulla base di quanto messo in luce da una recente relazione del COPASIR sul tema, si propone di:

- informare sul cyber space e su tutte le sue implicazioni;
- giungere, attraverso un articolato dibattito che vede impegnati esperti e responsabili di alto livello, all'individuazione di una proposta di soluzione condivisa, per garantire un'azione

unitaria di indirizzo e coordinamento delle iniziative di contrasto alla minaccia cibernetica, sia in campo civile, pubblico e privato, sia in campo militare nell'ambito dell'Alleanza Atlantica;

per far sì che i rappresentanti dei Gruppi Parlamentari, in particolare del Senato, possano esprimere un loro parere su di una mozione che io ho preparato, al fine di pervenire, al termine dei lavori del convegno, ad un concreto risultato.

Mi sono riproposto, ormai da alcuni convegni tenuti dal Ce.Stu.Di.S. (convegni questi molto onerosi ed impegnativi nella loro organizzazione), di dare un significato più sostanzioso ai dibattiti tenuti dalle menti che vi hanno partecipato - ma soprattutto per non mandare sprecato il loro grande lavoro svolto e per non mortificare le conclusioni raggiunte – presentando, ora un disegno di legge in derivata, ora una mozione.

Per questo convegno, come accennato, ho approntato una mozione che potete leggere in allegato al presente opuscolo.

Permettetemi una ultima considerazione: il convegno precedentemente tenuto dal Ce.Stu.Di.S., sul tema degli aiuti ai Paesi in via di sviluppo, è stato certamente un after day, cioè abbiamo denunciato già d'allora la situazione difficile nella quale si trovavano tanti Paesi, in particolare dell'Africa, e la grettezza politica dei Paesi avanzati. La situazione è drammatica e porta ad un vero ed autentico sconvolgimento in diversi Paesi (la Tunisia, l'Egitto e gli altri) proprio perché le condizioni di vita sono disperate. In quel convegno si disse che ci saremmo dovuti impegnare di più e, se lo si fosse fatto in precedenza, forse anche la democrazia si sarebbe manifestata più facilmente. Ricordo, a tal proposito, quanto foga mise il Min. Belloni (anche oggi è qui con noi) nel dire tutto questo ed ora è costretta ad operare in situazioni molto drammatiche.

Concludo ringraziandovi per essere intervenuti così numerosi e spero che il convegno potrà risultare interessante. Passo la parola alla 1^ sessione che è coordinata dal mio amico dott. Ludovico

PRIMA SESSIONE
QUADRO GENERALE

Coordinatore:
Dott. Marco LUDOVICO
Relatori:
Dott. Domenico VULPIANI
Dott. Alessandro GAZZINI
Ten. Col. Marco DE FALCO
Ing. Luca IZZOTTI

Dott. Marco LUDOVICO
Il Sole 24 Ore

Grazie. Il quadro prospettato dal Gen. Ramponi è così chiaro che non vi è nulla da aggiungere, se non un dato di cronaca: un paio di giorni fa ho letto su un quotidiano che alcuni blog dei ribelli libici erano stati attaccati da hacker riconducibili alle forze lealiste del Governo di Gheddafi e mi sono chiesto, e credo che sia legittimo chiedersi, se questi stessi hacher volessero, a scopo offensivo, agire contro di noi, saremmo attrezzati? Sulla carta, probabilmente si, per quello che è l'articolazione dei sistemi che oggi possiamo vantare di avere.

Ma proprio l'introduzione del Gen. Ramponi ci spiega che non è così scontato, proprio perché la minaccia è variabile, aggiornata, imprevedibile, non legata alle forze specifiche degli Stati che tra di loro si contrappongono.

Voglio partire da questa suggestione per introdurre la nostra prima sessione ed andare direttamente a presentare la prima relazione del dott. Alessandro Gazzini che è il Vicepresidente di Booz&Company che è una grande multinazionale di consulenza strategica operativa.

Mi fa molto piacere che i lavori comincino da questa relazione proprio perché essa ci darà il quadro internazionale e ci dirà come oggi la Francia, la Germania, gli Stati Uniti e l'Inghilterra, con varie e diverse modalità si sono attrezzate nel confronti del cyber space. Ricordo, in linea generale i 10' a disposizione per ogni relatore e mi prenderò il diritto di interrompere per fare qualche domanda. La parola al dott. Gazzini.

Dott. Alessandro GAZZINI
Vice President
Booz & Company Italia

SITUAZIONE INTERNAZIONALE

Grazie. Saluto tutti i partecipanti a questo convegno, ringrazio il Sen. Ramponi ed il Ce.Stu.Di.S. per questa opportunità. Io porterò una breve e veloce riflessione su qualche modello organizzativo messo in campo da nostri principali partner internazionali

BREVE ANALISI COMPARATA DEI MODELLI INTERNAZIONALI DI CYBER SECURITY

1. Contesto di Riferimento

Le Infrastrutture tecnologiche, informatiche e di telecomunicazioni sono un elemento imprescindibile del mondo moderno, divenute ormai essenziali per il funzionamento della quasi totalità delle aziende e delle pubbliche amministrazioni. Risultano, in particolare fondamentali per l'erogazione di servizi estremamente critici, quali ad esempio l'approvvigionamento e l'erogazione di energia elettrica, la comunicazione e lo scambio di informazioni, i trasporti di merci e persone, le reti idriche, i sistemi di difesa e di sicurezza nazionale.

E' grazie a tali infrastrutture che ogni secondo viene trasferita una significativa mole di dati, spesso altamente confidenziali, di persone, governi e aziende, permettendone l'accesso i in modo ubiquo e sempre più pervasivo anche grazie a device mobili sempre più diffusi, che spaziano dal PC laptop, allo smartphone, all'iPad.

Tali infrastrutture utilizzano tecnologie complesse, realizzate anche con standard "aperti" e

spesso interconnessi con la rete Internet. L'apertura degli standard adottati, se da una parte garantisce un accesso universale ed una interoperabilità crescente, dall'altra costituisce una vulnerabilità al sistema stesso nel suo complesso.

Questo aspetto non è trascurabile, stante la continua ed apparentemente inarrestabile crescita esponenziale degli attacchi informatici, evidenziata anche da qualificati studi Symantec Global Internet Security Threat Report April 2009, , IBM Trend and Risk Report 2010, McAfee Virtual Criminology Report 2009, Richard Clark and Robert Knake Cyber War: The Next Threat to National Security and What to do About it, 2010 sul tema nonché in sedi istituzionali. Ad esempio, le intrusioni o *probes* non autorizzate, a danno dei sistemi informativi della Difesa USA, sono state quantificate essere pari a 250.000 all'ora CSIS Cybersecurity Discussion with Gen. K. Alexandre 3 June 2010, come espresso dal Generale Kieth Alexandre, Direttore NSA e Comandante dell'*US Cyber Command*, in un recente intervento al CSIS a Washington.

La crescita delle minacce alle infrastrutture rappresenta pertanto un problema serio in relazione alle potenziali conseguenze al benessere dei cittadini, delle istituzioni ed organizzazioni, quanto più grave a causa della strutturale asimmetria associata con le misure "in attacco" o "in difesa".

Difatti, in termini tattici, chi gioca in attacco si trova in una posizione di favore, essendo facilitato da diversi ordini di grandezza rispetto alla complessità della difesa. L'organizzazione di un attacco significativo ad una grande azienda può implicare un investimento complessivo di circa alcune centinaia di migliaia di Euro (per mantenersi larghi), mentre la preparazione della difesa necessaria allo stesso attacco come misure preventive e reattive necessita tipicamente di diversi milioni se non decine di milioni di Euro annui.

Naturalmente ciò che allarma non è solo la progressiva crescita numerica degli attacchi, in parte semplice risultato matematico derivante dalla continua digitalizzazione (più apparati installati, più persone preparate ma tasso di criminalità costante), ma soprattutto il livello qualitativo delle intrusioni e la pluralità dei soggetti malevoli, che sono evoluti rapidamente da hackeraggio celebrativo e criminalità organizzata, ad organizzazioni complesse con capacità e strumenti simili a veri e propri apparati statali.

Questa realtà se calata nel mondo dei sistemi logici di controllo e comunicazione dei processi industriali critici (es. PLC, SCADA, etc) è assai preoccupante. Non si tratta più di fantascienza, come ha ampiamente dimostrato anche il recente caso "Stuxnet".

Il punto non è più se sia giusta o meno l'innovazione digitale dei nostri sistemi industriali mediante adozione di nuove tecnologie (quali ad esempio, con riferimento al caso della rete elettrica, SmartGrid, Smart Metering, Contatore Elettronico, etc), imprescindibili allo sviluppo della nostra società, ma quale sia la corretta dose di sicurezza da garantire, non solo a tutela della singola azienda (compito dell'azienda stessa), ma a salvaguardia di un'adeguata sicurezza a livello nazionale.

Pian piano che ci si muove verso scenari di controllo remoto della rete, comprese funzionalità di "shut down" del servizio, è evidente che il rischio connesso con attacchi malevoli, eventuali errori, leggerezze, possibile disallineamento di obiettivi tra necessità privata e bene pubblico, costituisce un tema di tale importanza strategica che non può essere responsabilità delegata semplicemente alla singola azienda.

Ad aggravare questa situazione, contribuiscono inoltre effetti economici dell'insicurezza digitale al nostro sviluppo economico, stimati da un nostro recente studio come value-at-risk di circa 1% del PIL dell'EU, pari all'incirca a 124 miliardi di euro Booz & Company and Liberty

Global, “Digital Confidence”, 2009….

L’urgenza di intervenire in modo strategico e strutturato a livello nazionale sulla sicurezza delle Infrastrutture ICT e più in generale delle informazioni e telecomunicazioni è divenuta pertanto una priorità assoluta, in quanto elemento fondamentale per garantire lo sviluppo di Internet, dei servizi digitali, nonché la sicurezza delle Infrastrutture Critiche Informatizzate per la nostra società.

2. Panorama Internazionale

Dinanzi a questa realtà la gran parte dei paesi industrializzati si è mossa aggressivamente per rivedere in profondità i propri assetti organizzativi ed operativi. Raramente nella mia esperienza professionale ho potuto osservare una tale concentrazione di cambiamento attuata in un arco temporale cosi breve, da un numero cosi elevato di paesi, in una comune direzione di potenziamento delle capability di cyber security nelle sue componenti principali: infrastrutture critiche, *law enforcement*, intelligence e comparto militare.

I modelli organizzativi possono variare secondo necessità, cultura, legacy nazionali ma il focus strategico rimane “a tutto tondo” sullo sviluppo di un “sistema nazionale” complessivo integrato di capability operative distintive.

Tralasciando il dettaglio del singolo paese, possiamo ben identificare alcune caratteristiche comuni a tutti i modelli analizzati :

- Cyber come **priorità di sicurezza nazionale** con un impegno diretto del vertice governativo e il posizionamento del problema non più semplicemente in termini di lotta alla criminalità, ma come rischio prioritario alla sicurezza nazionale (es. cyber qualificato in Francia come “menace majeur”, oppure in UK come “tier one risks”);

- Articolazione di un **piano strategico** per chiarire obiettivi, delineare confini, ruoli ed attività all’interno di un’architettura univoca a livello nazionale spesso con identificazione di risorse finanziarie incrementali (es. “Cyber Security Strategy for Germany”, o “Défense et sécurité des systèmes d’information - Stratégie de la France”);

- Identificazione di **un organismo di indirizzo e coordinamento centrale** tipicamente a riporto del vertice governativo(es. “Office of Cyber Security and Information Assurance” presso il “Cabinet Office, National Cyber Security Coordinator” presso la Casa Bianca in USA, o piuttosto “Agence Nationale de la Sécurité des Systèmes d’Information (ANSSI)” presso il Primo Ministro Francese, o il National Cyber Security Council e BSI in Germania ;

- **Consolidamento e rafforzamento delle strutture operative** (es. il nuovo “National Cyber Defence Centre” a riporto di BSI con risorse multi agency, o il “Cyber Security Operations Center” presso il GCHQ, w nuovamente in ottica multiagency, l’autorità unica tra NSA e “Cyber Command” nella figura del sopra citato Generale K. Alexandre);

- Immediato e urgente **reclutamento e sviluppo di competenze specializzate** (es. lancio di competizioni nazionali, cosi dette Contest, in USA e UK, “National Initiative for Cyber Security Education (NICE)” in USA, il reclutamento diretto e straordinario presso il settore privato attuato dall’ANSSI e BSI);

- Cyber come **catalizzatore di ricerca e innovazione (R&D) e capacità industriali** nazionali (es. l’estesa rete di laboratori e centri di ricerca presso le Università USA in partnership con vari organismi: NSA, Difesa, FBI, etc; lo sforzo incrementale di fondi destinati alla ricerca cyber in

UK, Germania, Francia, USA; il progetto di creazione di un centro nazionale per la ricerca di cyber defence in Francia);

- Rafforzamento generale delle **capacità cyber in ambito militare, intelligence, *law enforcement* e infrastrutture critiche** (es. pluralità di nuovi centri e comandi operativi, allocazioni di budget straordinari e dirottamento di fondi ordinari sulla mission cyber in UK, USA, Germania);

- Sviluppo di un approccio di "**multi agency" e di forte collaborazione pubblica su infrastrutture critiche** (es. GCHQ, Cyber Command e NSA, partecipazione strategica delle infrastrutture critiche in Germania, Olanda, Francia);

- Incremento di **presenza "pubblica" degli organi di intelligence sui temi di cyber security** e.g. GCHQ in UK, collaborazione tra NSA e Cyber Command e Homeland Security, collaborazione di BSI e Intelligence

- Sviluppo di una **politica estera cyber di collaborazione internazionale e nuova regolamentazione** (es. proposte di trattati di non proliferazione cyber, proposte di regolamentazione sul cyber crime, proposte di Internet *governance*, istituzione di un nuovo "Office for the Coordination of Cyber Issues" presso il Department of State, in USA);

- **Revisione degli assetti normativi nazionali** in modo da chiarire meglio ruoli, poteri, regole di ingaggio e ambiti di intervento (es. decreti emessi da BSI nel Dicembre 2010, decreti attuativi dell'ANSSI, oltre 5 nuove proposte legislative cyber presso il Congresso USA, valutazioni in corso in USA sulle regole di ingaggio relative a scenari di cyber war, etc).

Il quadro generale viene confermato anche se estendiamo lo sguardo, oltre i quattro modelli prescelti, ad altri paesi come Estonia, Canada, Australia, Olanda nonché a istituzioni multinazionali come NATO ed Unione Europea. Con particolare riferimento a quest'ultima, infine, possiamo evidenziare il potenziamento dell'Agenzia ENISA (European Network and Information Security Agency), lo stanziamento di fondi di ricerca incrementali sulle attività cyber, le iniziative legislative relative al Cyber Crime e tutela dell'identità elettronica, l'esecuzione di esercitazioni cyber.

3. Road Map per l'Italia

In coerenza con quanto sinora rappresentato, l'Italia non è rimasta ferma, provvedendo a sviluppare diverse iniziative e capability decisive, a livello di singole Forze di Polizia, CNAIPIC della Polizia Postale e delle Comunicazioni, Forze Armate, Poste Italiane con la Fondazione "Global Cyber Security Center" e "European Elettronic Crime Task Force", ENEL con il centro di ricerca sui sistemi scada e altre attività presso organismi nazionali, centri di ricerca, università e settore non for profit.

Tuttavia, come già sopra evidenziato oltre ad essere ben messo in luce recentemente dal rapporto COPASIR Copasir, Relazione sulle possibili implicazioni e minacce per la sicurezza nazionale derivanti dall'utilizzo dello spazio cibernetico, 15 Luglio 2010, occorre a questo punto sviluppare un approccio al tema "a tutto tondo" che possa dare una visione ed articolazione strategica, organizzativa, operativa e regolamentare complessiva che abbracci tutto il fenomeno dagli aspetti di *cyber crime*, protezione delle infrastrutture critiche, *cyber espionage* e *cyber war*. Ciò, naturalmente nel rispetto dei ruoli istituzionali ma anche avvalendosi in modalità sinergica delle competenze acquisite e delle strutture operative già attive sul territorio nazionale.

Il percorso non è semplice, come illustrato dall'Ammiraglio Picchio, data la natura del

fenomeno cyber difficilmente governabile a livello strategico con gli attuali assetti organizzativi, ed è pertanto necessario affrontarlo con i dovuti approfondimenti, condotti nell'ambito di una commissione di studio nazionale.

Dalla nostra esperienza in situazioni paragonabili esistono alcuni passaggi estremante utili per formulare una strategia nazionale. In estrema sintesi occorre affrontare quattro macro attività, ovvero, *capability assessment*, *best practices analysis,* chiarimento dei gap e vincoli, per poi sviluppare una strategia con la definizione di vision ed obiettivi, organizzazione, modello operativo, risorse e roadmap di sviluppo, cioè:

1. ***CAPABILITY MAPPING:*** stabilire con chiarezza una mappatura delle attività e capabilities cyber a livello nazionale a secondo una tassonomia univoca di "servizi cyber"; aree di eccellenza; gaps; etc.;
2. ***BEST PRACTICES:*** sviluppare un confronto dettagliato con selezionati paesi alleati e rispettivi programmi cyber; lessons learnt; organizzazione; regolamentazione; risorse; ricerca; strategia diplomatica; etc.;
3. ***PRIORITA' / GAPS / VINCOLI:*** identificare macro priorità, perimetro operativo e "ambizione nazionale"; gap da colmare; vincoli da superare (legislativi, culturali, finanziari,…); linee guida da seguire;
4. ***MODELLO OPERATIVO:*** formalizzare strategia, organizzazione, modello operativo e "roadmap" di sviluppo; evitare duplicazioni e concentrazione capabilities critiche; favorire ruolo privati e ricerca; allocare risorse.

Nonostante che il tempo disponibile e l'attuale contesto macro economico non siano favorevoli, vista l'intensa attività già messa in campo dai nostri principali alleati e la continua crescita della minaccia, è indispensabile assicurare una regia unitaria degli interventi e completare velocemente la fase di studio e di definizione formale degli assetti attuali, e consentire di passare quanto prima alla fase operativa.

A chiusura aggiungerei solo un'enfasi aggiuntiva sull'urgenza, di là delle potenziali architetture organizzative, di lanciare un serio piano di sviluppo e reclutamento delle competenze specializzate sia nel settore governativo che privato. Senza la materia prima, ossia risorse umane qualificate, sarà arduo sviluppare delle capability di cyber security significative.

Dott. Marco LUDOVICO

Grazie al dottor Gazzini. Vorrei sottolineare il valore della sua relazione che ci ha fatto e che ci consente di avere un quadro internazionale molto chiaro ed in particolare, fra tutte le sue indicazioni (lo dico senza alcuna retorica), un dato molto efficace che ci dovrebbe far riflettere molto e cioè gli investimenti di risorse che sono stati fatti dagli altri Stati su questo tema e dai quali noi siamo molto indietro. Ricordo che al termine di questa sessione ci saranno circa 10' a disposizione per il dibattito.

Vi faccio presente che l'intervento dell'ing. Massimo Sarmi che sarebbe dovuto essere adesso, sarà tenuto nella seconda sessione e per tanto sto per dare la parola al Ten. Col. Marco De Falco, che è il rappresentante italiano presso la Nato, e che quindi nella sua relazione illustrerà il lavoro fatto nel campo della cyber security da parte del Patto Atlantico.

Ten. Col. Marco DE FALCO

SITUAZIONE NATO

Illustri ospiti, sono il Ten. Col. Marco De Falco, dell'Aeronautica Militare Italiana, e presto servizio presso il centro di eccellenza della cyber defence sito a Tallinn in Lettonia. Nel mio intervento, che sarà veloce, farò un rapido excursus della situazione Nato fornendovi alcune informazioni su ciò che ha portato alla definizione di una nuova strategia di cyber defence.

Introduzione

Tra le principali minacce "emergenti, non tradizionali e asimmetriche" presenti nel panorama geopolitico attuale, i cyber attacks, oltre ad essere una realtà con la quale la NATO ha dovuto confrontarsi da tempo, sono quella più difficilmente controllabile (anche a causa della difficoltà di attribuzione) e nel contempo anche quella meno percepita dall'opinione pubblica, seppure avvertita da quest'ultima più che in passato.

La dipendenza, ormai da tempo globalizzata, delle società tecnologicamente avanzate dai sistemi CIS[1] fà della Cyber Defence un' esigenza irrinunciabile, che tuttavia ha iniziato ad apparire tale solo recentemente, e che è maturata nella considerazione della NATO attraverso il susseguirsi di importanti eventi.

Gli eventi storici - Evoluzione della minaccia e adattamento

La NATO sebbene abbia sempre protetto i propri sistemi CIS, componenti essenziali di qualsiasi strumento militare, è soltanto in occasione del vertice di Praga del 2002 che questo obiettivo fu esplicitamente incluso nella sua agenda politica. L'attenzione fu posta sul problema per via di alcuni attacchi condotti da hackers serbi alla fine degli anni '90, in seguito all'intervento NATO nei Balcani. In questa occasione fu anche dato mandato di creare l'NCIRC (NATO Incident Response Capability).

Sulla base dei risultati tecnici messi in atto, i leader alleati ribadirono la necessità di proteggere questi sistemi di informazione anche durante il vertice di Riga nel novembre 2006.

Nel 2007, una serie di attacchi informatici di grande portata condotti in Estonia contro siti Internet di istituzioni pubbliche e private[2] costrinse la NATO a riesaminare attentamente le sue capacità di difesa informatica. Alla riunione di giugno 2007, i Ministri della Difesa dei paesi NATO, sensibilizzati dagli eventi dell'Estonia, convennero che un intervento urgente era necessario in questo settore. Di conseguenza, la NATO condusse una valutazione approfondita del suo approccio alla Cyber Defence e ne riferì gli esiti nel mese di ottobre 2007, raccomandando sia l'adozione di ruoli specifici sia l'attuazione di un certo numero di nuove contromisure tese a migliorare la protezione dagli attacchi informatici. Inoltre, fatto ancora più notevole, per la prima volta fu richiamata l'attenzione sulla necessità di definire una politica di difesa informatica della NATO.

L'attacco all' Estonia può essere considerato una svolta nella concezione delle minacce informatiche, tanto che in ambito NATO è divenuto comune parlare *di pre-Estonia* e *post-Estonia* riferendosi proprio a questi avvenimenti.

Precedentemente a questo evento, gli sforzi di difesa informatica della NATO erano concentrati più che altro sulla protezione dei propri sistemi di comunicazione. A seguito degli attacchi, perpetrati contro servizi di pubblica utilità nazionali e portati a termine massicciamente attraverso Internet, la sfera di azione della NATO è stata allargata in modo da poter comprendere

[1] Communication and Information Systems

[2] Furono oggetto di massicci attacchi DDoS e di defacements, per oltre due settimane, i server DNS degli ISP e i siti delle maggiori banche (Hansa Pank (SEB), Swedbank), dei partiti politici, delle università, di quasi tutti i Ministeri, del Parlamento, della Presidenza della Repubblica, della televisione nazionale, delle società telefoniche, e di diversi giornali e radio.

anche la sicurezza informatica dei singoli alleati. Come risultato, la NATO ha sviluppato opportune soluzioni per assistere quegli alleati che dovessero richiedere il sostegno dell' Alleanza per la protezione dei loro sistemi ICT[3], anche attraverso l'invio di *Rapid Reaction Teams*[4] (RRT).

Il 7 gennaio 2008 il Consiglio Atlantico approva il suo primo documento di "NATO Cyber Defence Policy". Il documento stabilisce i principi di base della Cyber Defence e fornisce indicazioni agli organismi militari e civili della NATO e raccomandazioni alle nazioni NATO. In esso viene riconosciuta una sempre maggiore dipendenza tra i sistemi CIS e la condotta delle operazioni dell'Alleanza, e che l'attacco a detti sistemi - soprattutto se dislocati in reti classificate - sarebbe causa di pesanti degradazioni alle funzionalità della NATO e delle Nazioni alleate.

Nel vertice di Bucarest (aprile 2008), nel ricordare la politica appena adottata, si ribadisce che è in corso lo sviluppo di specifiche strutture e autorità per realizzarla, e che "*la NATO resta impegnata a potenziare i sistemi di informazione chiave dell'Alleanza contro gli attacchi informatici*", auspicando il rafforzamento dei legami tra NATO e autorità nazionali.

Dopo gli attacchi contro l'Estonia, le minacce informatiche si sono rapidamente evolute in frequenza e sofisticazione. Nell'estate del 2008, la guerra in Georgia ha dimostrato che gli attacchi informatici sono ormai diventati una componente importante di una guerra convenzionale.

Nel vertice di Strasburgo-Kehl del 2009, le Nazioni, in virtù del mutato scenario geopolitico mondiale, convengono sulla necessità di definire un nuovo Concetto Strategico NATO per il successivo decennio, nel quale contemplare anche gli aspetti di cyber defence.

Nel maggio 2010, il Vice Segretario della Difesa americano William Lynn riconosce ufficialmente il cyberspace quale "quinto dominio"[5] di applicazione delle operazioni militari, sdoganando in un certo senso con questa definizione l'accettazione del cyber warfare come una nuova tipologia di operazioni belliche.

L' evento sicuramente più importante del 2010 è però il vertice NATO di Lisbona, in occasione del quale gli stati membri approvano il nuovo Concetto Strategico, che, in particolare, dà mandato per lo sviluppo di una nuova politica NATO di difesa informatica e per un relativo piano d'azione la cui stesura è prevista entro la fine di giugno 2011.

Le asserzioni contenute nel nuovo Concetto Strategico e nella Dichiarazione del vertice di Lisbona indicano chiaramente che la rapida evoluzione e la crescente complessità degli attacchi cyber fanno della protezione degli assetti CIS degli Alleati un compito urgente da cui la stessa sicurezza futura della NATO può dipendere. Il vertice ha infatti posto la sicurezza informatica in prima linea tra le nuove sfide alla sicurezza che la NATO (anche attraverso la sua nuova "Emerging Security Challenges Division") si troverà ad affrontare negli anni a venire, e ha rilasciato precisi orientamenti politici e il compito di apportare una revisione approfondita alla attuale politica di Cyber Defence tramite aggiornamenti rilevanti.

Organismi ed enti NATO

All'interno della struttura organizzativa della NATO sono attualmente presenti numerosi enti che risultano coinvolti a vario titolo nelle attività di Cyber Defence (di tipo "decision making", "operational" e "advisory"[6]):

Ente	Tipologia	Ambito	Dipendenza

[3] Information and Communication Technology. Detto di sistemi che elaborano o comunicano dati in forma digitale.

[4] In via di attivazione; previsti all'interno della FOC (Full Operation Capability) di NCIRC per il 2012.

[5] USSTRATCOM Cyberspace symposium, 26 maggio 2010 (keynote speech), e articolo "*Defending a New Domain: The Pentagon's Cyberstrategy*", Foreign Affairs, Volume 89 n. 5, September/October 2010.

[6] Si definiscono, nella terminologia NATO, *decision-making* gli enti che hanno potere decisionale, *operational* quelli operativi e *advisory* quelli che forniscono consulenza e pareri tecnici.

NAC	Decision-making	Globale, politico	-
DPPC	Decision-making	Globale, politico	(NAC)
CDMA/ DMB	Operational/Advisory	Specialistico CD[7]	NC3B/NAC
ESCD	Advisory	Specialistico	NIS
ACT	Operational/Advisory	Globale	NMIS
NC3A / NC3B	Operational/Advisory	Globale	ACT
NCSA	Operational	Specialistico	ACT
NCIRC	Operational	Specialistico CD	NCSA
CCDCOE	Advisory	Specialistico CD	ACT/SNs

Tabella 1: elenco dei principali enti coinvolti nella Cyber Defence NATO e loro caratterizzazione.

Il ***Consiglio Atlantico*** (o **"NAC",** cioè North Atlantic Council) è il massimo organo politico decisionale della NATO e come tale ad esso spetta il controllo globale sulla politica e sulle attività NATO, anche in materia di cyber defence.

Il ***Defence Policy and Planning Committee*** **(DPPC)**[8] ha il compito di elaborare proposte a livello politico (come, ad esempio, la preparazione di documenti di politica di Cyber Defence della NATO o la creazione della CDMA) e di sottoporle per l'approvazione al Consiglio Atlantico.

La ***Emerging Security Challenges Division*** **(ESCD)** è un' articolazione del NATO International Staff presso il Quartier Generale di Bruxelles, ed è l'organismo di più recente istituzione (agosto 2010). La divisione, creata per analizzare e relazionare a livello politico problematiche di sicurezza di nuova generazione e/o di tipo non tradizionale, si si articola su cinque sezioni di cui la prima tratta proprio di Cyber Defence, mentre le altre si occupano di terrorismo, proliferazione delle armi di distruzione di massa, nucleare e sicurezza energetica (aree esplicitamente indicate dal nuovo Concetto Strategico NATO approvato nel vertice di Lisbona[9]).

La ***Cyber Defence Management Authority*** **(CDMA),** concepita nel 2008 nell'ambito della prima stesura del documento di Cyber Defence Policy NATO e ufficialmente riconosciuta durante il vertice di Bucarest dello stesso anno, è la massima autorità specializzata in Cyber Defence e agisce come unico responsabile di coordinamento in materia. Essa raccoglie nella sua *board* (CDMB) tutti gli attori (membri effettivi e osservatori) interessati a vario titolo alla Cyber Defence. La CDMB si riunisce almeno due volte l'anno e si adopera per lo sviluppo di strategie, di assessment e di specifici documenti di implementazione operativa relativamente agli aspetti di Cyber Defence della NATO.

L'***Allied Command Trasformation,*** **ACT,** è il Comando NATO per la *trasformazione*[10], ovvero l'organismo incaricato di valutare i cambiamenti in atto negli ambienti in cui la NATO è chiamata ad operare e fornire le adeguate risposte di adattamento in termini di strutture e capacità per l'efficacia delle operazioni future.

Il ***NATO Consultation, Control and Command Board,*** **NC3B,** costituisce il principale organo di consultazione per gli aspetti tecnici e di implementazione di Cyber Defence.

L'agenzia **NC3A** ha responsabilità specifiche per l'identificazione delle esigenze operative (ricerca, sviluppo, sperimentazione) e soprattutto per l'acquisizione e l'attuazione delle capacità NATO di Cyber Defence (stipula di contratti e procurement).

---

[7] Cyber Defence.

[8] Il DPCC ha sostituito l' *Executive Working Group*, abrogato nel giugno del 2010.

[9] Specificatamente: artt. 9, 10, 12, 13, 19 dello "*Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organisation*" (Lisbon , 19 Nov. 2010)

[10] Definita nel *NATO Glossary of Terms and Definitions* (AAP-6(2010)) come "*A continuous and proactive process of developing and integrating innovative concepts, doctrines and capabilities in order to improve the effectiveness and interoperability of military forces*". (30-Jun-2005)

La ***NATO CIS Services Agency*, NCSA**, attraverso il dipendente NCIRC *(NATO Computer Incident Response Capability*) Technical Center, è responsabile della fornitura di servizi informatici tecnici e operativi di sicurezza in tutta la NATO.

L' **NCIRC** ha un ruolo chiave nel rispondere a qualsiasi aggressione informatica contro l'Alleanza, e può essere considerato il CERT[11] della NATO. Esso, oltre a fornire i mezzi per la gestione e la segnalazione di incidenti e la diffusione di importanti informazioni sugli stessi agli organi di gestione della sicurezza e agli utenti, accentra e coordina le azioni di *incident handling* in un unico punto, eliminando di conseguenza duplicazione di attività.

Il ***Cooperative Cyber Defence Center of Excellence*, CCDCOE**, è un ente dislocato a Tallinn (Estonia), del tutto particolare nel suo genere. Come gli altri Centri di Eccellenza accreditati in ambito NATO, questa istituzione non fa parte della catena di comando NATO e viene finanziata e alimentata nella sua componente umana su base volontaria da 9 Sponsoring Nations NATO, tra cui l'Italia che fà parte del "gruppo fondatore" fin dal 2008. Il Centro fornisce servizi estremamente specialistici di ricerca, studio, consulenza e formazione tecnica sul cyber warfare, ed è considerato una sorta di importante "think tank" a cui la NATO fà sempre più spesso riferimento (il CCDCOE viene regolarmente invitato alle riunioni della CDMB).

La situazione attuale

Immediatamente subito dopo il vertice NATO di Lisbona (Novembre 2010), il Consiglio Atlantico ha ufficialmente assegnato al DPPC il compito di sviluppare un nuovo *concept* sulla politica di Cyber Defence della NATO, con l'intento dichiarato di giungere alla definizione di un documento di policy ufficiale, derivante dal concept, entro la fine di giugno 2011. Il concept è stato rilasciato nella sua versione finale (rev.6) il 7 marzo, e approvato dai Ministri della Difesa dei paesi NATO il 10 marzo.

I punti della Dichiarazione del Vertice di Lisbona e del relativo Concetto Strategico che sono stati indicati come linee guida sulle quali basare la stesura del documento di policy sono[12]:

- il ricorso alla *cooperazione* con organizzazioni internazionali e con il settore privato;
- l'esigenza della *centralizzazione* della Cyber Defence;
- la necessità di incrementare le capacità NATO di prevenzione, rilevazione, difesa e recupero di operatività dagli attacchi informatici;
- il bisogno di migliorare l'integrazione della consapevolezza delle minacce, dei sistemi di allarme e delle azioni di risposta cyber con i paesi Membri;
- il raggiungimento della *Full Operation Capability* (FOC) per NCIRC entro il 2012

Viene inoltre fatto riferimento alla necessità di proteggere le Infrastrutture Critiche nazionali ICT dei singoli stati membri, prescindendo quindi dall'ambito esclusivamente militare.

Contemporaneamente alla redazione del concept, ACT ha prodotto due draft di studio:

- "Emergent Requirement Request - ACT Response To Lisbon Summit Taskings on Cyber Defence" (fine 2010);
- "HQSACT Point Paper: Cyber Transformation Activity Within ACT" (Gennaio 2011);

tipicamente finalizzati a definire il *piano di azione* attraverso cui gli orientamenti politici di Cyber Defence saranno messi in pratica, e ha richiesto a NC3A di accelerare la definizione del "*Cyber Defence Capability Framework*", un documento dettagliato nel quale vengono elencate e definite in maniera tassonomica tutte le *capacità* tecniche di cui la NATO e le Nazioni devono dotarsi per implementare una difesa efficace a 360°. La seconda revisione del documento è stata ufficialmente rilasciata da NC3A il 28 Febbraio 2011.

Stante quanto sopra considerato, il documento di policy di Cyber Defence in via di sviluppo dovrebbe caratterizzarsi, rispetto al 2007, per una valenza di più ampio respiro in quanto non

[11] Computer Emergency Response Team. Un' entità funzionale attiva H24, inserita all'interno di una qualsiasi organizzazione, appositamente concepita per gestire e contrastare in tempo reale incidenti e minacce informatiche.

[12] Direttamente derivabili dal paragrafo 19, punto ottavo dello "*Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organisation*" (Lisbon , 19 Nov. 2010)

contingente a una specifica situazione di crisi (non tralasciando tuttavia le "lessons learned" dai casi reali) senza però spingersi ancora all'assunzione di posizioni di una certa consistenza che avrebbero investito il Cyber Warfare di una importante maturità nel campo delle operazioni militari.

E' inoltre verosimile ritenere che la policy farà anche riferimento all'intenzione NATO di "*utilizzare anche i suoi processi di pianificazione della difesa al fine di promuovere lo sviluppo delle capacità di cyber defence delle nazioni alleate, aiutare le singole Nazioni su richiesta, e ottimizzare la condivisione delle informazioni, la collaborazione e l'interoperabilità*" e di collaborare "*strettamente con altri attori, come le Nazioni Unite e l'Unione Europea*". [13]

Conclusioni

Mai come allo stato attuale si è osservata una attività così intensa in ambito NATO relativa alle decisioni necessarie per definire una nuova politica di difesa informatica (o "Cyber Defence" che dir si voglia) adatta a contrastare efficacemente le minacce cyber potenzialmente inficianti gli assetti CIS dell' Alleanza e delle Nazioni facenti parte di essa.

Praticamente con cadenza mensile, negli ultimi sei mesi le consultazioni e le riunioni di coordinamento (specialmente in seno al DPPC e alla CDMB) si sono susseguite a pieno ritmo allo scopo di poter rispettare le scadenze temporali indicate nel documento di Strategic Concept del vertice di Lisbona, coinvolgendo tutti gli enti NATO elencati in precedenza sia per le decisioni del caso che per fornire pareri tecnici.

L'accelerazione nettamente percepibile è un chiaro indicatore della determinazione e dell'attenzione che i paesi membri della NATO stanno ponendo nell' affrontare in modo organico e definito le problematiche di Cyber Defence.

Ovviamente questo non è ancora abbastanza. Un livello di sicurezza relativamente accettabile potrà essere raggiunto soltanto dopo l'implementazione nella pratica delle indicazioni fornite, obiettivo per il quale sarà necessario tempo e investimenti (molto probabilmente, NC3A e/o NCSA sarà incaricata del procurement delle soluzioni tecniche solo a partire dal 2012).

Ma soprattutto, le singole nazioni dovranno fare la propria parte[14], in quanto la responsabilità della difesa sul proprio territorio rimane ad esse devoluta, e vulnerabilità insolute in ambito nazionale possono mettere a rischio l'intera Alleanza.

Il percorso per conseguire questi obiettivi non sarà nè breve nè semplice, ma appare tracciato in maniera appropriata al contesto di minaccia dalla nuova policy NATO, e, nella fattispecie, l'Alleanza e le Nazioni sembrano avere ben compreso i rischi derivanti dalla mancata adozione di un adeguato dispositivo di Cyber Defence.

Dott. Marco LUDOVICO

Grazie al ten. Col. De Falco per questo quadro che è obbiettivamente è molto articolato ma che ci da una percezione dei tempi dello sviluppo Nato: l'appuntamento è proprio per giugno del 2011.

Invito l'Ing. Luca Izzotti, Direttore Pianificazione Strategica e di Prodotto, della Selex Sistemi Integrati del Gruppo Finmeccanica, per darci il punto di vista dell'Industria della Difesa. Passiamo, quindi dal quadro della Difesa in ambito Nato, al quadro nazionale che sarà illustrato dall'Ing. Izzotti, prima e che il Dott. Domenico Vulpiani concluderà. Prego Ing. IZZOTTI.

[13] Art. 40 dello "*Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organisation*" (Lisbon , 19 Nov. 2010)

[14] Come anche richiesto nella Parte V (*Recommendations*), punto 63, comma c. del Rapporto "*NATO and Cyber Defence*" (documento NATO P.A. 173 DSCFC 09 E bis), di Sverre Myrli.

Ing. Luca IZZOTTI
Direttore Pianificazione
Strategica e di Prodotto
Selex - Sistemi Integrati

SITUAZIONE NAZIONALE

Apporto dell'Industria

Ringrazio voi tutti ed il Cestudis per questa opportunità. Il mio compito è quello di illustrare come l'industria nazionale sta rendendo disponibile al Paese queste capacità e le strategie che si stanno seguendo.

Vista la brevità di tempo a disposizione, analizziamo subito quali sono i pilastri strategici secondo cui ci stiamo movendo ed investendo.

La minaccia Cyber costituisce una sfida reale e concreta all' economia ed alla sicurezza del nostro paese. E' mio compito prospettare sinteticamente come l' industria nazionale si stia preparando a rispondere a questa sfida ed indicare le principali ricadute strategiche di questi sforzi.

Finmeccanica, tramite la sua capofila per i Sistemi Integrati Selex SI, ha in corso significativi investimenti atti a traguardare varie esigenze strategiche :

Rendere disponibile al paese prodotti di difesa Cyber che coprono il completo spettro operativo che va dalla protezione delle reti e delle informazioni agli strumenti di intelligence e di indagine sino alla detezione ed al contrasto di attacchi di tipo cyber altamente organizzati

Traguardare le iniziative in ambito NATO/UE posizionando l' Italia in prima fila fra i paesi che possano contribuire ad una Difesa coordinata dell' alleanza intercettando efficacemente i piani di sviluppo e di procurement europei

Supportare efficacemente l' export nazionale dei sistemi complessi proponendo soluzioni integrate di CyberDefence atte a distinguere sul mercato i propri prodotto rendendoli competitivi e completi

A tale scopo ha sviluppato la soluzione denominata Cybershield che comprende un approccio integrato olistico al problema ove la soluzione operativa è data da un' efficace integrazione di procedure operative, organizzazione, architetture HW e SW e soluzioni tecniche specifiche.

Cybershield costituisce il concetto architetturale di riferimento sviluppato dall' industria nazionale sulla base di investimenti atti allo sviluppo di programmi e prodotti complessi afferenti alla classe dei Grandi Sistemi Integrati.

Travalicando i confini della soluzione tecnologica l' approccio alla soluzione integrata di sistema prevede un progetto integrato fra organizzazione, processo di impiego ed architettura tecnica , capitalizzando esperienze nazionali precipue quali gli investimenti nei più recenti ed avanzati sistemi sia civili che militari , quali i sistemi di controllo del traffico aereo , il sistema di protezione civile, i sistemi di difesa navali (Nave Cavour e Orizzonte) e Forza NEC.

La soluzione Cybershield si differenzia dai convenzionali approcci al problema in quanto ha l' obbiettivo di rendere disponibile una sala di controllo nazionale delle infrastrutture informatiche adatta a supervisionare e coordinare la reazione agli attacchi cyber in ottica analoga a quella delle grandi sale di controllo operative.

Spiccano le esigenze di integrazione dei dati di intelligence che spesso nel caso della cyber è un' intelligence su fonti open (internet e social network-OSINT) ove la grande mole di data i richiede motori automatici di analisi delle informazioni. Di rilievo il concetto del data fusion applicato alla realizzazione di una CYOP (Cyber Operational Picture) sulla base della fusione di diverse informazioni che vanno dall' analisi tecnica dei comportamenti dei calcolatori interessati alla

supervisione degli stati di connessione con l' identificazione di schemi di connessione precipui di situazioni di attacco cyber.
Ad integrazione di tali funzioni sono preposti i sistemi di gestione degli eventi. Essi vanno ascritti eminentemente alla iniezione di sw specifici per contrastare le minacce ed alla disconnessione cosciente di tratti di rete ed unità di calcolo.
Al di là di tali classi di strumenti sussitono le potenzialità per le implementazioni di sw di exploitation (raccolta informazioni) e di contrasto il cui impiego rientra nei compiti specifici di tipo militare.

Anche da ciò consegue l' interazione con le tematiche dell' Information Assurance e della gestione del rischio, tematiche che indirizzano verso un forte coordinamento da parte dell' Autorità Nazionale della Sicurezza, analogamente a quanto avvenuto in numerosi paesi esteri.

La soluzione sin qui descritta costituisce un riferimento importante per molti mercati internazionali. Esistono esigenze specifiche a livello di forze armate e di sicurezza per sistemi di difesa cyber. Tali richieste si articolano in strategie molto diverse da paese a paese comprendendo gare di procurement articolate e relativamente frammentate in cui la design authority viene avocata ai livelli istituzionali, così come attività di procurement che prevedono l' esistenza di grandi aziende con il ruolo di integratore di sistema. In questo secondo caso l' esperienza pregressa e la collaborazione con i propri enti governativi costituisce un elemento discriminante per la competitività del sistema paese Italia, fornendo altresì l'opportunità per accordi operativi bilaterali e multilaterali.
Al di là delle esigenze specifiche di Cyber, ogni sistema complesso che viene proposto sul mercato internazionale deve soddisfare i requisiti di sicurezza cyber oltre che di sicurezza dell' informazione in generale. Tale logica si applica a tutte le categorie dei sistemi che vanno dalle reti di sorveglianza militare e civile ai singoli sistemi di protezione delle infrastrutture.

In tale contesto l' Italia viene vista come un riferimento fondamentale stante le sue capacità innovative e la disponibilità alla collaborazione ed al trasferimento di tecnologia, elementi che vengono sempre visti come una chiave inderogabile di accesso al mercato soprattutto nei paesi emergenti. In tale contesto l' industria nazionale si trova ben posizionata.

In conclusione la cyber costituisce non solo un problema di sicurezza nazionale ma anche un' opportunità di export industriale e di accordi internazionali nel caso in cui l' organizzazione e gli investimenti siano adeguati alla percezione che del nostro paese hanno i principali mercati emergenti nonché quelli tradizionalmente consolidati.
Grazie per l'aqttenzione

Dott. Marco LUDOVICO

Grazie Ing. Izzotti, per la puntualità e le sue parole perché è confortante sapere che c'è un apporto delle nostre Imprese che è significativo ed altamente specialistico, in questo caso del Gruppo Finmeccanica.

L'ultimo intervento è affidato al dott. Domenico Vulpiani la cui qualifica è quella di Consigliere Cyber Security del Ministero dell'Interno. Il Dottor Vulpiani ha una lunghissima esperienza nel settore e mi fa molto piacere affidagli ultima parte di questa sessione per darci il quadro nazionale nel dettaglio delle sue articolazioni e, possibilmente, su quelle problematiche che sono state accennate dal Gen. Ramponi all'inizio.Prego Dottor Vulpiani.

Dott. Domenico VULPIANI
Consigliere Cyber Security
del Ministero dell'Interno

Grazie Marco ed un particolare ringraziamento al Sen. Ramponi per avermi invitato a questo simposio e a tutti voi che siete qui ad ascoltare.

Cercherò, nel tempo che ho a disposizione, quali sono soprattutto i ruoli che nel nostro Paese sono svolti nell'ambito della cyber security, intesa come argomento generale.

"E-voting" - un termine a cui in Italia non siamo ancora abituati, ma che è apparso con frequenza, in questi giorni, sui quotidiani di tutto il mondo, associato all'Estonia, dove in occasione della recente elezione del Parlamento si è fatto ricorso al voto elettronico.

L'iniziativa è stata accolta in maniera contrastante[15], non senza perplessità da parte di chi ritiene che il computer da cui viene inviato il voto *on line* possa essere bersaglio di un'attività di *hackeraggio* e favorire così brogli elettorali.Non sono poi così lontani i tempi in cui l'Estonia appariva vittima del primo episodio di *cyber war*.

Nel 2007, a seguito della rimozione del soldato di bronzo dalla piazza principale, i più importanti siti istituzionali del Paese furono presi di mira da un violento attacco di tipo D-dos che in breve tempo ridusse al silenzio le banche, i ministeri, gli organi di informazione e via dicendo.

Quell'attacco è stato il primo di una serie di *cyber attacks* che si sono poi registrati qua e là, in svariate parti del *cyber space*. Per fare un esempio recente, basti pensare a quelli messi a segno dagli *hacktivist* di Anonymous contro PayPal, Visa, Mastercard, in risposta alla decisione di bloccare il trasferimento di denaro verso Wikileaks.

Un'attività che si è giovata della partecipazione di una folta comunità internauta, costituitasi attraverso i *social network* che hanno offerto la piattaforma privilegiata di divulgazione dei link utili per partecipare all'attacco.

Del resto sul potere di aggregazione dei *social network* non è necessario aggiungere niente, bastano le recenti rivolte in Nord Africa ed in Medio Oriente e prima ancora la manifestazione pacifica in Belgio, a cui hanno partecipato 50.000 persone chiamate a raccolta da 5 frequentatori di Facebook.

I *social network* hanno dimostrato che il passaparola funziona e che il passo dalla **denuncia** di una situazione di malcontento ad un'organizzazione di una rivolta violenta e coordinata, può essere breve. Soltanto nei giorni caldi della rivolta in piazza Tahir, sono stati creati su Facebook 32.000 gruppi di oppositori al regime egiziano.

La rete si è trasformata nell'ultimo ventennio da semplice vettore di informazioni e conoscenza a strumento imprescindibile per il mantenimento della stabilità economica e sociale del nostro e di altri Paesi.Questa "creatura" è cresciuta, per così dire, prima ancora che gli Stati si avvedessero completamente della potenza e della pervasività del mezzo e che quindi attuassero per tempo politiche volte a salvaguardare l'integrità della rete, nonché degli *users*, siano essi privati che pubblici.Ci si è trovati, pertanto, di fronte a sfide sempre nuove da contrastare.

---

15 A tal proposito, il Segretario di Stato Americano Hillary Clinton ha detto: *"in the 20 years since Estonia's independence, the country has become a successful model for others, with* ***its internet voting****, cyber innovations, commitment to good governance, the rule of law, and fiscal responsibility".*
Mentre Barbara Simons, esperta di sicurezza informatica ed ex ricercatrice dell' IBM negli USA ha dichiarato : "*non è ancora arrivato il momento per questa innovazione e, secondo me, si tratterebbe di un errore*", aggiungendo che non sarà possibile accertare se il computer dal quale il voto viene inviato sia, in realtà, vittima di "*hackeraggio*"."*Realizzare brogli nelle votazioni on-line è più semplice che rubare soldi nell'e-banking*

In prima istanza quelle legate al ***cyber crime***, ovvero al furto d'identità digitale, alla clonazione di carte di credito, alla diffusione di materiale pedopornografico *on line*, alla violazione del diritto d'autore.

A cui hanno fatto seguito minacce afferenti al ***cyber espionage,*** che, quando perpetrato a danno di aziende che gestiscono servizi essenziali per il Paese o che sono depositarie di conoscenze specialistiche ed innovative, assume dei tratti di allarmante problematicità. Frequenti sono due tipologie di attacchi, volti o a trafugare il patrimonio informativo, il cosiddetto *know how* o anche volti a paralizzare ogni attività.

Infine il ***cyber terrorism,*** ovverosia l'impiego della rete da parte di gruppi terroristici a scopo di propaganda, nonché di reclutamento di nuovi adepti e perché no? come mezzo per condurre *cyber attacks.*E qui, entra in gioco la nuova frontiera della criminalità *on line*, quella che concentrando tutte queste possibilità ha come soggetto agente non più l'*hacker*, ma gli stessi Stati, desiderosi di misurarsi e farsi valere nella ***cyber war***.

A tal proposito, non sono mancati episodi anche più recenti, come gli attacchi, ancora anonimi, rivolti contro la centrale nucleare iraniana di Natanz, per mezzo di un virus, lo Stuxnet ideato ad hoc.Ebbene, il nostro Paese ha cercato di fornire una risposta a questo scenario, operando su più livelli che vanno da quello **meramente conoscitivo** della minaccia che viaggia in rete a quello più sostanziale **di contrasto**, affidato ad una normativa adeguata e soprattutto agli organi di Polizia.

1.Ambito conoscitivo del reato condotto a mezzo internet.

1.1 Ogni utente della rete, dal privato cittadino alle aziende, attua delle politiche di **difesa logica passiva** (per così dire **privata**) del proprio perimetro, mediante l'impiego dei mezzi messi a disposizione dalle grandi multinazionali produttrici di antivirus, come la McAfee e la Symantec ed in linea con quanto disposto dalle leggi ed in particolare dal codice della *privacy*[16].

A tali difese, se ne aggiungono poi altre di tipo pubblico ed istituzionale. Nell'ambito della standardizzazione degli apparati *software* ed *hardware*, va pertanto menzionata l'attività svolta dalla **Fondazione Bordoni** - sottoposta alla vigilanza del Ministero dello Sviluppo Economico – che ha altresì la finalità di promuovere il progresso scientifico e l'innovazione tecnologica.

1.2 Svolgono, invece un'attività di allarme su eventuali vulnerabilità dei **sistemi operativi** *e* dei principali applicativi, oltre che sulla diffusione di *virus*, *worm, trojan*, i **CERT** *"Computer Emergency Response Team,"* a cui è altresì demandato il compito di segnalare delle contromisure da intraprendere nel caso di incidente informatico.

Un esempio importante di Cert è quello della Difesa creato presso lo Stato Maggiore Difesa che fornisce assistenza in tal senso agli utenti della Difesa nel campo delle reti telematiche.

Un altro esempio è il Cert- SPC - Computer Emergency Response Team del Sistema Pubblico di Connettività, istituito presso l'allora CNIPA ed operativo dall'inizio del 2008, che si pone come referente centrale delle Unità Locali di Sicurezza[17] per la prevenzione, il coordinamento e supporto informativo e l'analisi degli incidenti di sicurezza in ambito SPC.

Attualmente sono 65 le ULS delle Amministrazioni centrali che costantemente dialogano con il Cert-SPC, alimentando il flusso informativo e favorendo uno scambio tempestivo di notizie in materia di sicurezza informatica.

1.3 Per quanto riguarda **la sicurezza delle infrastrutture critiche**, il compito di analisi e studio è invece, demandato al Tavolo PIC (Protezione Infrastrutture Critiche) un tavolo di lavoro, istituito nel 2007, presso l'ufficio del Consigliere Militare della Presidenza del Consiglio, al quale partecipano rappresentanti dei ministeri principali.

---

16 Il Decreto legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali" all'art.34 ha stabilito delle norme precise per il trattamento dei dati con strumenti elettronici.

17 In base al DPCM del 01/04/2008 ogni amministrazione centrale che aderisce all'SPC deve dotarsi di un'**Unità Locale di Sicurezza (ULS)** a cui è affidato il compito di attuare le misure di prevenzione degli incidenti informatici, nonché la gestione operativa degli stessi.

Con Ordinanza di Protezione Civile n. 3836 del 30 dicembre 2009 è stato stabilito che il nucleo di Difesa Civile e NRBC della Protezione Civile costituisca anche Segreteria per il coordinamento interministeriale delle attività nazionali, anche in consessi internazionali, riguardanti le infrastrutture critiche, alle dipendenze funzionali del Consigliere militare del Presidente del Consiglio dei Ministri.

1.4 Con decreto Presidente del Consiglio dei Ministri del 05 maggio 2010 è stato costituito presso la Presidenza del Consiglio dei Ministri, il Nucleo Interministeriale situazione e pianificazione (NISP), quale organismo di supporto alle attività del CoPS Comitato Politico Strategico, allo scopo di gestire situazioni di crisi, quindi situazioni emergenziali, non certo la sicurezza nella quotidianità, che resta affidata agli organi di *law enforcement*.

2.Ambito di repressione dei reati condotti a mezzo Internet.

Le difese finora menzionate sono tutte passive, mentre l' azione di contrasto al *computer crime* è in gran parte affidata alle investigazioni delle forze di polizia ed in particolare della Polizia di Stato.

La competenza principale[18] le è stata attribuita con Decreto del Ministero dell'Interno. La norma dispone infatti che …"*sia rimesso alla competenza primaria della Polizia di Stato garantire, in via generale, l'integrità e la funzionalità della rete informatica*"…

Anche in materia di pedofilia *on line*, la norma prevede che la prerogativa ad intervenire con specifici strumenti investigativi (attività sottocopertura ed acquisti simulati) sia del Servizio Polizia Postale e delle Comunicazioni.[19]

Inoltre la legge 155/2005 all'art.7 bis ha attribuito, "*ferme restando le competenze in materia dei Servizi informativi e di Sicurezza*" all' "*organo del Ministero dell'Interno per la sicurezza e per la regola*rità *dei servizi di telecomunicazione*" e cioè al Servizio Polizia Postale e delle Comunicazioni, il compito di assicurare *"i servizi di protezione informatica" delle Infrastrutture Critiche Informatizzate (CII) individuate con decreto del Ministro dell'Interno."*

A seguito di tali disposizioni normative, sono stati realizzati tre organismi, quali il Commissariato virtuale di PS[20], il CNCPO[21] (Centro Nazionale per il Contrasto alla

---

[18] Decreto del Ministro dell'Interno 28 aprile 2006 "Riassetto dei comparti di specialità delle Forze di polizia", che segue un percorso storico iniziato sin dal 1992.

[19] Il legislatore è intervenuto due volte in materia di pedofilia *on line*: nel 1998 con la legge 3 agosto 1998 n.269, recante: "*Norme contro lo sfruttamento della prostituzione, della pornografia, del turismo sessuale in danno dei minori, quali nuove forme di schiavitù*", con la quale ha introdotto nel codice penale le fattispecie volte a sancire le condotte criminali circa lo sfruttamento sessuale dei minori attraverso la pornografia in rete. La legge 269/98 è stata poi novellata nella legge 06 Febbraio 2006, n.38, recante: *"Disposizioni in materia di lotta contro lo sfruttamento sessuale dei bambini e la pedopornografia anche a mezzo internet",* per renderla più rispondente alle esigenze di contrasto di alcuni aspetti della pedopornografia *on line*, particolarmente subdoli e che si erano rivelati impermeabili all' azione di Polizia.

[20] **Commissariato virtuale di PS** - portale dedicato a tutti gli utenti per denunciare, segnalare reati informatici (frodi on line, casi di phishing, clonazioni di carte di carte di credito) o comportamenti anomali, rilevati durante la navigazione, ovvero per chiedere informazioni.

[7] Il **CNCPO**, istituito con la legge 38/2006 ed inaugurato il 1 febbraio 2008, è destinato invece a coordinare le complesse attività di contrasto alla pedopornografia *on line*, in collaborazione con gli ISP (Internet Service Provider) e con le Onlus che si occupano del problema sotto l'aspetto sociale. Al CNCPO è, infatti, demandato il compito di stilare quotidianamente una *black list* dei siti a contenuto pedopornografico, da inviare ai provider, al fine di filtrare la navigazione verso di essi.

Pedopornografia on line) ed il CNAIPIC[22] (Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche), volti rispettivamente al contrasto del crimine informatico in genere, alla repressione dell'adescamento di minori *on line*, nonché della diffusione di materiale pedo-pornografico ed alla tutela delle infrastrutture critiche.

Tutte e tre le piattaforme tecnologiche poggiano su una stretta **collaborazione tra pubblico e privato**, che vede il coinvolgimento attivo in primis dei cittadini privati, nonché dei provider, delle Onlus,nel caso del CNCPO.

E così anche per il CNAIPIC, laddove la stipula di apposite convenzioni tra il Dipartimento di Pubblica Sicurezza con gli Enti o imprese private che forniscono servizi vitali per il Paese è prevista per legge. In tal modo sono avviate piattaforme di comunicazione privilegiata di dati e modalità di intervento più efficaci per la repressione dei *cyber attacks*[23].

Sottesa alla realizzazione dei tre Centri vi è la consapevolezza che parlare di *cyber attacks* altro non è che parlare di reati, commessi nel *cyber space*, ma pur sempre reati.

Vi è altresì il convincimento, supportato dall'esperienza, che i *cyber attacks*, per quanto abbiano finalità diverse e siano diretti contro differenti obiettivi, si avvalgano sempre **delle stesse tecniche.** Per fare un esempio, i pedofili si nascondono nel mondo *underground,* al pari dei terroristi.

Questi due ordini di motivi inducono a concludere che, di fronte ad un attacco informatico, quindi ad un reato, la cui matrice sia inizialmente oscura, la prima risposta non può che non essere di natura investigativa, ovverosia di un organo con elevate competenze tecniche e soprattutto con poteri di polizia giudiziaria.Considerato anche che, una volta assodata la provenienza dell'attacco e le finalità, sarà sempre compito di tale organo attuare, per quanto di propria competenza, la

---

[8] Infine il **CNAIPIC** - realizzato in attuazione della legge 155 del 31 luglio 2005, rappresenta una sorta di centrale operativa a cui le Infrastrutture Critiche indirizzano segnalazioni di attacchi presunti o conclamati, a cui fanno seguito le indagini, volte a rintracciare i colpevoli. L'esperienza insegna che difficilmente un soggetto della rete colpito, ad esempio, da un virus renda noto ad altri di essere stato colpito. Il timore del danno d'immagine prevale sulle esigenze collettive di sicurezza. La comparazione di segnalazioni di attacchi a obiettivi diversi, ma condotti con tecniche analoghe è invece molto utile per risalire ad una matrice comune. Così come spesso è fondamentale l'attività *d'intelligence* che il CNAIPIC conduce con lo scopo di sondare preventivamente quali soggetti, o organizzazioni criminali o terroristiche abbiano l'intenzione e gli strumenti per insinuarsi nelle vulnerabilità dei sistemi informativi delle IC, per colpirle, o anche per sottrarne o alterarne il patrimonio informativo. L'obiettivo principale del Centro pertanto è quello di ottenere quante più informazioni possibili dalle vittime, garantendo però ad esse la comprensibile riservatezza.

[23] Attualmente, gran parte delle infrastrutture critiche informatizzate individuate dalla norma, ovverosia quelle operanti nel settore economico, energetico, dei trasporti e delle comunicazioni, hanno già scelto la strada delle convenzioni.

Quella più datata nel tempo è con Poste Italiane, a cui ha fatto seguito nel settore economico quella con Banca d'Italia, Unicredit Sp.A, Banca Intesa ABI, CONSOB, mentre nel settore delle Comunicazioni figurano Ansa, Telecom Italia, Vodafone e Rai. Nel settore dei trasporti hanno aderito a questa strategia ACI, ATM, Ferrovie dello Stato, Enav; infine nel settore energetico Terna ha siglato l'accordo.

Come si può notare un panorama variegato, ma suscettibile ancora di variazioni, giacché altre convenzioni sono in attesa di essere definite, in particolar modo quelle con soggetti che detengono il *know how* tecnologico italiano.

Infine in tale ambito, va altresì considerata **la European Electronic Crime Task Force** realizzata Polizia, Poste Italiane, e US Secret Service, a protezione dell'infrastruttura finanziaria che si pone tra i suoi obiettivi l'analisi e lo studio dei fenomeni di criminalità informatica che possono minare la sicurezza dei servizi telematici offerti agli utenti.

repressione.Questo modello ha prodotto finora risultati lusinghieri, nel contrasto a tutte le manifestazioni della *cyber threat*[24].

Per concludere, un cenno va all'attività svolta dal CNAPIC, che con **l'Operazione Catanzaro**, condotta nel contrasto al *cyber terrorism* ha portato all'arresto dell'imam della moschea di Sellia Marina (CZ) e dei suoi due figli accusati di addestramento ad azioni violente con finalità di terrorismo. Nella circostanza, sono stati rinvenuti supporti di memoria informatica contenenti istruzioni e manualistica per il confezionamento e l'uso di armi ed esplosivi, per rendere anonime e sicure le comunicazioni telematiche, nonché per il compimento di sabotaggi di sistemi informatici.

Più di recente il CNAIPIC si è occupato degli attacchi rivolti contro sito del Governo Italiano e prima ancora è stato impegnato dell'Operazione Stop Intrusion.

Nel corso di tale Operazione si è avuto modo di constatare che alcune banche dati istituzionali di interesse pubblico erano state violate e che erano stati effettuati migliaia di accessi abusi.[25]

A prima vista, quello che poteva apparire come un *cyber attacks* volto a compromettere gli interessi statali, si è poi rilevato, al termine delle indagini, un atto a valenza esclusivamente criminale.

Conclusioni.

La disamina di questi pochi casi mostra come nella sicurezza del *cyber space* sia fondamentale il ruolo svolto dal Ministero dell'Interno in prima battuta, nonché dagli altri organi di polizia, sebbene in forma limitata all'attività di supporto tecnico-scientifico, dai Carabinieri, nelle indagini che riguardano reati tradizionali e dalla Guardia di Finanza per quanto concerne le frodi *on line* e le clonazioni dei titoli di pagamento elettronico.

---

[24] Ad esempio, nel campo delle frodi *on line* si è registrato un trend positivo che ha portato ad un aumento delle persone denunciate ed arrestate dal 2006 al 2010. Si è passati dalle 216 persone denunciate in stato di libertà nel 2006 alle 396 del 2007, alle 723 del 2008, alle 986 del 2009 fino alle 1240 del 2010, così come per gli indagati sottoposti a provvedimenti restrittivi, passati dai 45 del 2006 ai 73 del 2007, a 70 nel 2008, fino ai 113 del 2009 ed i 66 del 2010.
Risultati analoghi per quanto concerne la pedopornografia. In tale ambito si è passati dalle 370 persone denunciate in stato di libertà nel 2006 alle 388 del 2007 fino alle 1167 del 2008, alle 1186 del 2009 ed alle 582 del 2010. Per quanto concerne gli arrestati, si è passati dai 16 del 2006 ai 33 del 2007 , ai 39 del 2008 , ai 53 del 2009, fino ai 63 del 2010.
Per avere un' idea dell'attività svolta in questo settore, basti pensare che soltanto nella recente operazione **RESCUE**, coordinata da Europol e condotta dalla Polizia Postale di Catania sono state indagate 459 persone, arrestate altre 71 e soprattutto identificati 173 minori vittime di abusi. Tale operazione ha permesso di individuare una rete internazionale di pedofili con collegamenti in varie parti del mondo: Australia, Belgio, Canada, Grecia, Islanda, Italia, Olanda, Nuova Zelanda, Polonia, Romania, Spagna, Svizzera, Regno Unito e Stati Uniti.

[25] La tecnica impiegata mirava ad appropriarsi direttamente delle credenziali di accesso dei dipendenti delle pubbliche amministrazioni interessate, mediante messaggi ingannevoli di posta elettronica provenienti da Enti presunti noti. La tecnica utilizzata sfruttava la buona fede di ignari dipendenti delle pubbliche amministrazioni che, raggiunti da falsi messaggi di posta elettronica, contenenti un malware, non esitavano a digitare le proprie credenziali e ad effettuare tutte le operazioni richieste - che una volta registrate, venivano inviate direttamente su server collocati all'estero. Laddove un criminale italo-rumeno con dei complici raccoglieva i dati provenienti da centinaia di computer compromessi sul nostro territorio e se li rivendeva ad agenzie di investigazione o di recupero crediti.

Alcune vicende come il caso Wikileaks, o il caso del *network* dei giovani *hacktivist* di Anonymous, che attaccano di volta in volta il nemico di turno che si oppone in rete ai loro ideali libertari e anarcoidi, oppure episodi, ritenuti, a torto o ragione, di *cyberwarfare*, mostrano come la rete si possa trasformare in teatro di operazioni di spionaggio o di natura bellica.
In tali situazioni è indispensabile un intervento dei servizi di informazione o delle forze armate nella fase di risposta all'aggressore, soprattutto laddove l'intervento di polizia risulti non di stretta competenza.

Tuttavia tali interventi suppletivi debbono avere come accade nel mondo reale, percorsi autonomi, target e tempi diversi da quelli giudiziari.

Ciò non toglie che per il futuro sia auspicabile una maggiore collaborazione e scambio di informazioni tra tutti gli "attori" pubblici e privati che operano per la sicurezza del *cyber space*, pur nel rispetto dei ruoli e delle competenze di ciascuno di essi.

Sotto il profilo politico, i nuovi *social network*, come Facebook e Twitter, si stanno rivelando uno strumento formidabile in mano agli stati democratici per sostenere gli insorti e gli oppositori ai regimi dittatoriali, come è accaduto nel nord Africa.

I *social network*, favorendo la diffusione degli ideali di libertà attraverso la rete, si stanno rivelando un'arma di tipo cibernetico più potente ed efficace di bombe e carri armati.
Appare di straordinaria attualità il pensiero di Sun Tzu, (VI-V sec.a.C) espresso nel "L'arte della guerra": "*combattere e vincere cento battaglie non è prova di suprema eccellenza: la suprema abilità consiste nel piegare la resistenza del nemico senza combattere*."

La tutela degli strumenti di espressione è essa stessa un'arma, in quanto costituisce la massima garanzia di un'informazione "trasparente," non strumentalizzata, non inquinata da ideologie politiche, ma prodotta dagli utenti stessi che fino a ieri ne erano i fruitori. Difficilmente vi potranno essere "guerre sporche," condotte all'insaputa dell'umanità, senza che qualcuno ne sia testimone con un video, con una foto, con un messaggio,pubblicato in rete.

Grazie per l'attenzione.

SECONDA SESSIONE

Coordinatore:
Gen. C.A.(r) Bruno SIMEONE

Relatori:
Gen. Biagio ABRATE
Amm.Sq. Alessandro PICCHIO
Pref. Gianni DE GENNARO
Ing. Massimo SARMI

Gen. C.A.(r) Bruno SIMEONE
Coordinatore

Buongiorno a tutti e diamo l'avvio alla sessione. L'introduzione che ha fatto il Sen. Ramponi e lo sviluppo dei lavori della prima sessione hanno evidenziato che in ogni ambiente il sistema "internet" è oggi molto vulnerabile da attacchi di vario tipo. Sono stati ripetutamente citati gli attacchi di *cyber crime, cyber terrorism, cyber espionage, cyber war* ed altre minacce. In questa seconda sessione, che mi accingo a presentare, sentiremo che la minaccia cibernetica viene vissuta, viene valutata, vieni contrastata, in ambito delle varie sedi Istituzionali dello Stato. Acquisiremo, quindi, il pensiero sulle valutazioni e sulle attività poste in atto in Organismi diversi. Ci parleranno personaggi di vertice di queste organizzazioni ed in particolare: il Capo di Stato Maggiore della Difesa, il Gen. Abrate; il Consigliere Militare del Presidente del Consiglio, Amm. Sq. Picchio; il Direttore del Dipartimento Intelligence e Sicurezza della presidenza del Consiglio, Pref. De Gennaro; l'Amministratore Delegato delle Poste Italiane, l'ing Sarmi, che non è potuto intervenire nella prima sessione. Sarà invece assente, come è stato già detto, il Pref. Antonio Manganelli. Prenderà adesso la parola il Gen. Biagio Abrate, Capo di SMD.

Gen. Biagio ABRATE
Capo di Stato della Difesa
òè

Buongiorno a tutti. son riuscito a partecipare a questo convegno anche se, come potete immaginare, gli impegni di questi giorni mi chiamano H 24 sulle vicende, in particolare, della Libia. Ringrazio dell'invito il Sen. Ramponi ed il Cestudis. Sono certo di ripetere, in parte (perché non ero presente durante la prima sessione), quando può essere stato detto nei precedenti interventi e pertanto sarò rapido nelle mie espressioni.

1. Caratteristiche evolutive di conflitti e crisi: comprendere dove e come le F.A. italiane saranno chiamate ad operare.

Il carattere dei conflitti e delle crisi evolve continuamente, poiché riflette normalmente i cambiamenti della società in cui essi si generano. Gli scenari che oggi si presentano e che già sono riscontrabili in parte nei teatri operativi in cui le nostre forze operano, possono definirsi assai complessi se non addirittura caotici.

Questi scenari impongono necessariamente uno strumento militare parte di un dispositivo intergovernativo e molto probabilmente multinazionale che, seguendo un approccio multi-dimensionale[26], deve supportare la tutela degli interessi nazionali verso gli *"end states"* definiti dalla politica.

E' chiaro quindi che il "focus" militare è, e deve rimanere, centrato sulle "operazioni", includendo con esse, le capacità e le forze necessarie alla loro pianificazione e conduzione. Operazioni che ci vedranno coinvolti principalmente, e probabilmente, fuori dai confini nazionali, ma anche pronti a supportare l'eventuale contributo richiesto per possibili crisi (calamità naturali e non solo) all'interno della madrepatria.

Di fatto, però, l'evoluzione delle minacce, rese ancora più insidiose da meccanismi di globalizzazione facilmente utilizzabili, rendono sempre più permeabili e artificiose le frontiere tradizionali. Non dico nulla di nuovo affermando, quindi, che la canonica distinzione tra problematiche in materia di difesa e quelle di sicurezza potrebbe essere molto sfumata, e molto più difficile da percepire, specialmente nel dominio cibernetico.

[26] Cfr. documento di riflessione congiunto MAE-DIFESA "Approccio Nazionale Multi-Dimensionale alla gestione delle crisi", edizione dicembre 2010 di SMD III/CID.

E' già ormai acclarato che la soluzione di queste crisi richiede un'azione "integrata", concertata o multi-dimensionale (sulla base della cosiddetta metodologia del *"Comprehensive Approach"*), sin dalla fase di prevenzione, poiché i problemi complessi necessitano di un approccio non lineare, mirato all'utilizzo di tutti gli elementi del potere di una Nazione[27], e quindi delle future Coalizioni, per generare effetti coerenti verso un *"end state"* condiviso.

Tutto questo si complica ulteriormente quando, ai noti ambienti operativi (terrestre, marittimo ed aereo), si affiancano ambienti emergenti quali lo spazio e il cyberspazio.

2. Cyberspazio in ottica militare: implicazioni principali

Mentre la conoscenza e l'accesso allo spazio extra atmosferico sono già da alcuni anni oggetto di numerose iniziative, vi sono una serie di sfide, ancora non definite, che attengono al cyberspazio. Un nuovo "terreno" di possibili minacce che spinge, oltre i confini nazionali, il dispiegamento degli assetti di difesa, entrando in un mondo virtuale costituito dal web, dal flusso di Internet, dai sistemi e dalle reti di comunicazione.

E' evidente che le minacce operanti in tali ambienti, e le azioni anche non cinetiche ivi condotte, possono creare effetti, di ampiezza e possibile ripercussione a carattere strategico, potenzialmente afferenti all'intero "sistema Paese".

Nell'*"Information Age",* le tecnologie (dell'Informazione e Comunicazione-ICT), garantiscono un elevato grado di dominanza ma, nel contempo, costituiscono un forte elemento di vulnerabilità. Se solo si pensa a quali e quanti settori sono dipendenti da queste tecnologie (energia, trasporto, finanza, *"governance"*, infrastrutture, salute, informazione, difesa[28] e sicurezza) e dalle relative infostrutture, si evince chiaramente quale possa essere il livello di rischio al quale ci si espone.

E' quindi legittimo chiedersi come agire per comprendere, mantenere l'accesso e poter operare nel *"cyberspace",* al fine di conservare e proteggere gli interessi nazionali. Il mondo militare, in particolare, vive da qualche anno una fase di profonda trasformazione verso il concetto "*Network Enabled Capabilities"* (NEC), principalmente applicato all'infostruttura C4ISTAR[29]. Tali capacità[30] di *"Defence Information Infrastructure"* (DII) sono un requisito importantissimo per le operazioni nonché, d'altro canto, un elemento di criticità in termini di interoperabilità nazionale e di Coalizione. L'obiettivo finale è quello di raggiungere una condizione di preminenza o di vantaggio, nei confronti dei potenziali opponenti e/o avversari, nel dominio informativo, tecnologico, organizzativo e decisionale.

3. Le iniziative della Difesa nel dominio Cibernetico

A seguito degli eventi occorsi in alcuni paesi dell'Est, la Difesa ha adottato una serie di provvedimenti per contrastare con più efficacia la minaccia cibernetica alla proprie reti, perseguendo, in sinergia con la NATO, l'aggiornamento della propria politica di *"Cyber Defence"*. Sono state, al riguardo, emanate specifiche direttive tecniche[31] e di politica di sicurezza[32], dettate

---

[27] Cfr. documento di riflessione congiunto MAE-DIFESA "Approccio Nazionale Multi-Dimensionale alla gestione delle crisi" - paradigma del DIME (Diplomatico, Informativo/Interno, Militare ed Economico), edizione dicembre 2010 di SMD III/CID.

[28] Un esempio di rischio notevole è l'ipotesi in cui un sistema di "Blue Force Tracking", che fornisce ai Comandanti la posizione delle forze amiche, fosse compromesso modificando in modo randomico le tracce reali.

[29] Command, Control, Communication, Computer, Intelligence, Surveillance, Target Acquisition and Reconnaissance.

[30] Cfr. Defence Information Infrastructure (DII).

[31] SMD-I-013 – Procedure di risposta agli incidenti informatici riguardanti le reti telematiche della Difesa, ed. 2008.

[32] SMD-I-019- Politica di sicurezza per i sistemi di telecomunicazione e informatici non classificati della Difesa, ed. 2009 e JIC-011-Joint Integrated Concept per le Computer Network Operations.

istruzioni in merito alla *"governance"*[33] e iniziata la costituzione, anche se ancora in una forma embrionale, di unità organizzative, denominate *"Computer Emergency Response Team"* (CERT), sia a livello centrale, il CERT Difesa[34], sia presso le Forze Armate, con compiti di contrasto e di contenimento di attacchi informatici alle rispettive reti.

Ciò ha richiesto il potenziamento della collaborazione e dello scambio informativo con le corrispondenti strutture di sicurezza in ambito nazionale (in particolare con il "Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche della Polizia di Stato" - CNAIPIC) ed internazionale (CERT dei Paesi alleati e della NATO), e con il "*Cooperative Cyber Defence Centre of Excellence"* (CCD COE) di Tallin in Estonia[35].

In tale ambito preme rimarcare anche l'organizzazione e conduzione di esercitazioni nazionali di *"Cyber Defence"*, denominate "*Cyber Shot*", in concomitanza con la corrispondente esercitazione NATO *"Cyber Coalition"* a cui, nel 2010, hanno partecipato, tra gli altri, la Presidenza del Consiglio dei Ministri, vari centri specialistici di settore e ben 13 nazioni tra cui l'Italia in qualità di "*Player*" e 11 nazioni come osservatori.

4. La minaccia nel Cyberspazio: maggiori criticità

Il quadro generale sinora descritto presenta, di fatto, un notevole numero di sfide ed incertezze, che tenterò di delineare:

- primo: questa situazione di dominanza è nota ai potenziali opponenti; essi pertanto difficilmente accetteranno di confrontarsi su questo piano, dove partirebbero svantaggiati;
- secondo: le nazioni tecnologicamente avanzate espongono, su questo ambiente, numerosi e sensibili centri di gravità[36] che devono essere trattati e gestiti in maniera integrata, per evitare pericolosi ed inefficaci frammentazioni e/o duplicazioni di sforzi e di risorse;
- terzo: l'utilizzo massivo di reti di connessione informatizzate può divenire elemento di vulnerabilità facilmente attaccabile, specialmente se non incentrato su una struttura dell'informazione agile, dinamica, standardizzata e gestibile[37] e se non accompagnato da una diffusa consapevolezza nella gestione delle informazioni, di garanzia e protezione delle stesse[38]. Ciò richiede lo sviluppo di capacità anche coerenti con gli impegni internazionali che la Nazione ha assunto[39];
- quarto: le risorse umane necessarie ad operare nel settore del *"cyberspace"* richiedono livelli di specializzazione, formazione e addestramento, attualmente insufficienti a soddisfare le esigenze;

---

[33] CCSI: Comitato di Coordinamento per la Sicurezza ICT (*Information and Comunication Tecnology*), a guida SMD II Reparto.

[34] CERT Difesa: costituito, sul modello NATO, da un Coordination Centre presso SMD RIS, deputato agli aspetti di coordinamento ed Early warning sulle minacce cibernetiche e dal Technical Centre, presso il Comando C4 Difesa, per la gestione tecnico-operativa, in piena sinergia con le strutture delle FA, delle attività di risposta agli attacchi.

[35] l'Italia è sponsor. Presso il CCD COE un Ufficiale dello Stato Maggiore della Difesa svolge l'incarico di Scientist.

[36] Caratteristiche, potenzialità o località da cui una nazione, un'alleanza, un complesso di forze militari o di altra natura traggono la propria libertà d'azione, la forza o la volontà di combattere (SMD G 024).

[37] "Linee di indirizzo per lo sviluppo della Defence Information Infrastructure (DII) Nazionale" – direttiva SMD NEC 004, edizione 2009, emanata da SMD VI.

[38] Information Management ed Information Assurance che includono nuove organizzazioni, procedure e tecnologie.

[39] Ad esempio: Afghan Mission Network (AMN) accelera ed anticipa alcuni concetti e realizzazioni, pianificati e concordati in ambito NATO (dai quali derivano Forza NEC e DII), che ora in maniera pressante sono ritenuti requisiti urgenti per una migliore condivisione, ed al tempo stesso, garanzia e protezione delle informazioni in Teatro.

- quinto: le implicazioni legali connesse a questo ambiente operativo sono ancora non chiare ed oggetto di approfondimento e dibattito[40], anche in seno all'Alleanza Atlantica;
- sesto: l'industria nazionale di settore si trova ad affrontare una nuova sfida produttiva che risulta essere di interesse strategico per quanto concerne le garanzie di affidabilità in termini di *"hardware"* e *"software"*. Ciò dovrà comportare un approccio innovativo all'ingegnerizzazione dei sistemi e dei relativi servizi, che preveda il coinvolgimento dell'industria sin dalla definizione dei requisiti[41], onde meglio collocare le nuove realizzazioni nel *"cyberspace"*.

5. **Conclusioni**

Come militare, quindi, ribadisco che il nostro obiettivo principale anche nel *"cyber space"* è quello di continuare ad assicurare la condotta delle operazioni, che anche nel nostro concetto di base nazionale[42] abbiamo definito proprio "*Computer Network Operations*" (CNO). Operazioni militari che si basano sullo sviluppo capacitivo di tre pilastri fondamentali: la difesa[43], l'analisi e lo sfruttamento dei dati[44] e l'attacco[45]. Ritengo le prime due prioritarie, almeno nel medio periodo, per i seguenti motivi:

- innanzitutto perché coerenti con lo spirito della nostra Costituzione;
- poi perchè coerenti con gli orientamenti di *"policy"* che si stanno delineando in ambito alleato ed europeo. Su questo aspetto il comparto tecnico-militare può fungere da elemento di armonizzazione in merito a possibili *"standards",* prescrizioni, disposizioni e requisiti provenienti dalla NATO e dall'Unione Europea, massimizzando l'interoperabilità con la Presidenza del Consiglio e con gli altri Dicasteri oltre che con le altre Amministrazioni del Paese;
- ed infine, ripeto, la difesa e l'analisi e lo sfruttamento dei dati costituiscono i due pilastri su cui si catalizzano naturalmente gli interessi militari, quelli intergovernativi e quelli della società civile nazionale, sia nel pubblico che nel privato, prospettando quindi opportunità di concrete e sinergiche condivisioni.

Quello che manca è però un meccanismo che armonizzi tali capacità e prerogative, così come già sottolineato dal Comitato Parlamentare per la Sicurezza della Repubblica (COPASIR) e stigmatizzato dalla recente iniziativa della Presidenza del Consiglio dei Ministri[46].

In tale contesto, le sfide che dovremo affrontare esigono che l'Italia sviluppi la volontà e la capacità di fare sistema, di essere protagonista con proprie iniziative, sia in campo nazionale che in quello internazionale. Iniziative che, a differenza del passato, prevedano una completa integrazione multi-dimensionale delle strutture decisionali, militari e civili, per garantire risposte pronte, efficaci e giuridicamente compatibili.

---

[40] E' in atto un dibattito, a livello nazionale ed internazionale, sul livello di danno, causato da un attacco cibernetico, oltre il quale sia possibile adottare, per legittima difesa, misure di carattere offensivo per bloccare o ridurre gli effetti dell'azione malevola. Nel merito, la stessa comunità internazionale , ovvero la NATO e l'UE, sta disquisendo sul tema, partendo da posizioni non sempre coincidenti.

[41] "Metodologia e Framework Architetturale del Ministero della Difesa (MDAF) per lo sviluppo e la descrizione di architetture C4ISTAR e NEC", direttiva SMD NEC 002, edizione 2010.

[42] Joint Integrating Concept 011 - CNO, edizione 2009, emanata da SMD III/CID.

[43] Cyber Defence: " the application of security measures to protect CIS infrastructures components against cyber attack" (JIC 001 –CNO).

[44] Cyber Exploitation : "l'azione intrapresa per avvalersi di un computer, nonché delle informazioni ivi contenute, per ottenere un vantaggio" (JIC 001 –CNO).

[45] Cyber Attack: "azione, condotta nei confronti di un avversario dal territorio nazionale o dall'estero, attraverso l'utilizzo, anche combinato, di computers, sistemi informatici, telematici e cibernetici, al fine di distruggere, disattivare, rendere inaccessibili, alterare, smembrare i sistemi stessi o dati, informazioni e servizi in essi contenuti. Ciò in forma parziale, totale, permanente o temporanea "(JIC 001 –CNO).

[46] Cfr. riunione del Nucleo Interministeriale di Situazione e Pianificazione (NISP) del 17 gennaio 2011.

Grazie dell'attenzione.

Gen.C.A. Bruno SIMEONE

Ringrazio il Gen. Abrate per quanto ci ha detto, soprattutto per averci confermato che le Forze Armate stanno lavorando in questo settore, che ci sono spazi di miglioramento ma che, sotto il controllo e l'egida della Nato, sicuramente raggiungeremo obiettivi migliori. Lascio la parola all'Amm. Sq. Alessandro Picchio che è Consigliere Militare del Presidente del Consiglio.

Amm. Sq. Alessandro PICCHIO
Consigliere Militare del
Presidente del Consiglio

Già da tempo la Presidenza del Consiglio dei Ministri è particolarmente sensibile e pone moltissima attenzione alla problematica della Cyber security; ciò grazie anche all'opera quotidiana di informazione e sensibilizzazione svolta in materia dal Dipartimento informazioni per la sicurezza, che ha come riferimento di vertice il Presidente del Consiglio dei Ministri.

Come noto l'assetto legislativo oggi vigente, in base al dettato costituzionale e alle leggi in vigore, attribuisce al Presidente del Consiglio dei Ministri funzioni di indirizzo, impulso e coordinamento come "primus inter pares", ferme restando le responsabilità dei singoli Ministri (art. 95 Costituzione); tale assetto pone importanti limiti e vincoli all'azione del Governo in tema di sicurezza.

Tuttavia, un significativo passo avanti nell'assetto organizzativo è stato comunque fatto con l'emanazione, il 5 maggio 2010, del Decreto del Presidente del Consiglio dei Ministri sull' "Organizzazione nazionale per la gestione di crisi" che ha introdotto alcune interessanti novità nell'architettura politico-decisionale nazionale, dando impulso alle attività sia di prevenzione che di gestione di possibili situazioni di crisi riguardanti la sicurezza nazionale.

Infatti con quel Decreto è stato formalmente istituito il Comitato Politico Strategico (CoPS) ed il suo organismo di supporto, il Nucleo Interministeriale di Situazione e Pianificazione (NISP). In aggiunta, per un'indispensabile e sentita esigenza di chiarezza e di linguaggio comune, sono state introdotte con esso alcune definizioni, condivise a livello interministeriale, dei termini da utilizzare in occasione di situazioni di crisi.

Il Comitato, che si riunisce sotto la presidenza del Presidente del Consiglio, è costituito da un nucleo permanente di quattro Ministri, Affari esteri, Interno, Difesa, Economia e finanze, integrato a seconda della situazione da fronteggiare, da altri Ministri.

Al Comitato partecipano anche il Sottosegretario di Stato alla Presidenza e segretario del Consiglio dei Ministri, il Segretario Generale della Presidenza, il Dirigente Generale del Dipartimento Informazioni e Sicurezza, il Capo della Protezione Civile, i Consiglieri Diplomatico e Militare del Presidente del Consiglio, il Segretario Generale del Ministero Affari Esteri, il Capo di Stato Maggiore della Difesa, il Direttore Generale della Pubblica Sicurezza e il Capo del Dipartimento dei Vigili del Fuoco, del soccorso pubblico e della difesa civile.

Il Nucleo interministeriale di situazione e pianificazione è presieduto dal Sottosegretario di stato alla Presidenza del Consiglio dei Ministri; di esso fanno parte rappresentanti ad hoc designati dai Ministri e dagli altri membri del Comitato politico strategico. Il Nucleo si avvale anche del supporto della Commissione Interministeriale Tecnica di Difesa Civile (CITIDC) istituita dal Ministro dell'Interno ed ha principalmente funzioni di coordinamento e di promozione dell'attività interministeriale, di analisi di situazione e di stimolo della programmazione e pianificazione operativa per contrastare situazioni di crisi, in particolare quando interessano più Ministeri, di avanzare proposte da sottoporre al Comitato politico strategico per le decisioni.

Comitato politico strategico e Nucleo interministeriale svolgono le loro funzioni in via continuativa e permanente, promuovendo le attività di valutazione e pianificazione interministeriale

nel settore della Sicurezza nazionale ed assicurando, in caso di crisi, l'attivazione di un tempestivo processo decisionale.

L'assetto organizzativo descritto, prova tangibile della sensibilità del Governo per i problemi della sicurezza, ormai sperimentato per oltre un anno in alcune attività specifiche ed esercitazioni, ha trovato impiego reale nei recenti critici avvenimenti che hanno interessato i Paesi del Nord Africa e del medio oriente. Il Nucleo interministeriale ha infatti operato ed opera come elemento di supporto al Comitato permanente di Ministri per la crisi in Libia, che ha avviato la sua attività sin dai primi eventi (ndr: ha composizione e funzioni coincidenti con quelle del CoPS).

Nel Comitato politico strategico e nel Nucleo interministeriale affiancato hanno trovato anche adeguata concreta risposta le raccomandazioni rivolte al Governo dal COPASIR nella relazione del luglio 2010 su "Possibili implicazioni e minacce per la sicurezza nazionale derivanti dall'utilizzo dello spazio cibernetico", in particolare sulla necessità di una cabina di regia in grado di gestire questa tematica di elevatissima sensibilità.

Il Nucleo interministeriale, presieduto dal Sottosegretario Dr. Letta ed integrato dagli altri Ministeri ed Enti interessati, si è riunito il 17 gennaio scorso per fare un punto di situazione e discutere sullo specifico tema "sicurezza nazionale e spazio cibernetico", tenendo conto non solo dell'ampio quadro di situazione che emerge dalla relazione del COPASIR, ma anche delle conclusioni del Vertice dei Capi di Stato e di Governo della NATO, tenutosi a Lisbona il 20 novembre 2010, che ha promulgato il nuovo "concetto strategico" dell'Alleanza Atlantica con il quale viene posta in rilievo la necessità di sviluppare la difesa contro attacchi cibernetici (cyber defence), impegnando i Paesi alleati a "develop further ability to prevent, detect, defend against and recover from cyber attack".

Il sommario quadro d'insieme emerso dalle relazioni delle diverse Amministrazioni su capacità, attività, organizzazione e risorse dedicate presentate nella riunione ha evidenziato che:

non sembrerebbero esservi in prima analisi sovrapposizioni di competenze e di attività tra le Amministrazioni; emergono primari, ciascuno per materie di competenza, i ruoli del Dipartimento informazioni per la sicurezza, dei Ministeri dell'interno, della difesa, dello sviluppo economico (aspetti di certificazione hardware), ma anche degli esteri per rappresentare adeguatamente anche nei massimi consessi politici multilaterali la posizione, partecipazione o contribuzione italiana alle iniziative internazionali e alleate;

se dovesse essere rilevata un'aggressione sarebbe molto probabilmente necessaria una valutazione interministeriale per determinare la tipologia dell'aggressione e l'eventuale esigenza di misure di reazione o risposta delle diverse Amministrazioni, opportunamente coordinate; in questa valutazione gioca un ruolo essenziale il fattore tempo, ovvero l'esigenza della tempestività e dell'immediatezza, perché nel cyberspazio i tempi di reazione consentiti sono minimi, dell'ordine dei secondi o dei minuti al massimo, ed il fattore tempo diviene dunque cardine di tutta l'attività;

alcune indispensabili funzioni, come ad esempio la protezione operativa con presenza in rete, l'early warning, il contro-attacco ed altre, andrebbero potenziate, opportunamente pianificate e programmate, in modo da assicurare lo svolgimento in modo più completo ed esaustivo.

Tenuto conto dell'assoluta importanza della tematica e della necessità di predisporre anche in Italia i più adeguati assetti organizzativi e difensivi con una strategia unitaria, il Presidente del NISP ha concluso rilevando la necessità di costituire, con apposito DPCM, un gruppo di studio e di lavoro di alto profilo, composto da personalità di grandissima esperienza e professionalità, supportato da tecnici delle Amministrazioni ed integrato da esperti a livello scientifico o accademico che provveda:

alla ricognizione delle strutture esistenti presso le varie Amministrazioni valutando la loro adeguatezza, in relazione alle rispettive competenze e in funzione della potenzialità delle minacce;

all'esame, ai fini meramente di studio, degli assetti organizzativi realizzati in altri Paesi, con particolare riguardo a quelli facenti parte dell'UE, della NATO e del G8;

a formulare una proposta organizzativa per mettere a sistema le strutture esistenti e, se necessario, ad indicare ed elaborare i conseguenti interventi normativi, per realizzare uno strumento

nazionale in grado di affrontare la minaccia cibernetica e di rispondere a livello massimo di difesa, in un contesto interministeriale, interfacciandosi efficacemente a livello internazionale, in particolare con l'Unione Europea e con la NATO.

Il DPCM è in elaborazione, ai sensi della legge 400/1988, che consente al Presidente del Consiglio dei Ministri, con proprio decreto, di "disporre la costituzione di gruppi di studio e di lavoro composti in modo da assicurare la presenza di tutte le competenze dicasteriali interessate ed eventualmente esperti anche non appartenenti alla pubblica amministrazione".

In base a questo esame e studio, il Nucleo interministeriale di situazione e pianificazione proporrà al Comitato Politico Strategico le soluzioni più opportune, cercandone la condivisione con tutte le Amministrazioni.

La tempistica di tale attività, che prevede la definizione di un progetto d'insieme, potrebbe richiedere però alcuni mesi; nel frattempo è però urgente iniziare ad operare con la massima efficacia ed efficienza con le forze già oggi in campo, quanto prima possibile, prevedendo forme di stretta collaborazione e procedure di coordinamento tra addetti ai lavori delle varie Amministrazioni e, senz'altro ove possibile, anche il coinvolgimento di grandi organizzazioni private. Il NISP, presieduto dal Sottosegretario di Stato alla Presidenza del Consiglio, si presenta al momento come l'elemento di organizzazione già pronto a svolgere nel settore del cyber space, infrastruttura che supporta attività in ogni campo della vita produttiva e non della nazione e come tale sicuramente critica, la funzione di coordinamento, uno stretto ed efficace coordinamento, e di promozione dell'attività interministeriale, di analisi di situazione e di stimolo della programmazione e pianificazione operativa, di "valutazione di eventuali aggressioni" e di esigenze di iniziative interministeriali di protezione e contrasto.

Sia in ambito NATO che Unione Europea, il cyber space è un'infrastruttura oggetto di particolare attenzione, in quanto presenta le caratteristiche per essere candidata a infrastruttura critica per eccellenza. Per gli aspetti che interessano direttamente l'Alleanza atlantica è attualmente il Ministero Difesa, in coordinamento con il Ministero degli Affari esteri, l'Amministrazione deputata ad interfacciarsi con le altre Nazioni. Invece, per le molteplici attività che vengono sviluppate in ambito Unione Europea, è stata istituita presso la Presidenza del Consiglio, nell'Ufficio del Consigliere Militare, la Segreteria per le infrastrutture critiche. Tale Segreteria cura il coordinamento interministeriale delle attività Nazionali, anche in ambito internazionale, e delle attività tecniche e scientifiche per l'individuazione e la designazione delle infrastrutture critiche europee, in particolare per gli adempimenti della direttiva Europea 114 del 2008. In questi primi due anni della sua entrata in vigore, ai fini della sua applicazione sono stati inseriti solo i settori energia e trasporti, ma la Commissione europea sta elaborando ora i criteri per inserire nell'applicazione anche il settore cyber.

Grazie per l'attenzione

Gen. C.A. Bruno SIMEONE

Un particolare ringraziamento all'Amm. Sq. Alessandro Picchio che ci ha dato una visione di quelli che sono gli assetti della struttura d'intervento nel settore cyber in ambito della Presidenza del Consiglio, in ambito struttura Governativa e ci fornito anche una proiezione di quanto potrà avvenire. Lascio ora la parola al pref. Gianni De Gennaro che è il Direttore del Dipartimento Intelligence e Sicurezza della Presidenza del Consiglio.

Pref. Gianni DE GENNARO
Direttore Dipartimento Intelligence e Sicurezza - Presidenza del Consiglio

Desidero innanzitutto ringraziare e complimentarmi con il Senatore Ramponi, con il quale mi trovai completamente d'accordo quando, qualche mese fa, mi prospettò l'idea di organizzare questo convegno, la cui piena riuscita è ora evidente, sia per l'autorevolezza delle presenze che per la qualità degli interventi di coloro che mi hanno preceduto.

Vorrei utilizzare il tempo di cui dispongo per illustrarvi l'approccio culturale con il quale noi del Dipartimento delle informazioni per la sicurezza ci accostiamo ad una tematica così complessa come la minaccia informatica. Per dare concretezza alla mia esposizione partirò da un esempio tratto dalla cronaca.

Il 20 gennaio scorso ho letto un lancio d'agenzia che diceva: "*La Commissione europea ha deciso di sospendere temporaneamente le transazioni della borsa delle emissioni di CO2 (Emission trading system, ETS) da ieri sera sino almeno al 26 gennnaio, a causa di ripetuti attacchi informatici e frodi ai registri nazionali di cinque paesi Ue e riguardanti la vendita di circa 2 milioni di quote per un totale stimato di 28 milioni di euro".*

L'episodio mi ha incuriosito, sia perché è una materia che conoscevo assai poco, sia perché poi ho visto che la stampa aveva ripreso la notizia in modo molto evidente. Ho quindi approfondito l'argomento e ho potuto facilmente constatare che in gioco non c'erano solamente grandi cifre economiche, ma la potenzialità stessa del sistema industriale di una nazione.

Dunque, se globale è la potenzialità della minaccia, altrettanto globale deve essere l'approccio culturale al problema, se vogliamo trovare soluzioni efficaci.

La prima considerazione da fare è che risulta ormai evidente come la minaccia cibernetica possa mettere a dura prova qualsiasi tipo di mercato finanziario; a riprova di ciò sta il fatto che l'episodio dei "certificati verdi" ha coinvolto più Paesi.

Da qui la seconda considerazione, sempre in termini di approccio culturale: la stampa che ha ripreso la notizia l'ha collegata all'azione di organizzazioni criminali, cosa che è certamente possibile, visto che i certificati oggetto dell'attacco informatico sono stati subito rivenduti, ottenendo risultati economicamente rilevanti.

Ma se non si fosse trattato di un attacco di origine criminale, e l'azione fosse invece riconducibile all'industria di un altro Paese, determinata a mettere in crisi l'industria concorrente? E se dietro a quell'industria ci fosse stata un'istituzione che faceva riferimento anche al Paese?

Sono solamente ipotesi, ma illustrano bene la necessità di affrontare questa materia con un approccio culturale più ampio da parte di tutti i sistemi e sottosistemi esposti alla minaccia cibernetica e, in maniera particolare, da parte del Sistema di informazione per la sicurezza.

Abbiamo visto coniugare la parola *cyber* con molte altre: *cyber war*, *cyber espionage*, *cyber crime*, *cyber attack*, *cyber security*, *cyber defence* ma penso che il termine onnicomprensivo sia *cyber threat*, cioè la minaccia cibernetica. E penso anche che una sola parola non ci è consentito accostare a *cyber*: *fear*, la paura.

Non ci è consentita la paura perché ormai il cyber spazio è una dimensione del mondo globalizzato, e l'uso di internet è parte integrante delle nostre abitudini e delle nostre capacità relazionali.

Non possiamo quindi permetterci alcun tipo di panico informatico. Ricordo il passaggio all'anno 2000, quando il rischio del *millennium bug* indusse ad adottare consistenti predisposizioni: in quel caso, la consapevolezza del rischio, pur notevolissimo, non si tradusse in paura. In un mondo globalizzato, che parla la lingua del web, bisogna semplicemente imparare a convivere con questa minaccia e a difenderci da essa.

In questo caso, difenderci significa saper organizzare i sistemi di protezione. L'Amm. Picchio ha fornito delle delucidazioni e ci ha detto che c'è una precisa volontà della Presidenza del Consiglio – anche io ho partecipato alle riunioni cui si faceva riferimento – di organizzare il sistema al meglio: è tempo di farlo, perché come sistema Italia siamo forse in ritardo rispetto ad altri Paesi.

E proprio guardando alle scelte adottate da Paesi come il Regno Unito, gli Stati Uniti, la Germania e altri, devo dire che non concordo pienamente con l'impostazione del Sen. Gasparri, perché credo che non ci si possa limitare al mero coordinamento e si debba invece pensare a una unità di comando e di controllo.

Sono cresciuto con "il coordinamento" e posso assicurarvi che è faticosissimo, perché il sistema funziona solo se c'è una forte volontà di farsi coordinare.

Il Gen. Abrate ci ha dato un quadro chiaro e ben preciso della sensibilità che esiste, anche a livello internazionale, per un settore tra i più delicati, come quello che è affidato alla sua responsabilità: di fronte a minacce così gravi occorre quindi andare oltre il concetto di coordinamento, anche perché ci sono tutte le potenzialità per fare al meglio il nostro lavoro.

La minaccia informatica si muove su un terreno apparentemente immateriale ma è terribilmente concreta, come dimostra in maniera eloquente il caso dei "certificati verdi" che ho prima citato: a seguito del mancato acquisto dei certificati verdi l'industria si trova in difficoltà nell'emissione di anidride carbonica ed è limitata nelle sue potenzialità.

Lo stesso esempio ci consente di vedere altre caratteristiche della *cyber threat*: essa è puntiforme ed è difficilmente prevedibile, tanto che ha spiazzato l'UE costringendo Bruxelles a chiudere le contrattazioni per i "certificati verdi". E, aggiungo, tocca gli interessi che la legge di riforma dei servizi di informazione, ha individuato con precisione (interessi politici, militari, economici, scientifici, industriali) nell'affidarne la difesa alle nostre Agenzie, interna ed esterna, per controbattere le minacce all'integrità e all'indipendenza della Repubblica.

Infine, la minaccia può colpire – mi rifaccio ancora una volta all'esempio dei "certificati verdi" - gli interessi nazionali di più Stati.

Se queste sono le caratteristiche della minaccia, prima di concludere vorrei fare un accenno ai tratti salienti della difesa che, come già accennato, deve essere organizzata in termini di prevenzione, per ridurre quanto più possibile le sorprese e garantire al massimo le capacità di reazione. Una difesa che non può prescindere da una sinergia tra il pubblico e il privato - la presenza a questo tavolo del dott. Sarmi ne è la prova più significativa e concreta – vale a dire una difesa che coinvolga il sistema Paese nella sua globalità, in un quadro che veda le Istituzioni pubbliche fare leva sulla comunanza d'interessi con le Istituzioni private.

In questo quadro, la parte pubblica è chiamata a declinare verbi come coordinare, organizzare, fare squadra, mentre alla parte privata corrisponde un preciso dovere, che è poi anche un interesse: quello di giocare a pieno titolo ma con grande consapevolezza della responsabilità di essere della stessa squadra. Grazie.

Gen. C.A. Bruno Simeone

Un grazie particolare al Pref. De Gennaro e lascio la parola all'Ing. Sarmi che è l'Amministratore Delegato delle Poste Italiane il quale ci parlerà del progetto italiano, cioè quello che può essere il punto di vista delle Mondo Civile su quelle che sono le problematiche del cyber war. Ingegnere a lei la parola.

Ing. Massimo SARMI
Amministratore Delegato
delle Poste Italiane

Grazie per l'invito e grazie al Pref. De Gennaro per il richiamo effettuato. La presenza oggi di numerosi rappresentanti della Società Civile evidenzia la rilevanza del tema trattato. Sono diverse le ragioni per cui noi ci siamo avvicinati all'argomento che, come già detto dal Pref. De Gennaro, non può trovare soluzioni se non attraverso una stretta cooperazione.

Per quale motivo Poste Italiane si pone al centro di questo tema? Poste Italiane è da sempre il soggetto di fiducia al quale viene affidata la corrispondenza scambiata tra due soggetti, un mittente ed un destinatario. Tale comunicazione deve essere tutelata.

Oggi mandare una email su internet, è come mandare una cartolina illustrata. Il concetto di comunicazione elettronica sicura riguarda tutti coloro che operano nel mondo civile, non solo il civile che scambia corrispondenza con un altro civile, ma anche il civile che dialoga con le Amministrazioni e viceversa.

Come si può pensare allo sviluppo dei servizi di governance se non si pone chiaro e forte il problema dell'identità elettronica? È evidente che non si può inviare un certificato, diffondere dati privati, dare comunicazioni di carattere sanitario, fra soggetti dei quali non si conosce l'identità.

A mio avviso, tutti questi fenomeni nella società civile non sono stati ancora adeguatamente affrontati, studiati e normati.

Il punto che intendo trattare, non è solo quello della difesa delle infrastrutture, anche perché egregiamente esposto dagli oratori che mi hanno preceduto. Sarebbe troppo facile affermare che ogni giorno le infrastrutture di Poste Italiane ricevono milioni di tentativi di attacchi, evidentemente generati da botnet che setacciano la rete alla ricerca di sistemi vulnerabili attraverso i quali infiltrarsi e propagarsi.

Io intendo trattare un tema che ritengo molto più importante per il mondo civile, quello della funzionalità dei servizi on line. Si pensi a cosa accadrebbe alle quaranta milioni di transazioni che ogni giorno vengono registrate sulla rete - infrastruttura, per inciso di Poste Italiane, canali on line ed infrastruttura diretta – se non venissero attuati, in tempo reale, dei controlli di sicurezza. Un conto è prescrivere, come si fa per le pasticche, un altro è utilizzare un oggetto come una chiavetta per assicurare un transazione, un conto è governare un sistema.

Un'azienda di servizi, io credo, debba sentire tutta questa sua responsabilità: non è possibile alzare barriere, isolarsi dal resto del mondo e lasciare senza servizi trenta milioni d'italiani.

Questo è a mio avviso, un problema molto importante, da analizzare in tutte le sue declinazioni, sia nel mondo dell'energia, sia negli altri ambiti industriali. Ci tengo ad evidenziare il mondo dei servizi, nella sua fruizione normale, che sappiamo essere adiacente ad altri mondi la cui trattazione e la cui competenza sale naturalmente di livello.

Esaminiamo come nasce questa iniziativa di Poste Italiane. Essa nasce con l'utilizzo di sistemi di pagamento su internet e risponde al crescente verificarsi di episodi di furto di identità. Nasce dalla necessità di Poste Italiane di garantire ai propri clienti il più alto livello di sicurezza delle transazioni, seguendole in tempo reale, prevenendo possibili furti di identità che potrebbero determinare prelievi illeciti di denaro.

Flussi di denaro questi, di importi significativi, come già detto in precedenza il Pref. De Gennaro, le cui somme a me risultano addirittura di gran lunga superiori rispetto a quelle citate.

Quando negli USA interagivamo con le Istituzioni preposte a questo tipo di problematiche, si parlava di frodi di 90 milioni di dollari per un istituto di credito, nell'arco di un solo fine settimana. Tali dati non devono necessariamente essere resi noti, ma a una platea così importante come questa, di addetti ai lavori, le suddette situazioni devono essere sicuramente prospettate per dare l'idea delle dimensioni di questi fenomeni.

Le catene, quindi, su cui operare sono a mio avviso, due:

La prima è quella del governo di un sistema che a sua volta non può che essere governato: un operatore di servizi come Poste Italiane, non può non avere dietro di se un regolatore che valuti quali siano le tipologie, gli investimenti, le attività, dei controlli da effettuare. Questa figura, però, oggi non esiste. Al di sopra del regolatore dovrebbe essere definito un sistema di norme, per definizione internazionali: anche queste non ci sono.

Quando ogni giorno siamo attaccati, anche dal famoso phishing, che è la forma più semplice e banale del tentativo di frode, e quando vediamo con precisione l'indirizzo IP da cui proviene, cosa possiamo fare? Una telefonata a qualcuno, magari ignaro, che sta dall'alta parte del mondo perché è stato triangolato, per chiedergli di spegnere il server? E' incredibile che, ancor oggi, per operare con strumenti così complessi ed articolati, non sia stato definito un profilo internazionale di regole.

Noi abbiamo costruito una fondazione senza fini di lucro, la Global Cyber Security Center (www.gcsec.org), al fine di supportare ed agevolare la definizione di suddetta regolamentazione, facilitando l'incontro e lo scambio di informazioni tra pubblico, privato, autorità ad ogni livello del mondo legislativo, del mondo regolatorio nazionale ed internazionale, della Polizia di Stato Postale.

La fondazione oltre a fornire supporto specializzato al Governo e alle imprese per la definizione di regolamentazioni, strategie e standard nazionali ed internazionali, favorisce la ricerca con altri centri di eccellenza nazionale ed internazionale, identifica e forma personale altamente specializzato da impiegare presso le Istituzioni e le Imprese Italiane.

L'obiettivo della Global Cyber Security Center è di fungere da acceleratore e aggregatore della conoscenza e cultura internazionale sulle problematiche riguardanti la Cyber Security e di diventare uno dei punti di riferimento più importanti a livello internazionale sulla Cyber Security, attraendo talenti, esperti e ricercatori da tutto il mondo.

Poste Italiane ha inoltre costituito, con la fondazione Global Cyber Security Center, la Polizia di Stato Postale ed i "Secret Services" statunitensi, consapevoli anch'essi della valenza internazionale di questi fenomeni, una task-force sul crimine elettronico. La Polizia di Stato e Poste Italiane sono invitate a partecipare ai lavori che si tengono a New York, con la presenza di Aziende Statunitensi, proprio per raccogliere tutte le tipologie d'informazione, sicuramente disponibili in ogni istituzione, ma che spesso si fa fatica a mettere insieme.

Quando il sito di Poste Italiane è stato violato, fortunatamente solo nella facciata, la Polizia di Stato ha individuato tre soggetti: un mitomane, un figlio di buona famiglia ed un rumeno, che si era trovato lì solo per caso, nella sua ricerca di afferrare soldi. Ma come si erano incontrati questi tre soggetti? Nel mondo stupendo del web, ci si incontra allo stesso modo con il quale si incontrano e si organizzano, ma con molta più fatica, tre amministrazioni dello Stato o con altrettanti soggetti privati. È questo il senso che dobbiamo richiamare e sentire proprio ogni giorno, perché la rapidità con cui si costruiscono disegni di tipo eterodosso non trova dall'altra parte un'analoga rapidità nel prevenire e nel reagire ai fenomeni.

Vanno coinvolti, e noi lo abbiamo fatto nel nostro settore, le Autorità Internazionali che presiedono la regolamentazione, e più specificatamente, le Agenzie dell'ONU (Unione Postale Universale, Unione Internazionale delle Comunicazioni) che hanno affidato a Poste Italiane il compito di costruire le specifiche dei servizi di comunicazione elettronica su internet.

Poste Italiane hanno inoltre ottenuto da ICANN, il soggetto deputato a dare ed a stabilire ogni giorno i nomi dei Domini su internet, un dominio di primo livello che si chiama .post, che possiede le caratteristiche di interoperabilità nella quale i civili possono trasferire le proprie comunicazioni con standard internazionali, mondiali, certi che la loro comunicazione su internet abbia caratteristiche di sicurezza.

Io chiedo che queste iniziative di Poste Italiane, ma anche di altre organizzazioni, trovino il coordinamento, così come effettuato da noi con i soggetti istituzionali precedentemente indicati.

Concludo con un augurio. Prima sentivo parlare di internet 2.0 (teniamo presente che stiamo cercando di difenderci sulla 1.0) molto "simpatico e bello" ma che rappresenta un disastro per i social network dove viene scambiato di tutto. Volendo guardare il futuro, l'auspicio è di trovarci pronti ad affrontare l'imminente arrivo del web 3.0 che, come gli addetti sanno, sarà veramente

l’impiego più ampio e globale di internet, l’internet in cui si tracceranno nello spazio le fisicità degli oggetti.

Ritengo necessaria una riflessione in merito, ma questa volta, da effettuare in anticipo.

Grazie.

TERZA SESSIONE

Relatori:
Sen. Francesco RUTELLI
Sen. Anna FINOCCHIARO
Sen. Maurizio GASPARRI
Sen. Sandro MEZZATORTA

CONCLUSIONI
Dott. Gianni LETTA

Sen. Francesco RUTELLI

Ringrazio il Gen. Ramponi, cui esprimo il mio apprezzamento per questa iniziativa, congratulandomi per la presenza di numerosi e autorevoli ospiti.

Nel luglio del 2010 il Comitato Parlamentare per la Sicurezza della Repubblica (CoPaSiR) ha approvato e trasmesso al Parlamento una relazione che ho personalmente curato e che analizza molti degli aspetti già evidenziati dagli interventi precedenti, da ultimo quello dell'Amm. Picchio.

Mi limito quindi a condividere alcune riflessioni sulla crescente attualità delle problematiche relative al rapporto tra cyber-spazio e sicurezza nazionale, verso le quali il lavoro svolto dal CoPaSiR si è dimostrato senz'altro tempestivo.

Vicende recenti come quella di Wikileaks o del virus informatico Stuxnet che avrebbe intaccato la capacità di arricchimento dell'uranio nelle centrali nucleari dell'Iran, o ancora l'importanza decisiva delle reti cibernetiche nei rivolgimenti politici in corso nel Mediterraneo e in Medio Oriente, dimostrano le implicazioni strategiche dei possibili utilizzi del cyberspazio.

Gli "addetti ai lavori" presenti in questa sala sono perfettamente consapevoli dell'impatto che la tecnologia di rete – da internet alle telecomunicazioni, ai network satellitari – sta avendo sulle rivolte del Nord Africa; vorrei citare i tre principali aspetti di questa interazione: il collegamento tra cittadini, autentici motori delle rivolte; la censura applicata dai governi assediati verso i network di comunicazione; l'attività, spesso clandestina, di reti internazionali schieratesi a favore e in supporto degli insorti.

Per la prima volta, in uno scenario così complesso e così vicino a noi, osserviamo come il terreno di battaglia, la formazione del potere e la sua contestazione siano parte di un paradigma che si crea e si distrugge innanzitutto nello spazio cibernetico.

Lo scenario globale è ormai attraversato da una serie di minacce asimmetriche; il cyber-spazio è il nuovo luogo per eccellenza di questa nuova forma di confronto e, potenzialmente, di conflitto.

Ben consapevoli di questa sfida, vorrei segnalare come, nel corso della recente Conferenza di Monaco sulla Sicurezza, alla presenza del Segretario di Stato americano Hillary Clinton e del Presidente russo Medvedev, Stati Uniti e Russia abbiano aderito alla proposta avanzata da un autorevole think tank internazionale sulla necessità di predisporre una sorta di "Trattato opranazionale" per la regolamentazione dell'utilizzo in termini offensivi e militari dello spazio cibernetico.

I cinque punti preliminari di un possibile, futuro accordo sono i seguenti:

- individuare nella rete cibernetica i soggetti e le categorie così detti "vulnerabili" prevedendo meccanismi di tutele internazionale;
- applicare al cyber space il concetti di emblema, di distintivo come fu per la Croce Rossa Internazionale;
- riconoscere a pieno titolo lo status di attore non statale e di cittadinanza digitale con un corredo di diritti e doveri di utilizzo e navigazione in rete;
- considerare l'estensione al cyber spazio l'applicabilità della convezione di Ginevra: neutralità, protezione, responsabilità,
- avviare l'esame dell'applicabilità dei concetti di "non pace" e "non belligeranza", anche al cyber space.

Di fronte a cambiamenti così rapidi e profondi, ritengo che le raccomandazioni formulate dal CoPaSiR nel Rapporto al Parlamento siano quanto mai utili, e la loro attuazione urgente. In particolare, come ben rammentava l'Ammiraglio Picchio, occorre accelerare sul percorso della operatività di nuove strutture dedicate alla prevenzione delle minacce legate al cyber-spazio, come pure ha egregiamente iniziato a fare il Dipartimento Informazioni per la Sicurezza su direttiva del suo Direttore, Pref. Gianni De Gennaro.

L’elemento di novità che va colto è anche di natura “culturale”: le evoluzioni di cui parliamo sono, a differenza di moltissimi altri temi strategici, maggiormente comprensibili e accessibili a tutti i cittadini, che ormai interagiscono e utilizzano le reti telematiche nella quotidianità.

Ci troviamo, cioè, ad affrontare problematiche che sempre più escono dalla ristretta cerchia degli addetti ai lavori e che coinvolgono i diritti e le libertà dei singoli individui. Il dr. Domenico Vulpiani da tempo affronta con efficacia il tema della prevenzione delle minacce elettroniche, con riguardo particolare alla protezione delle reti e ai crimini commessi a danno degli utenti di internet.

Quello della “rete” è un mondo complesso, che presenta almeno due facce: esso ha una straordinaria potenzialità espansiva della libertà ma presenta al contempo insidie e minacce enormi, che spetta a noi monitorare e governare.

L’Italia ha già messo in campo capacità notevoli, sia all’interno delle istituzioni che nel comparto privato e industriale – come nel caso dell’iniziativa di una Fondazione per la Cyber-Security Globale sostenuta dal Gruppo Poste Italiane. La sfida, adesso, consiste nell’inserire queste eccellenza all’interno di un disegno organico, portando ad unità il contributo pubblico e privato per una piena tutela della sicurezza nazionale anche in questa nuova dimensione, innanzitutto potenziando la cabina di regia presso la Presidenza del Consiglio.

Vi ringrazio e vi auguro buon proseguimento dei lavori.

Sen. Anna FINOCCHIARO

Mi sembra che questa sala sia la dimostrazione più evidente dell'interesse suscitato dal tema e dalle riflessione sulle quali il Senatore Ramponi, che ancora una volta ringrazio, ci ha invitato a soffermarci. Ci siamo visti l'anno scorso per un incontro di questo genere e l'esito fu una mozione condivisa da tutti i Gruppi Parlamentari: io credo che anche l'esito della giornata di oggi sia, sentito anche il Presidente Gasparri, una mozione parlamentare che incominci a fissare l'impegno del Governo rispetto a linee condivise.

Debbo ringraziare particolarmente il Senatore Ramponi per l'attenzione che ha fatto accendere su questo tema. Avevo già letto la relazione del COPASIR, che è stato l'atto introduttivo di una riflessione Parlamentare su queste questioni, ma dopo il Suo invito è scattata ulteriormente la mia curiosità ed ho continuato a studiare.

Credo che il tema sul quale ci stiamo confrontando oggi sia uno degli argomenti sui quali dovremmo appassionarci nei mesi e negli anni che verranno, perché costituisce uno squarcio sulla modernità e sul futuro. E purtroppo su questo tema noi siamo, come Italia, certamente, più indietro rispetto ad altri paesi. Gli Stati Uniti hanno già adottato, ovviamente nella loro tradizione, misure importanti, anche simbolicamente: mi riferisco, per esempio, ai primi poteri conferiti al Presidente in caso di cyber attacco delle strutture strategiche del Paese. La valigetta che ci è stata presentata in tanta letteratura è stata sostituita ora, molto probabilmente, da una chiave d'accesso ad un computer.

L'Italia si trova comunque ad un buon grado di definizione di un problema che implica un attento coinvolgimento anche di agenzie private, oltre che di agenzie pubbliche, ed io credo che sia giunto il momento di stringere ed in particolare di affrontare due questioni che sono molto importanti e delicate anche da un punto di vista legislativo ed ordinamentale.

Una è quella della ridefinizione delle strutture esistenti. L'altra è quella della rimodulazione delle attuali competenze e delle attuali responsabilità e mi riferisco in particolare a quelle che sono le competenze e le responsabilità dei nostri Servizi d'intelligence.

Penso poi alla possibilità di pensare (come diceva prima il Senatore Gasparri, come c'è scritto nella relazione del COPASIR e come ho sentito anche nel pensiero del Senatore Ramponi) ad un luogo unico, ad un ordinamento unico, che ovviamente non può che essere radicato presso la Presidenza del Consiglio, ma anche ad un coordinamento tra gli attori privati e gli attori pubblici che sia di piena ed assoluta garanzia per i soggetti interessati e soprattutto per i così detti *spy coldness* che sono da una parte le istituzione e dall'altra parte i cittadini, mantenendo sempre sullo sfondo l' interesse comune che è l'interesse nazionale che deve rimanere primario.

Si tratta di un tema che peraltro sollecita, ed è stato sostenuto anche nell'incontro di Lisbona tra i Capi di Stato e di governo della Nato, una collaborazione internazionale particolarmente significativa, una collaborazione che probabilmente avrà caratteristiche diverse da quelle che abbiamo conosciuto e registrato in passato, perche' questo tema in qualche modo 'disordina' quelle che sono state le strategie e i moduli con i quali Paesi sono entrati in relazione internazionale nel passato. Ma se e' un vento che disordina credo sia necessario trovare il punto comune e a questo fine sarebbe un bene il protagonismo dell'Italia e dell'Europa.

Questo quinto dominio ci fa apparire così piccolo il mondo, perché è tutto così piccolo e così legato e,come dicevano gli economisti di un tempo, *un battito d'ala di una farfalla in Cina può spostare capitali degli Stati Uniti d'America.* Insomma un bit o probabilmente l'intervento di un soggetto sulla rete in un luogo remotissimo, può cagionare, produrre effetti devastanti su impianti strategici per la sicurezza nazionale di tanti Paesi.

E' in qualche modo affascinante e bello (lasciatemelo dire) che il Parlamento si occupi di una tema di questo tenore e di questa novità: forse per una volta riusciremmo a sintonizzare il nostro lavoro con l'ultima frontiera sino adesso conosciuta, sapendo che tra un anno quella frontiera sarà già una retrovia. Questo ci obbligherà, però, ad una lungimiranza, ad un capacità di dibattito approfondito e soprattutto consapevole, ad uno sforzo di conoscenza di tutte le interrelazioni che

possono derivare dal regolare questa materia che può solo fare bene allo spirito ed alla vita democratica del Paese.

Vi ringrazio tutti e mi scuso ma, per impegni parlamentari, sono costretta a scappar via. Vi auguro un buon lavoro e consentitemi di ringraziare, ancora una volta, il Senatore Ramponi per l'occasione che ci ha dato.

Sen. Maurizio GASPARRI

Ringrazio il Sen. Ramponi per questa importante iniziativa, alla quale non volevo far mancare un mio personale contributo. Le riflessioni sin qui già fatte ed il dibattito che grazie al Cestudis da qualche anno sta maturando deve avere il sostegno anche del Parlamento. E come presidente del Gruppo Parlamentare del Popolo della Libertà al Senato voglio personalmente assicurare il pieno e convinto sostegno a tutte le iniziative che dovremo assumere affinché le problematiche emerse in questo convegno trovino soluzione e completa attuazione. Mi riferisco in particolare all'ipotesi di discutere, nell'Aula di Palazzo Madama, della costituzione di una struttura centrale di coordinamento e di controllo per la protezione nazionale nei confronti della minaccia cibernetica. Una esigenza, questa, sempre più avvertita.

Il sen. Ramponi ci ha giustamente richiamati ad un maggior impegno per una serie di considerazioni che non possono non essere condivise e che riguardano anche il rafforzamento delle strutture esistenti. Penso, ad esempio, come è stato già detto da altri ospiti, alla Polizia Postale e delle Telecomunicazioni, anche perché sono cresciute le esigenze di protezione delle strutture strategiche nel Paese.

La tecnologia irrompe, nel bene o nel male, sotto ogni punto di vista nel nostro quotidiano, e le vicende come quelle di Wikileaks hanno dimostrato come anche lo scambio di corrispondenza e di informazione sia altamente permeabile. Giudizi e commenti estrapolati dal contesto nel quale sono stati elaborati possono generare valutazioni del tutto fuorvianti. Quando poi queste riflessioni sono divulgate attraverso i media e magari selezionate anche in un determinato modo, quindi decontestualizzate, le problematiche che ne scaturiscono sono infinite. Anche la principale potenza internazionale ha visto i suoi più importanti rappresentanti girare il mondo per ristabilire dei rapporti e dei contatti minacciati pericolosamente dagli attacchi fatti attraverso siti web.

Ciò non vuol dire assumere un atteggiamento di condanna nei confronti della grande rete di comunicazione online. Anche oggi che la storia si è rimessa in cammino, ci sono alcuni aspetti legati alle sterminate potenzialità del web che non possono essere ignorate. Penso a quello che sta accadendo nel Nord Africa. Ebbene, le nuove generazioni hanno, anche attraverso un lungo e inesorabile 'tam tam' su internet, pianificato, organizzato e alimentato tutta la comunicazione riguardo le rivolte democratiche e civili dell'Egitto o della Tunisia. Anche lì, le nuove tecnologie hanno rappresentato uno strumento di scambio di informazioni indispensabile per raggiungere un obiettivo. Quelle barriere, fisiche oltre che ideologiche, che per secoli hanno protetto le dittature oggi sono state abbattute dalla potenza del web.

La nuova tecnologia, quindi, è uno strumento decisivo anche per gli eventi che stiamo vivendo in questi mesi. Con una differenza: le conseguenze di questa rivoluzione tecnologica non sono solo strettamente cibernetiche ma diventano, come nel caso delle rivolte del Nord Africa, anche fisiche con le trasmigrazioni dei popoli.

C'è una connessione di aspetti quindi e credo che chi ha una responsabilità in Parlamento debba assicurare, per offrire un contributo concreto, che le iniziative assunte in ambito di Presidenza del Consiglio dei Ministri, di coordinamento, abbiano il pieno sostegno parlamentare, evitando tuttavia la moltiplicazione inutile di strutture.

Ho più volte avuto modo di confrontarmi anche con il sen. Ramponi a proposito della necessità di dare sostegno alle strutture preesistenti, rafforzarle piuttosto che crearne delle altre. E so di non essere il solo ad auspicare strutture più solide nell'ambito dei Servizi, in ambito del Coordinamento dei Servizi, in ambito militare, delle Forze dell'Ordine, costituite da uffici che abbiano sviluppato una altissima professionalità. Prevedendo che tra queste strutture ci sia però una struttura di coordinamento, un Ente, che debba fare da riferimento per meglio valorizzare competenze e qualità.

Non v'è dubbio che l'Italia debba rafforzare la protezione di alcune strutture strategiche.

Siamo altrettanto certi che vi siano problemi nuovi che insorgono giorno dopo giorno, e quindi spetta a noi dare nuove risposte. Le riflessioni che tutti voi esperti di settore avete sin qui

fatto possono e devono essere tradotte in concrete proposte di lavoro ed in rispettive iniziative parlamentari e provvedimenti di attuazione del governo. L'impegno è quello di portare alla attenzione di tutti le problematiche sin qui affrontate e sulle quali mi auguro ci sia una franca discussione e una condivisione di opinioni dei vari gruppi parlamentari, considerando che stiamo parlando di questioni che non hanno una "bandiera", un'appartenenza, e visto che si tratta di esigenze primarie per la sicurezza del Paese, soprattutto in momenti così intensi.

La storia si è rimessa in cammino, nel bene e nel male. Nel bene, perché ci auguriamo che si possa aprire una stagione di libertà e di democrazia dei popoli che hanno visto sin qui umiliate queste possibilità. Mentre, d'altro canto, bisognerà vigilare, seguire, perché in altri momenti, in altri Paesi, non si ripeta quello che accadde in Iran alla fine degli anni '70: quella che sembrava una rivoluzione di libertà ha poi portato l'Iran al regime più oscurantista che si sia costituito in quell'area e che addirittura oggi minaccia attacchi non cibernetici ma nucleari. La storia si rimette in cammino: speriamo che vada nella direzione giusta!

Noi, intanto, pensiamo alla nostra storia, alla nostra sicurezza e quindi saremo pronti a sostenere le proposte operative che, anche da questa importante occasione, stanno emergendo. Grazie per la vostra attenzione.

Sen. Sandro MAZZATORTA

Buongiorno a voi. Innanzitutto vi porto i saluti del Presidente Bricolo che, per sopravvenuti impegni istituzionali, non ha potuto essere qui presente con Voi questa mattina: mi ha, pertanto, incaricato di ringraziare il Sen. Ramponi per aver promosso questa giornata di riflessione che si sta svolgendo in un momento particolare.

La data di questo seminario non avrebbe potuto esser scelta meglio perché ciò che sta accadendo in Tunisia ed in Libia sta facendo emergere una realtà importante e, secondo noi, decisiva e ci pone degli interrogativi, anche ai fini di questo Seminario.

Il tema che ci è stato proposto – inerente alle minacce per la sicurezza nazionale derivante dall'uso improprio dello spazio cibernetico – ha almeno due declinazioni.

Da un lato c'è l'aspetto tecnico, su quale si è parlato diffusamente in precedenza: la protezione delle infrastrutture strategiche rispetto al rischio di attacchi condotti in via informatica. I sistemi informatici portano indubbiamente sviluppo ma creano anche una maggior vulnerabilità delle infrastrutture critiche che mettono a rischio soprattutto la riservatezza e quindi la libertà dei nostri cittadini. Su questo aspetto non mi dilungo perché già la relazione del COPASIR e gli altri interventi di questa mattina hanno già ben definito il tema.

A me interessa l'altro lato, il secondo aspetto dell'approfondimento, che ha a che fare con la capacità di un sistema politico di proteggersi rispetto ai rischi della *eterodirezione* cioè, come si diceva una volta, *dall'intossicazione informativa.* Questa può essere, secondo me, una minaccia seria perché quando si subisce la disinformazione si perde sovranità e si è costretti a decidere sulla base di emozioni e di informazioni generati ad arte.

Esaminiamo il caso libico che è sotto i nostri occhi. All'indomani della così detta Giornata della collera, il 17 feb. u.s., siamo stati sottoposti ad uno straordinario bombardamento di immagini e di messaggi on line che hanno determinato, in modo decisivo, la nostra percezione degli eventi, generando emozioni ma precludendo la possibilità di assumere decisioni seguendo il concetto dell'interesse.

Questa, però, non è la prima volta che accade, perché vi sono stati altri precedenti casi: è successo in precedenza in Somalia, nei Balcani, prima in Bosnia e poi nel Kosovo. Le opinioni pubbliche internazionali sono state bersaglio di azioni informative e disinformative che hanno reso l'intervento militare della Nato inevitabile. In quel contesto informativo non si poteva ragionare: da una parte c'era il nero, dall'altra il bianco.

Questa è una esemplificazione pericolosa che impedisce qualsiasi ragionamento, spostando il dibattito dalla logica del conveniente a quella, evidentemente, morale dei giudizi di valore.

Negli anni '90 imperversava l'abitudine ed il metodo di spararla grossa a sufficienza perché i media catturassero gli eventi e li proponessero nel modo più opportuno al grande pubblico.

È arrivata, successivamente, la rete, è arrivato internet, che ha prodotto quelle rivoluzioni colorate ed in parte significative dell'ex Unione Sovietica e per ultimo abbiamo il web 2.0., cioè l'integrazione di internet e della video telefonia cellulare.

Il risultato è stato notevolissimo, perché Facebook, Youtube, i social network , hanno contribuito decisivamente a travolgere il regime di Ben Alì in Tunisia e quello di Mubarak in Egitto, senza peraltro creare delle alternative credibili.

Il tam-tam della rivolta è dilagato sul web ed i dittatori sono stati sconfitti: questa rivoluzione, guidata anche da una attività politica on line, non ha ancora prodotto una alternativa credibile. La protesta informatica, sui blog, sui forum, sulle chat, sui social network, può distruggere ma difficilmente crea un progetto politico: un serio progetto politico on line è una realtà ancora sconosciuta.

In Tunisia, così, i *"Gelsomini"* hanno vinto, ma coloro che sono insorti ora vengono da noi in massa a Lampedusa, e tra quelli che sono rimasti c'è chi ancora si da fuoco, mentre in Egitto si sono enormemente rafforzati i *"Fratelli Musulmani"*.

In Libia il web 2.0 è stato ugualmente enorme, perché non solo ha veicolato la percezione, tra l'altro veritiera, di un regime eccezionalmente brutale, ma soprattutto perché ha diffuso l'illusione che la vittoria fosse a portata di mano, che il destino di Gheddafi fosse ormai irreversibilmente segnato.

Questa deformazione, in prospettiva, ha fortemente condizionato il nostro processo politico permettendogli, solo con molto ritardo, di reagire in modo corretto agli eventi. Altri, occorre ammetterlo, sono stati più lucidi di noi, rapidi nell'adeguarsi al mutamento dello scenario per coglierne meglio le implicazioni.

Cosa fare, sotto questo punto di vista, per fronteggiare questo nuovo tipo di pericolo, che dilata sul web e sull'universo parallelo, creato ed alimentato dalle reti globali di comunicazioni di computer?

È difficile dirlo anche perché la preservazione della libertà della rete è certamente un principio non negoziabile.

È certo che dobbiamo pensare ad un nuovo modo di proteggerci dai condizionamenti esterni: dalle minacce della rete e dalla disinformazione perché è logico che in questa dimensione stia diventando sempre più importante.

Ogni società ha il suo tipo di lotta. Siamo nella società dell'informazione, la guerra non può non avere una prepotente dimensione virtuale e la politica ne sta prendendo atto. Ai tecnici compete suggerire le soluzioni, le opzioni efficaci, per fronteggiare la nuova minaccia proveniente dal mondo cyber space: ogni computer, ogni PC, ogni IPAD, è una finestra sul cyber space.

Questa realtà artificiale, virtuale, multidimensionale, è costituita da un mare di dati, d'informazioni e nuove fluide associazioni di persone, con nuovi modi e modelli di comunicazione interpersonale.

Cyber space, secondo noi, ha e deve avere una geografia, una natura e delle leggi date dall'uomo: dobbiamo riuscire in questo obiettivo se vogliamo mantenere la nostra sovranità, nel mondo complesso di questo ventunesimo secolo e se vogliamo veramente vincere questa sfida per l'umanità.

Crediamo che spetti al Senato ed alla Camera, nella pienezza e nella sovranità del Parlamento, valutare quali azioni, in termini di prevenzione della minaccia alla sicurezza e alla nostra sovranità, assumere anche alla luce delle considerazioni espresse dalla relazione approvata dal COPASIR e di quelle svolte in questo seminario dagli autorevoli relatori. Vi ringrazio per l'attenzione.

Dott. Gianni LETTA
Sottosegretario alla Presidenza
*del Consiglio dei Ministri**

CONCLUSIONI

Il ringraziamento che rivolgo al Sen. Ramponi non è formale e non si limita certamente al pur cortese invito, che ben volentieri ho accettato. È infatti un "grazie" che va dritto alla sostanza di questo convegno, dichiaratamente e – mi permetto di aggiungere - meritoriamente teso alla individuazione di una proposta condivisa, per garantire un'azione unitari di indirizzo e coordinamento delle iniziative di contrasto alla minaccia cibernetica.

Condivisione e coordinamento sono infatti due parole-chiave in una materia che rappresenta già oggi – ma lo farà sempre più in futuro – il punto nodale dei problemi legati alla difesa degli interessi nazionali, alla sicurezza nazionale e quindi alle attività dei nostri Servizi d'Informazione.

La condivisione è infatti fondamentale quando si tratta di decisioni politiche e legislative riguardanti gli assetti fondamentali del sistema-Paese, e non è certo a questa platea che debbo ricordare l'assoluto rilievo strategico delle infrastrutture critiche o la delicatezza costituzionale della disciplina delle attività di intelligence.

Il coordinamento è un dei problemi di fondo dell'azione amministrativa nelle società complesse e ciò risulta particolarmente evidente nel campo della sicurezza cibernetica nel quale – cito qui alcuni passi della relazione approvata dal COPASIR il 7 lug. dello scorso anno – " i soggetti, che a vario titolo e con diverse competenze sono coinvolti nel processo di contrasto alle minacce, sono numerosi" e pur trattandosi di organizzazioni "importanti per la qualità delle operazioni che spesso riescono a garantire" nel complesso costituiscono una realtà che può "rappresentare, laddove non adeguatamente coordinata e sollecitata al costante aggiornamento operativo, un limite per la sicurezza della Nazione".

Ma – dobbiamo dirlo con chiarezza – di fronte alla qualità e ai possibili sviluppi della minaccia cibernetica "coordinare", per quanto necessario, non è sufficiente. Per verificarlo bastano alcune essenziali riflessioni.

Nella relazione al Parlamento sulla politica dell'informazione e della sicurezza nell'anno 2010, presentata dal Governo il mese scorso, la *cyber threat* è indicata tra le "sfide crescenti", cioè tra le minacce che nell'anno passato hanno richiesto un aumento di impegno da parte dei nostri Servizi di informazione.

Nel documento si sottolinea, in particolare, "la potenziale gravità del pericolo al quale risulterebbe inevitabilmente esposta, nell'eventualità di un attacco informatico, la struttura economico produttiva" di un Paese tecnologicamente avanzato quale è l'Italia.

Alla luce di questa considerazione appaiono evidenti le ragioni che rendono oggi preminente la minaccia cibernetica, soprattutto nelle sue configurazioni direttamente riconducibili a finalità *latu sensu* politiche (ciberterrorismo o vera e propria guerra cibernetica): in questi casi, infatti, l'attacco mira dritto al cuore del sistema-Paese, cioè agli interessi vitali della collettività nazionale, siano essi economici, scientifici o industriali.

È assai significativa, a questo proposito, l'indicazione che viene da studi recenti circa lo strettissimo intreccio esistente tra le attività della cosiddetta intelligence economica e quelle di *cyber espionage o cyber warfare.* La competizione economica, anche tra alleati, è destinata ad accrescersi e con essa il ricorso allo spionaggi tecnologico ed industriale, che un Paese come l'Italia è fonte è fonte di rischi gravissimi.

In una società che affida in maniera vertiginosamente crescente all'informatica le proprie capacità di trasmettere le informazioni, di conservarle e di utilizzarle a fini di analisi e di programmazione, il numero e la qualità delle notizie che saranno acquisite, mediante la penetrazione nelle reti di trasmissioni e nelle banche, dati è destinata ad aumentare ulteriormente.

La protezione delle notizie riservate è comunque una priorità anche per gli operatori economici ed industriali.

Il carattere sistemico della minaccia cibernetica ha due implicazioni principali: richiede la più ampia cooperazione internazionale e impone un'effettiva e concreta integrazione pubblico-privato.

In questo senso, del resto, è esplicitamente orientato il nuovo concetto strategico della Nato, adottato a Lisbona nel novembre dello scorso anno. Il documento, come vi è ben noto, impegna i Paesi membri dell'Alleanza a potenziare le proprie capacità di prevenire, individuare e difendersi dagli attacchi informatici potenzialmente pericolosi per la sicurezza nazionale e quella euro-atlantica.

A questo proposito, e sempre con riferimento ai Paesi dell'ambito NATO, particolari capacità operative appaiono contraddistinguere l'iniziativa recente assunta dagli Stati Uniti con la costituzione di un *Cyber Command,* posto al centro di un sistema che coinvolge tutte le forze armate del Paese e non esclude la possibilità di "attacchi preventivi".

Ed ecco la terza, decisiva parola-chiave in questa complessa materia:"sistema".

Per fronteggiare efficacemente una minaccia che appare in grado, ogni giorno di più, di aggredire le strutture vitali di uno Stato e di una collettività nazionali, cioè il sistema-Paese nella sua globalità, la risposta non può che essere una risposta di "sistema o, se volete, "del" sistema.

La ricetta vincente non può che essere la messa a fattor comune delle non indifferenti capacità operative – lo sottolineo qui, ma lo sapete bene quanto me – di cui l'Italia già dispone, organizzando queste preziose tessere pubbliche e private, in un mosaico unitario.

Fuori metafora, occorre individuare una sede autorevole, dotata di poteri e responsabilità, alla quale affidare l'attuazione di una pianificazione operativa delle capacità di difesa dei soggetti esistenti.

Questa pianificazione unitaria è la condizione indispensabile per dotare il nostro Paese di una forte e tempestiva capacità di reazione nei confronti degli attacchi su larga scala, quelli che, come dicevo prima, mirano a paralizzare il sistema-Paese nei suoi gangli vitali. Solo operando secondo queste direttrici si potrà arrivare, infine, a pianificare una difesa preventiva, che non può essere certamente realizzata con il solo coordinamento e, men che meno, facendo leva sulla pur fondamentale buona volontà dei soggetti interessati.

È il classico salto di qualità, al quale siamo chiamati con assoluta urgenza dall'evolversi della situazione internazionale, scandita dall'intensificarsi degli attacchi informatici e dall'arricchirsi della loro casistica.

Il Governo dedica a questa materia una particolare attenzione, non limitata alle direttive impartite ai Servizi d'informazione e sicurezza. È, infatti, all'opera un apposito gruppo di lavoro interministeriale, che sta approfondendo lo studio della minaccia, in tutti i suoi aspetti, per definire conseguentemente le metodologie operative più adeguate, la riorganizzazione delle competenze esistenti e la riallocazione delle responsabilità decisionali.

Sono certo che questo lavoro risulteranno molto utili le risultanze della discussione di questa mattina. È per questo che rinnovo i miei ringraziamenti agli organizzatori e a tutti gli oratori intervenuti.

NOTA (*): non ha potuto presenziare per un imprevisto ed improrogabile impegno istituzionale e, pertanto la relazione è stata presentata dal Senatore Ramponi.

Legislatura 16 Atto di Sindacato Ispettivo n° 1-00405

Atto n. 1-00405

Pubblicato il 7 aprile 2011
Seduta n. 537

RAMPONI , GASPARRI , FINOCCHIARO , BRICOLO , RUTELLI , PISTORIO , D'ALIA , VIESPOLI

Il Senato,
considerato che:

- le tecnologie dell'informazione e della telecomunicazione costituiscono sempre di più una parte fondamentale per la vita della società;
- a struttura aperta del sistema *Internet* è vulnerabile ad attacchi che possono avere origine criminale (*cyber crime*), terroristica (*cyber terrorism*), per attività di spionaggio (*cyber espionage*) o, addirittura, dar vita ad una *cyber war*, cioè un vero e proprio conflitto tra nazioni combattuto attraverso la paralisi di tutti i gangli vitali per la vita delle società dei reciproci contendenti;
- il decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155, all'art. 7-*bis* rubricato "Sicurezza Telematica", dispone che "Ferme restando le competenze dei Servizi informativi e di sicurezza […] l'organo del Ministero dell'interno per la sicurezza e per la regolarità dei servizi di telecomunicazione (Servizio Polizia Postale e delle Comunicazioni) assicura i servizi di protezione informatica delle infrastrutture critiche informatizzate di interesse nazionale individuate con decreto del Ministro dell'interno [...]";
- con decreto del Ministro dell'interno 9 gennaio 2008 sono state individuate le infrastrutture critiche informatizzate di interesse nazionale;
- in ossequio allo stesso decreto, è stato istituito con decreto del Capo della Polizia, direttore generale della pubblica sicurezza, il Centro nazionale anticrimine informatico per la protezione delle infrastrutture critiche (CNAIPIC);
- il nuovo concetto strategico della NATO e la dichiarazione finale del vertice di Lisbona hanno individuato come nuovo obiettivo la tutela della sicurezza del *cyber space*;
- i principali Governi europei, e in particolare, in ordine di tempo, il Regno Unito, la Francia, la Germania e l'Olanda, si sono dotati di una dottrina *cyber* sicurezza nazionale, grazie alla quale si individuano le priorità di intervento e si attribuiscono ruoli e responsabilità con l'obiettivo di ridurre la frammentazione di competenze e di stimolare una più profonda collaborazione sul piano multilaterale;
- nel convincimento che i *cyber attack*, oltre ad essere cresciuti in frequenza, siano divenuti oltremodo pericolosi per il mantenimento della prosperità dei singoli Paesi, l'Alleanza Atlantica ha avvertito la necessità di introdurre la dimensione informatica dei moderni conflitti nella propria dottrina strategica, nonché l'urgenza di potenziare la propria capacità nella prevenzione da un attacco, reagire ad esso, migliorando la resilienza e limitando i danni;
- il decreto del Presidente del Consiglio dei ministri del 5 maggio 2010 ha dato vita al Nucleo Interministeriale Situazione Pianificazione (NISP) quale organo di studio e supporto alle attività del Comitato politico strategico (COPS) in materia di organizzazione nazionale per la gestione della crisi;
- le istituzioni nazionali hanno preso atto dei vari tipi di minaccia cibernetica e hanno avviato iniziative di contrasto;
- il quadro di difesa contro tali attacchi presenta in Italia una situazione diffusa di sistemi di protezione in via avanzata di completamento, nell'ambito dei diversi assetti pubblici e privati;

nelle conclusioni e raccomandazioni della relazione del COPASIR sulle possibili implicazioni e minacce per la sicurezza nazionale, derivanti dallo spazio cibernetico, si auspica un adeguato coordinamento di tutti i soggetti interessati alla messa a punto di un sistema di protezione di tutti gli assetti sensibili, riguardanti la vita economica, sociale e politica dello Stato,

impegna il Governo:

- a costituire, nell'ambito della Presidenza del Consiglio dei ministri, una struttura centrale di coordinamento e controllo dell'organizzazione di protezione nazionale nei confronti della minaccia cibernetica: all'ente, una volta costituito, sulla base delle determinazioni relative alla minaccia, individuate dal Dipartimento delle informazioni per la sicurezza (DIS), spetta il compito di predisporre una pianificazione concettuale ed organizzativa unitaria, con la conseguente adozione di misure nonché l'emanazione di apposite disposizioni coordinate ed integrate. A tale organismo compete altresì l'effettuazione dei controlli necessari ad assicurare la concreta attuazione, da parte di tutti gli organismi pubblici e privati interessati, delle misure e delle disposizioni in materia di protezione nazionale nei confronti della minaccia cibernetica;
- a definire, mediante l'adozione di un apposito provvedimento, la struttura, la composizione e le procedure operative del costituendo ente, la cui direzione deve essere affidata ad un dirigente di prima fascia o equiparato dell'Amministrazione dello Stato;
- ad affidare al Ministero della difesa la protezione delle strutture e della reti di comunicazione militare, riconoscendogli, oltre ai compiti istituzionali, la capacità di prevenire, monitorare, individuare, contrastare e gestire le aggressioni cibernetiche, sviluppate nei riguardi delle sue strutture informatizzate, nonché la messa a punto di appositi sistemi offensivi di difesa preventiva dalla minaccia, con strumenti, procedure e prescrizioni propri e/o multinazionali (NATO e UE) mantenendo contatti diretti con i collaterali organismi.

INDICE

La vita pubblica e privata del Paese è *governata*
con ***Infrastrutture strategiche digitali.***
Il caso ***Wikileaks*** *ed i* ***cyber attack*** *subiti da organismi pubblici e*
privati di USA, Giappone, Germania e di altri Paesi,
danno la ***percezione*** *del* ***pericolo della minaccia cibernetica****.*

Il Cestudis*, anche alla luce della* ***relazione del COPASIR,***
ha organizzato questo convegno ***allo scopo di richiamare***
l'attenzione e sensibilizzare, Governo ed opinione pubblica,
sul ***cyber space*** *e le sue vulnerabilità ed, allo stesso tempo,*
individuare soluzioni politiche condivise per una mozione*.*

I relatori *della 1^ e 2^ sessione,* ***responsabili ed esperti di alto livello****, partendo*
da quadri di situazioni di livello nazionale ed internazionale,
hanno prospettato che*:*
- il Sistema Paese è vulnerabile ad attacchi cybernetici*,*
i quali sono ***sempre più numerosi*** *e provenienti da*
una ***minaccia globale,*** *sempre più* ***variegata****;*
- gli ***attacchi si avvalgono di tecnologie*** *costantemente* ***evolute*** *ed*
impongono *un attento e continuo* ***adeguamento delle contromisure****;*
- l'industria italiana ha le potenzialità *per controbattere e contrastare,*
*l'****evoluzione tecnologica*** *dei cyber attack;*
- è necessario *avere un* ***organismo centrale direttivo*** *per un unitario*
coordinamento delle attività di ***cyber war.***

I politici*, partecipanti al dibattito della 3^ sessione, hanno:*
- ***preso atto della situazione internazionale e delle problematiche nazionali,***
così come denunciato dai relatori della 1^ e 2^ sessione;
- recepito l'incombente pericolo della minaccia cibernetica*;*
- condiviso la necessità*, per un migliore contrasto alla cyber war,*
di creare un ***organismo centrale*** *per un unitario indirizzo*
a livello nazionale e per un proficuo coordinamento
sia in ambito Nato, sia in campo internazionale;
- sottoscritto una mozione che impegna il Governo ad assumere
un ruolo fondamentale nel contrasto alla minaccia cibernetica*.*

Il dott. Letta*, la cui relazione ha* ***concluso i lavori,*** *ha ringraziato il Sen. Ramponi*
per aver promosso questo simposio che ha portato a ***soluzioni politiche condivise,***
importante viatico per l'attuazione di efficaci predisposizioni ***a tutela del cyber space****.*
Ha fatto presente che il ***Governo sta dedicando particolare attenzione alla cibernetica***
ben consci che, per vincere la sfida nello cyber space, occorre:
- *un* ***Coordinamento Centralizzato,*** *che però da solo* ***non è sufficiente;***
- ***far sistema tra le istituzioni pubbliche ed il privato;***
- ***fare un salto di qualità*** *per contrastare la minaccia cyber.*

I testi degli interventi dei conferenzieri e dei politici
sono integralmente riportati nel volume.