COMMISSIONE IV
DIFESA

RESOCONTO STENOGRAFICO

INDAGINE CONOSCITIVA

9.

SEDUTA DI MERCOLEDÌ 25 GENNAIO 2017

PRESIDENZA DEL PRESIDENTE **FRANCESCO SAVERIO GAROFANI**

INDICE

N. B. Sigle dei gruppi parlamentari: Partito Democratico: PD; MoVimento 5 Stelle: M5S; Forza Italia - Il Popolo della Libertà - Berlusconi Presidente: (FI-PdL); Area Popolare-NCD-Centristi per l'Italia: AP-NCD-CpI; Sinistra Italiana-Sinistra Ecologia Libertà: SI-SEL; Lega Nord e Autonomie - Lega dei Popoli - Noi con Salvini: (LNA); Scelta civica-ALA per la costituente libera e popolare-MAIE: SC-ALA CLP-MAIE; Civici e Innovatori: (CI); Democrazia Solidale-Centro Democratico: (DeS-CD); Fratelli d'Italia-Alleanza Nazionale: (FdI-AN); Misto: Misto; Misto-Minoranze Linguistiche: Misto-Min.Ling.; Misto-Partito Socialista Italiano (PSI) - Liberali per l'Italia (PLI): Misto-PSI-PLI; Misto-Alternativa Libera-Possibile: Misto-AL-P; Misto-Conservatori e Riformisti: Misto-CR; Misto-USEI-IDEA (Unione Sudamericana Emigrati Italiani): Misto-USEI-IDEA; Misto-FARE ! - Pri: Misto-FARE ! - Pri; Misto-UDC: Misto-UDC.

PAGINA BIANCA

PRESIDENZA DEL PRESIDENTE FRANCESCO SAVERIO GAROFANI

La seduta comincia alle 14.30.

Sulla pubblicità dei lavori.

PRESIDENTE. Avverto che la pubblicità dei lavori della seduta odierna sarà assicurata anche attraverso la trasmissione televisiva sul canale satellitare della Camera dei deputati e la trasmissione diretta sulla *web-tv* della Camera dei deputati.

Audizione del Capo di Stato Maggiore della Difesa, Generale Claudio Graziano.

PRESIDENTE. L'ordine del giorno reca, nell'ambito dell'indagine conoscitiva sulla sicurezza e la difesa nello spazio cibernetico, l'audizione del Capo di Stato Maggiore della Difesa, Generale Claudio Graziano. Saluto il generale - cui faccio gli auguri di buon lavoro, vista la recente proroga del suo incarico - e i suoi collaboratori che lo accompagnano.

Ricordo che dopo l'intervento del generale darò la parola ai colleghi che intendono porre domande e svolgere osservazioni; successivamente il generale potrà rispondere a tali domande.

Do la parola al generale Graziano.

CLAUDIO GRAZIANO, *Capo di Stato Maggiore della Difesa*. Grazie presidente e grazie agli onorevoli membri della Commissione difesa per essere qui oggi. Vi ringrazio dell'opportunità offerta per illustrare l'evoluzione della capacità *cyber* della Difesa. Mi avvarrò di alcune lastrine che poi naturalmente saranno lasciate a disposizione.

Lo scopo della presentazione è quello di illustrare le attuali capacità delle Forze armate nel settore della *cyber defence* e la relativa organizzazione, nonché le future evoluzioni organizzative tese al raggiungimento di una piena capacità, anche nel settore militare di mia competenza, nelle *cyber operations*, attraverso la costituzione del Comando interforze per le operazioni cibernetiche e le connesse attività.

L'intervento sarà articolato nel seguente modo: svolgerò dapprima una presentazione generale sull'analisi della minaccia cibernetica; poi una breve introduzione sul quadro normativo vigente; passerò, quindi, a trattare dei risultati conseguiti nel settore della *cyber defence* nell'ambito della Difesa e dell'organizzazione preposta all'assolvimento dei compiti discendenti; delle evoluzioni degli aspetti che hanno portato il comparto Difesa verso un'evoluzione organizzativa ed operativa che in futuro sarà in grado di condurre operazioni cibernetiche, e non più soltanto la difesa delle reti, costituendo un elemento attivo, che abbiamo citato - ossia il Comando per le operazioni cibernetiche - sicuramente utile e io credo indispensabile per accrescere in generale la sicurezza del Paese nello specifico settore; infine, concluderò con alcune considerazioni finali.

Passiamo alla minaccia. Questa è ben nota in senso generale, per alcuni anche per l'interesse specifico nella materia. L'evoluzione di questa minaccia richiede all'Italia, alla stregua di tutti i membri di organizzazioni internazionali, di realizzare rapidamente un'efficace capacità di difesa cibernetica. La minaccia sta assumendo un crescente rilievo, che è direttamente proporzionale alla dipendenza informatica da parte dei Paesi tecnologicamente più avanzati, e costituisce uno dei più efficaci me-

todi di lotta asimmetrica (quando parliamo di lotta asimmetrica ci riferiamo al confronto tra due o più soggetti le cui rispettive forze, nello specifico militari, differiscono in modo significativo). Questo vuol dire che anche un singolo individuo può costituire una minaccia per lo Stato. Spesso la chiamiamo anche « minaccia ibrida », che in questo caso è una componente di una minaccia complessa, quando è anche accompagnata da altri tipi di attacchi o di minacce.

Gli attacchi *cyber*, come abbiamo imparato anche dai recenti fenomeni terroristici di Isis, possono essere condotti da una molteplicità di attori statuali e non, anche privi di identità, che sono in grado di agire con modalità diverse per conseguire obiettivi nei settori più importanti delle istituzioni di un Paese, da quello politico a quello economico, a quello sociale, a quello più specificatamente militare, per turbare le operazioni o per dirigerle in altri settori, o semplicemente per acquisire informazioni.

Gli attacchi *cyber* hanno una diretta incidenza anche nei confronti di tutti gli aspetti di interesse della Difesa, come l'organizzazione della sicurezza, la gestione dei sistemi d'arma, che come vedremo hanno sempre più una dipendenza dall'ambito informatico e cibernetico e, soprattutto, la condotta di operazioni militari. Riferendomi proprio alla condotta delle operazioni militari, è sempre più evidente come la disponibilità dei sistemi di comando e controllo tecnologicamente avanzati costituisca certamente un fattore abilitante al fine del conseguimento degli obiettivi.

In alcuni casi, però, il livello tecnologico si riduce addirittura a un limitato intervento dell'uomo (pensiamo, ad esempio, ai veicoli senza pilota, che seguono rotte preprogrammate). Tale progresso, che sicuramente è un punto di vista irrinunciabile, dall'altro rappresenta un'enorme vulnerabilità di fronte alla potenzialità di una minaccia cibernetica. Un'intrusione nei sistemi di comando e controllo finalizzata non solo allo spionaggio, ma anche al sabotaggio e al malfunzionamento, potrebbe compromettere l'esito di una campagna, di un'operazione, e sicuramente mettere in pericolo il nostro personale, generando effetti che si riverbererebbero sulla credibilità dell'operazione e sulla protezione delle forze.

Proprio queste considerazioni hanno stimolato lo sviluppo della strategia difensiva cibernetica della NATO, introdotta nel vertice del Galles e confermata con la determinazione del *summit* di Varsavia nel luglio 2016. La consapevolezza della NATO poggia anche sui dati concreti richiamati dal Segretario generale dell'Alleanza Stoltenberg, che ha evidenziato un incremento del 60 per cento degli attacchi *cyber* alle strutture NATO nel 2016, con una frequenza media di circa 500 attacchi al mese. La maggior parte degli attacchi non proverrebbe da privati, ma da istituzioni statali e statuali di altri Paesi, anche se poi la dimostrazione di questi dati analiticamente è sempre difficile, ed è più spesso deduttiva.

Alla luce di questa preoccupante evoluzione e per affrontare la minaccia *cyber* la NATO continua a promuovere un approccio sinergico tra gli alleati e anche tra gli altri *partner*, puntando sul miglioramento delle capacità nazionali di difesa cibernetica, per contribuire al rafforzamento della difesa collettiva e alla sicurezza dello spazio euroatlantico. Non dimentichiamo, infatti, che le nostre strutture di comando e controllo delle operazioni si vanno poi a inserire in altre strutture con cui devono operare. Quindi, i nostri comandi in Afghanistan si devono inserire nella rete della NATO, in altre operazioni nelle reti della coalizione.

La lastrina « Analisi della minaccia 2/2 », che sembra complessa ma che per noi è molto importante, rappresenta l'ambiente cibernetico e di riferimento per ogni operazione, dalla più complessa alla più semplice, compreso – ad esempio – il dispiegamento di un ospedale a Misurata. La minaccia cibernetica evidentemente è potenzialmente fattore inabilitante della capacità di comando e controllo della forza. Si consideri il caso di un comando impegnato in una possibile operazione multidimensionale e la minaccia cibernetica po-

trebbe manifestarsi in una moltitudine di aspetti, che potrebbero comportare ad esempio un'errata percezione, da parte dei comandanti a tutti i livelli, della situazione operativa reale, tale da generare rilevanti criticità anche nell'ambito della *force protection*, qualora dovessero incidere per esempio sugli schermi di controllo della situazione di comando e controllo. Quindi, potrebbero portare a una perdita di controllo dei propri assetti, a un decadimento delle reti di comunicazione, a un'errata geolocalizzazione delle forze in campo, fino ad arrivare alla paralisi dei sistemi di comando e controllo.

Delineata in larghe misure la minaccia nei termini più complessi, che probabilmente, entro certi limiti, non ha neanche ancora raggiunto i sistemi, perché attualmente i sistemi, specialmente quelli classificati, hanno una sufficiente protezione, l'attuale capacità di sicurezza raggiunta dalla Difesa discende dall'attuale quadro di riferimento normativo del Decreto del Presidente del Consiglio dei ministri del 2013, nel quale vengono forniti gli indirizzi dell'organizzazione e della sicurezza informatica nazionale, con particolare riferimento al settore della protezione, comunemente chiamata *cyber defence*. Quindi non sono ancora operazioni cibernetiche ma è la protezione.

Il decreto definisce l'architettura istituzionale deputata alla tutela della sicurezza nazionale relativamente alle infrastrutture critiche materiali e immateriali, con particolare riguardo alla protezione cibernetica e alla sicurezza informatica.

Come è stato già riportato anche dal Consigliere militare della Presidenza del Consiglio, tale organizzazione prevede un livello di indirizzo politico e coordinamento strategico, il Comitato interministeriale per la sicurezza della Repubblica, che risponde alla Presidenza del Consiglio, con il compito di individuare, attraverso l'elaborazione di un Piano nazionale per la sicurezza, gli obiettivi funzionali necessari a garantire la protezione cibernetica e la sicurezza informatica nazionale. Poi ci sono altri due livelli, uno di coordinamento e supporto operativo, ovvero il Nucleo di sicurezza cibernetica, e uno di gestione delle crisi, attraverso l'attivazione di un tavolo interministeriale di crisi cibernetica.

Al riguardo, il Nucleo di sicurezza cibernetica si avvale di un'unità per l'allertamento e la risposta a situazioni di crisi cibernetiche che è collocata presso il CERT (*Computer Emergency Response Team*) del comando C4 della Difesa (Comando, Controllo, Comunicazioni e Computer) ed opera alla luce di un definito quadro procedurale.

Il Nucleo di sicurezza cibernetica, in caso di crisi, ha il compito di verificare che le azioni di reazione e stabilizzazione siano svolte in maniera coordinata da parte dei ministeri e le agenzie coinvolte che abbiano disponibili le capacità per reagire. Oggi il rappresentante del comparto Difesa in tale consesso si identifica quindi nel personale di questo CERT.

Il Decreto del Presidente del Consiglio dei ministri del 27 gennaio 2014 introduce il Quadro strategico nazionale per la sicurezza dello spazio cibernetico e da esso deriva il Piano nazionale per la protezione cibernetica e la sicurezza informatica. Il primo, il Quadro strategico nazionale per la sicurezza dello spazio cibernetico, identifica gli indirizzi strategici, i ruoli e i compiti assegnati ai vari dicasteri, tra cui la Difesa. In particolare, al Ministero della difesa è riconosciuta la necessità di dotarsi della capacità di pianificare, condurre e sostenere operazioni nello spazio cibernetico atte a prevenire, localizzare difendere, contrastare e neutralizzare ogni possibile minaccia e azione avversaria cibernetica portata alle reti, ai sistemi e ai servizi della Difesa sul territorio nazionale e nei teatri operativi fuori dai confini nazionali, nel quadro delle proprie missioni istituzionali.

Il secondo, il Piano nazionale per la protezione cibernetica, definisce gli indirizzi operativi nel settore *cyber*, tra i quali evidenzio, per la Difesa, la realizzazione del Comando interforze per le operazioni cibernetiche, che poi è stato richiamato e dettagliato nel Libro Bianco per la sicurezza internazionale e la difesa, in via di implementazione, e che rappresenta uno dei nostri obiettivi prioritari. Tra l'altro,

esso viene a colmare una lacuna, perché in altri Paesi già esiste un organismo similare e in altri ancora è in corso di realizzazione il Comando *cyber*. È un concetto interforze sicuramente principale ed evidente, perché la minaccia *cyber* non ha limiti spaziali.

Passando all'attuale organizzazione, in attesa di definizione del Comando interforze, il CERT Difesa, che abbiamo prima citato, è integrato nell'organizzazione *cyber* del Dicastero per garantire la protezione delle reti e la gestione degli eventuali incidenti informatici. Il CERT Difesa si articola in due strutture organicamente distinte, poste alle dipendenze, in questo momento, di due reparti diversi dello Stato Maggiore della Difesa. La prima, il *Coordination Center*, dipende dal Reparto Informazioni e Sicurezza, ed è deputata ad assicurare il coordinamento, al fine dello scambio informativo, con le analoghe strutture di settore, interministeriale, internazionale, accademico e con le organizzazioni di sicurezza.

La seconda, il *Technical Center*, dipende dal VI Reparto, Comando, Controllo, Comunicazioni, Computer e sistemi informativi, che è alle dipendenze del qui presente generale Palmieri; quest'ultima struttura possiede le capacità tecniche per sviluppare le attività *cyber* e presiede alla realizzazione concreta e allo sviluppo dei progetti.

Evidentemente c'è una stretta interrelazione tra tutte le strutture CERT della Forza armata e Comparto difesa, che saranno meglio integrate nel costituendo Comando integrato. Devo anche dire che l'integrazione non è soltanto nell'ambito della Difesa, ma richiede un'integrazione interministeriale strettissima - che adesso c'è, ed è eccellente - con gli organi di sicurezza, con il DIS (Dipartimento delle informazioni per la sicurezza) e con tutti gli altri enti preposti alle operazioni, che ormai sono multidimensionali.

Nell'ambito dei lavori per la costituzione del Comando per le operazioni cibernetiche, la Difesa ha in atto un confronto continuo con tutti gli attori istituzionali interessati, in particolare con il Comparto informazioni e sicurezza, al fine di giungere ad una soluzione attagliata alle esigenze e condivisa per assicurare, nell'ambito del quadro normativo in vigore, il funzionamento delle nuove capacità *cyber* della Difesa, anche sulla base delle prerogative istituzionali.

In tale quadro, la Difesa, al fine di garantire una direzione unitaria alla sicurezza informatica delle reti e dei sistemi, ha avviato l'implementazione dell'iniziale struttura di comando e controllo. Il nucleo iniziale è rappresentato dal blocco capacitivo, che di fatto – insieme al già esistente CERT, che rappresenta l'attuale capacità di risposta della gestione informatica – costituisce la capacità *cyber* Difesa e il Comando difesa che è in fase di completamento, quindi il SOC (*Security operation center*), la protezione delle infrastrutture e la protezione del *network*.

Su queste, che sono le fondamenta, verrà poi costruita la capacità successiva di svolgere le *Network operation*, cioè non soltanto più la difesa del *network*, ma le *Computer network operation*, che si articolano in operazioni di difesa attiva, la *Computer network defence*, di raccolta informativa, la *Computer network exploitation*, necessaria a supportare lo sviluppo e la condotta delle operazioni nel dominio *cyber*; e il *Computer network attack*, a seconda delle responsabilità istituzionali nei diversi ambienti, nei teatri operativi o sul territorio nazionale più specificamente per gli organismi di sicurezza.

Le componenti rappresentate nel blocco soprastante costituiscono l'insieme delle capacità necessarie per sviluppare, nel loro insieme, le operazioni nel *network* dei computer (*Computer network operation*), che poi, integrate nei domini tradizionali – terrestre, marittimo e aerospaziale – consentiranno di effettuare le operazioni cibernetiche, le *cyber operation*, nella loro dimensione più importante.

Questa organizzazione per blocchi rappresenta concettualmente il progetto del Comando interforze per le operazioni speciali, che poi opererà – questo è importante – per cellule congiunte con gli altri sistemi di sicurezza.

Vi mostro adesso alcune lastrine in cui vi sono esempi schematici di progetti di

Analisi comandi *cyber* già realizzati o in fase di sviluppo in Paesi amici ed alleati. Abbiamo quindi *l'United States Cyber Command*, alle dipendenze dello *United States Strategic Command*, gli Stati Uniti operano per *Combat Commander*, quindi per comandi regionali o comandi funzionali. Per esempio, il comando supremo in Europa è un comando regionale; l'USSTRATCOM è un comando funzionale.

La Gran Bretagna è interessante perché il comando *cyber* britannico risiede in una sede congiunta, anche se in spazi diversi, con gli organi di sicurezza britannici. Quelli francesi, spagnoli e olandesi sono sostanzialmente simili, a parte alcune collocazioni organiche.

La nostra collocazione vede, alle dipendenze del Capo di Stato Maggiore della Difesa, il Comando operativo di vertice interforze, i comandi delle forze operative, il Comando per le forze speciali e il Comando interforze per le operazioni cibernetiche.

Prima di entrare maggiormente nel dettaglio del progetto della costituzione del Comando interforze per le operazioni cibernetiche, vediamo il contesto nel quale tali operazioni vengono condotte. Introduciamo dunque il concetto di spazio cibernetico, che consiste in un dominio creato dall'uomo, trasversale agli altri quattro domini tradizionali (terrestre, marittimo, aereo e spaziale), che è caratterizzato da mancanza di geospecificità, in quanto supera i confini geografici, limitate capacità di attribuzione, nella considerazione che solo raramente si è in grado di attribuire con certezza l'origine di un'attività nello spazio cibernetico ad una particolare entità statuale. Spesso, come dicevamo, si può dedurre che proviene da una certa area sulla base della complessità, ovvero da organizzazioni o gruppi di persone fisiche e giuridiche o indeterminate.

Quale dominio di nuova concezione – è molti anni che se ne parla, ma evidentemente la definizione si va man mano sostanziando con le diverse esperienze – tutti i principali Paesi e organizzazioni internazionali, compresa la NATO, che da questo punto di vista ha sempre rappresentato il motore, si stanno da un lato dotando di strutture militari di comando e controllo per operare nell'ambiente cibernetico, dall'altro studiando le diverse sfaccettature di tale dominio al fine di poter operare, anche nell'ottica di una cooperazione interalleata, in un quadro per quanto possibile chiaro, normato per operare in contesti interconnessi e/o federati, tenendo conto che evidentemente l'assenza di capacità in questo settore rappresenta la non possibilità di operare in modo credibile in un contesto interalleato.

Il raggiungimento della completa operatività delle strutture della Difesa – anche se ritengo oggettivamente che, man mano che la minaccia si evolverà, dovrà altrettanto evolversi il progetto, perché si tratta di una minaccia probabilmente permanente e in costante evoluzione – permetterà di completare le strutture della Difesa deputate a proteggere le infrastrutture e a operare nello spazio cibernetico, e consentirà, io credo, di contrastare adeguatamente gli attacchi condotti in tale dimensione, sia nel *network* nazionale della Difesa sia in quello esteso ai teatri operativi.

Passiamo a un'altra lastrina, abbastanza significativa e rappresentativa della realtà dell'impiego normale delle Forze armate nell'ambito dei comandi militari e delle forze proiettate al di fuori dei confini. Questa capacità *cyber* sarà implementata dalle cellule operative cibernetiche che saranno emanate dal Comando Interforze per le Operazioni Cibernetiche (CIOC) che quindi dovrà essere in condizione di emanare, per ciascun comando operativo, delle cellule per la condotta delle operazioni cibernetiche, collegate con il CIOC e con i vari sensori periferici della maglia, dai singoli mezzi che muovono, e comunque, nelle nuove concezioni *network* e nei nuovi sistemi d'arma anche i singoli combattenti muovono con dei sistemi cibernetici anche di geolocalizzazione tramite satellite per garantire la conoscenza dell'area delle operazioni.

Tale capacità *cyber* a livello tecnico funzionale opererà in sistema con il CIOC in madrepatria, per garantire, da un lato, la protezione degli assetti militari sempre più

decentralizzati e dall'altro la condotta delle possibili operazioni cibernetiche nell'area delle operazioni militari. Secondo la missione istituzionale e le direttive operative è una cosa molto importante, quella che definisce ogni operazione, che sono le regole di ingaggio, ossia le modalità sulle quali operano i nostri contingenti, che sono sempre definite al più alto livello di responsabilità politico.

Nello sviluppo del progetto CIOC sono previsti quattro elementi cardine. Il primo è quello dell'organizzazione: personale, logistica, dottrina, operazioni e le varie componenti normali di un comando, che poi dovranno essere in grado di proiettare i diversi elementi.

Il secondo è costituito dalla realizzazione delle infrastrutture necessarie per il costituendo CIOC. Quindi, si tratta di avere dei sistemi protetti e anche – oserei dire – delle modalità d'azione protette, che dovranno man mano crescere anche nella cultura di tutela cibernetica.

Il terzo fondamentale elemento si concretizza nella costituzione di opportuni ambienti virtuali per la capacità *cyber*, ovvero quello che noi chiamiamo *cyber range*, che poi è un istituto scolastico per la formazione ma anche un poligono virtuale per l'addestramento e il mantenimento delle capacità operative del personale impiegato nel settore *cyber*. Tale struttura, che auspicabilmente in futuro sarà federata con le analoghe capacità di Paesi amici e alleati, tra cui il centro di eccellenza NATO di Tallin, è in via di allestimento presso la Scuola telecomunicazioni delle Forze armate di Chiavari.

L'istituto opererà a favore degli ambienti interforze, interagenzia e interalleati e, soprattutto, in sinergia con il mondo accademico e quello industriale. Peraltro, il mondo accademico è un elemento anche centrale dello sviluppo delle operazioni *cyber*, perché in questo settore lo studio e la sperimentazione rappresentano un elemento centrale essendo un mondo in continua evoluzione cosicché nessuno di noi può dirsi al massimo della conoscenza.

Vi è inoltre il laboratorio *cyber*, Cyber Lab, che sarà realizzato sempre nella sede del Comando interforze delle operazioni cibernetiche, che permetterà di acquisire gli strumenti necessari per effettuare lo studio dei *malware* e dei rimedi contro la minaccia, oltre a fornire supporto ai responsabili della progettazione, sviluppo e gestione delle reti, man mano che la minaccia viene identificata e neutralizzata.

Il quarto elemento del progetto è relativo al personale, elemento sempre centrale delle organizzazioni. Come si è ormai imparato, bastano pochi individui altamente preparati, capaci e dotati per condurre attacchi *cyber* anche molto complessi. Quindi, tutti gli aspetti che vanno dalla selezione alla formazione, al reclutamento e al mantenimento del personale presso il CIOC, come in tutti gli altri ambienti cibernetici, sono fondamentali dal momento che si ritiene che più del 70 per cento della capacità generale di qualsiasi ambiente cibernetico dipenderà dall'abilità degli operatori.

Alla luce delle conoscenze tecniche estremamente specialistiche che alcuni operatori *cyber* dovranno possedere, sottolineo che probabilmente dovrà essere previsto il ricorso a reclutamenti mirati, che contempli anche la possibilità di selezionare detto personale in ambiti esterni alla Difesa, con appositi bandi di concorso e con le norme in vigore. Certamente occorrerà trarre beneficio da rapporti e dal supporto del mondo accademico e della ricerca e da altre istituzioni nazionali del comparto industriale.

Facciamo ora una breve previsione temporale della progettualità. Un credibile e realistico percorso di acquisizione delle capacità *cyber* fondamentali, iniziali della Difesa, prevede che entro il 2017 sarà possibile realizzare il Nucleo iniziale del Comando interforze per le operazioni cibernetiche che – di fatto – ha già preso forma, per poi raggiungere, intorno alla fine del 2018, la capacità di condurre operazioni cibernetiche.

In tale arco temporale, 2017-2019, occorrerà quindi completare soprattutto la protezione dell'info dominio della Difesa e acquisire i principali elementi capacitivi ovvero infrastruttura del comando, potenziamento della protezione del dominio, as-

setti per la pianificazione e gestione delle operazioni, *cyber operations picture*, cioè designare il quadro delle operazioni e realizzare il *cyber range* e il laboratorio *cyber*.

Un elemento essenziale e condizionante è la formazione e la preparazione del personale. Contiamo già su alcuni validi operatori, ma non dobbiamo essere assolutamente ancora soddisfatti. A tal fine – sulla base delle indicazioni ministeriali, in particolare quelle del nostro Ministro della difesa – anche tramite l'accesso ai finanziamenti previsti dal fondo in materia di protezione cibernetica e sicurezza informatica nazionale, ai sensi della legge di bilancio 2016, è stato sviluppato un piano programmatico per acquisire un *set* di capacità sufficientemente ampio, a partire da quelle volte al potenziamento delle protezioni dell'info dominio della Difesa.

Le risorse verranno rese disponibili sia attraverso i citati fondi per la sicurezza *cyber*, sia da altri che verranno poi individuati per i fondi di investimento, fermo restando che il volume dovrà essere reso disponibile sulla base anche delle capacità e della completezza delle progettualità che verranno man mano realizzate, e tenendo anche conto che non dobbiamo fare duplicazioni degli impegni e degli sforzi che verranno presi in altri settori.

Avviandomi alla conclusione del mio intervento, condivido alcune considerazioni. Sin dai primi degli anni 2000 si è registrata la condotta di operazioni cibernetiche. Cito soltanto alcuni virus principali o alcune attività tipo Stuxnet, che ho imparato anch'io preparandomi per questa relazione, perché non sono sicuramente un esperto cibernetico. Mi hanno spiegato che è un virus di particolare capacità, che addirittura ha messo in crisi i progetti nucleari di una nazione, quindi vi è la capacità di alto livello di organismi statuali di attaccare le reti.

Un attacco cibernetico di alto profilo, condotto da un organismo statuale o addirittura multinazionale, può creare dei danni assolutamente elevati.

Da noi gli attacchi cibernetici sono esponenzialmente aumentati e molte sono le evidenze che sono state registrate.

In questo contesto, assume un'elevatissima priorità la rapida implementazione del Comando interforze per le operazioni cibernetiche, progetto prioritario per la difesa e anche elemento essenziale per consentire di sviluppare in maniera unitaria i progetti, evitando le duplicazioni e rappresentando l'elemento di raccordo e di riferimento sia per l'attività di controllo e di ispezione degli organismi di governo e degli organismi parlamentari, sia per operare a stretto contatto con tutte le altre organizzazioni di riferimento.

Gli impegni presi dalla difesa, in linea con gli obiettivi definiti sia in ambito europeo sia in ambito NATO, comprendono la realizzazione di solide capacità di *cyber defence* e di protezione delle infrastrutture.

A tal riguardo, questo concetto è stato ulteriormente rafforzato nel già ricordato *summit* di Varsavia da parte del segretario generale, con la conseguente sottoscrizione del *Cyber defence pledge*.

Con esso, da un lato, si introducono i criteri volti a definire le misure minime di sicurezza cibernetica cui tutti i Paesi membri dovranno attenersi e, dall'altro, si introduce un forte orientamento verso il concetto « *non-compliance non-participation* », in base al quale, se non si aderisce a questi princìpi, non si può partecipare alle attività.

La Difesa, nell'ambito delle capacità *cyber* che sta sviluppando sia per proteggere i suoi sistemi sia per pianificare e condurre operazioni militari nel dominio *cyber*, in linea con il quadro normativo vigente, è come di consueto a disposizione del Paese, pronta a rendere disponibili in ogni momento le proprie capacità attuali e quelle future nel campo *cyber security*, per concorrere alla crescita della capacità cibernetica nazionale.

Con queste ultime osservazioni, concludo il mio intervento. Sono ovviamente a disposizione per le vostre eventuali domande o richieste di chiarimento. Vi ringrazio per l'attenzione.

PRESIDENTE. Grazie a lei, Generale, per le cose che ci ha detto ed anche per la presentazione informatica che ci ha lasciato, di cui autorizzo la pubblicazione in

allegato al resoconto stenografico della seduta odierna (*vedi allegato*).

Do ora la parola ai colleghi che intendano intervenire per porre quesiti o formulare osservazioni.

MASSIMO ARTINI. Ringrazio il Generale Graziano per averci fornito un quadro riassuntivo rispetto a quello dell'indagine, con alcuni spunti attualizzati. Io avrei alcune domande, che mi sono state stimolate anche dalla presentazione informatica che ha illustrato.

Lei ha parlato di *cyber operation*. Il concetto di *cyber operation* o comunque dell'azione che si deve fare per contrastare chi attacca, di cui sempre di più la stampa si sta occupando, a mio modo di vedere, ha un problema di copertura legale.

Le chiedo la sua opinione sul ruolo che le Forze armate hanno nella difesa del Paese rispetto ad altre realtà, perché nell'ambito della *cyber* si fondono e diventano non molto chiari i confini tra la sicurezza, la difesa e la raccolta delle informazioni.

Pertanto, vorrei una sua opinione su quale attore possa facilitare la costituzione di un ambito di *cyber operation* che sia anche coperto normativamente.

A questo si legano due temi. Il primo è la formazione del personale, non solamente nella Difesa, ma più in generale in tutti gli ambiti della *cyber*. Il rischio che si corre in un settore così importante per la sovranità nazionale è che il personale sia cooptato da aziende che hanno un'esperienza pluriennale nel settore e che comunque non sia totalmente integrato con il mondo della Difesa. Infatti, sicuramente non basta un anno per formare tecnici capaci di operare nella *cyber*, sia da un punto di vista tattico sia da un punto di vista strategico. Non occorre un corso di formazione, ma si impara con l'esperienza.

A questo proposito, vorrei sapere qual è l'approccio che lei sta mettendo in campo per la progettazione dei prossimi cinque o dieci anni nel mondo *cyber* per quanto riguarda la formazione.

Le prime lastrine ci hanno indicato la nostra struttura, paragonata con quelle del resto del mondo. A tal proposito la ringrazio, perché in alcune altre audizioni nel corso dell'indagine non c'era la completezza di tutti gli altri attori o perlomeno di quelli alleati.

Quello che emerge nella struttura indicata nel decreto del Presidente del Consiglio dei ministri del 2013 è una discreta polverizzazione sia dal lato strategico, sia dal lato tattico. I CERT sono polverizzati e gli attori sono molteplici, per cui è difficile dare una chiara linea di comando e comprendere chi fa alla fine il lavoro sporco di difesa del mondo *cyber*.

Vorrei sapere se c'è una valutazione della Difesa rispetto a una possibile riforma su questo tema.

Concludo – non me ne vogliano i colleghi, ma questa è l'ultima – con una domanda riguardo alle missioni internazionali (è stata da poco trasmessa la relazione governativa e, dunque, siamo nella fase di prima applicazione della legge-quadro e, quindi, delle prime deliberazioni).

Noi disponiamo di strumenti che ci permettono di essere relativamente sicuri (« certamente sicuri » non si può dire in questo mondo), perché le comunicazioni classificate per le missioni che facciamo all'estero avvengono, da quanto mi è dato sapere, tramite canali satellitari.

Vorrei sapere, in primo luogo, se negli ultimi due anni sono incrementate le minacce, soprattutto all'estero, e quindi anche gli attacchi e, in secondo luogo, quali strumenti in quelle particolari missioni sono messi in campo per contrastare eventuali falle che non derivino direttamente dai canali classificati. Ad esempio, appoggiarsi per la normale navigazione a *provider* locali potrebbe essere una falla che incrementa questo livello di pericolosità.

CLAUDIO GRAZIANO, *Capo di Stato Maggiore della Difesa*. Le operazioni cibernetiche sono un dominio abbastanza nuovo, per cui è sicuramente difficile discernere nei vari settori tra *exploitation*, *attack* e *defence*.

È un ambiente nuovo ed è un ambiente in cui la difesa opera in coordinamento con gli altri organismi. È evidente che io mi sento più di una volta al giorno con il direttore del DIS e con i coordinamenti, ma sull'architettura di questa struttura esiste

una valutazione generale che riguarda tutto il mondo, non solo il mondo della difesa e che è di competenza degli organismi di sicurezza.

Noi partecipiamo con l'attivazione del CIOC, che raccoglierà le capacità della Difesa messe a disposizione e integrate in quelle che già sappiamo che saranno delle cellule di coordinamento, in cui non ci sarà soltanto il personale della Difesa, ma si opererà congiuntamente con il personale di altre agenzie e dei servizi.

È chiaro che gli spazi di responsabilità devono essere definiti. Fuori dal territorio nazionale, nelle missioni, la responsabilità dovrà essere del comandante dell'operazione, che risponderà a 360 gradi della sicurezza.

A questo proposito - lo sottolineo perché è importante - io ho citato le regole di ingaggio. Attualmente ci sono delle regole d'ingaggio che valgono per la protezione, per la sicurezza e per l'attivazione. Probabilmente ci dovranno essere delle regole d'ingaggio relative anche alla dimensione *cyber*.

Per esempio, le regole di ingaggio della missione UNIFIL (*United nations interim force in Lebanon*) che ho comandato in Libano sono approvate dal Consiglio di sicurezza delle Nazioni unite.

Sulle regole d'ingaggio di UNIFIL c'è scritto che l'uso delle armi è regolato dall'intento ostile, quindi, pur essendo una missione delle Nazioni unite nell'ambito del capitolo sesto, che riguarda soltanto la difesa estesa del personale, ossia i cosiddetti baschi azzurri, l'impiego dell'arma deriva dalla minaccia alla sua sicurezza e viene valutata dall'individuo sulla base dell'intento ostile.

Dunque, se nelle operazioni avviene un attacco cibernetico che mette a rischio la sicurezza del personale, sulla base delle regole di ingaggio, il comandante deve operare la risposta e l'attacco e garantire la sicurezza e le operazioni del sistema.

C'è una parte sul territorio nazionale in cui la responsabilità non sarà della Difesa, ma competerà agli organi di sicurezza, sulla base delle disposizioni e del quadro che verrà delimitato, mentre in altri settori, avvalendosi degli organi di sicurezza, ci sarà una responsabilità della Difesa.

Sarà, quindi, fondamentale il coordinamento fra i diversi settori, che lavoreranno insieme nell'ambito di cellule integrate. Il fatto che in altri Paesi abbiano realizzato le cellule congiunte è indicativo di queste esigenze.

Per quanto riguarda le missioni internazionali, possiamo immaginare la delicatezza, perché noi abbiamo anche dei sistemi di difesa aerea che sono impiegati e che viaggiano sui canali di sicurezza radar della NATO. L'intera difesa aerea del territorio nazionale in definitiva è affidata alla NATO e agli organismi satellitari della NATO stessa.

Sono sistemi ad altissima protezione e ad altissima sicurezza, quindi probabilmente non sono il primo simbolo di un attacco *cyber*, perché l'attacco a questi sistemi forse potrebbe venire soltanto da una direzione e, quindi, potrebbe comportare delle reazioni importanti.

Tuttavia, più si diffonde, più è delicata: pertanto i sistemi commerciali di tipo semplice non possono essere utilizzati per far viaggiare informazioni classificate o informazioni di sicurezza.

Dall'Afghanistan abbiamo riportato l'*Afghan mission network*, che è stato l'esempio sul quale abbiamo costruito lo sviluppo dell'intero sistema informatizzato del « Soldato futuro » e del sistema di sicurezza. Il fatto che attraverso queste dotazioni al comando giungevano le informazioni dagli aerei, dalle navi e dal personale mi permetteva di costituire quello che si chiama « blue force tracking », ovvero di conoscere la situazione del personale sul terreno.

Si tratta di sistemi di alta sicurezza, che hanno rischi talmente elevati da richiedere protezioni elevate, ma di fronte a un attacco su questo dovrebbe esserci una risposta immediata e diretta della Difesa. Se si oscura l'immagine mentre delle forze sono a contatto, evidentemente i rischi sono elevatissimi e in questo caso la risposta deve essere anche immediata.

LUIGI LACQUANITI. Ringrazio il Generale per l'ampia spiegazione odierna. La sua audizione arriva dopo una serie di

visite che abbiamo svolto presso uffici e comandi specializzati nel settore della *cyber security*.

La prima domanda è riferita ad alcune ricerche che sono state svolte recentemente anche presso Palazzo Chigi sul fenomeno del terrorismo di matrice islamista. Quando noi parliamo di *cyber security*, e in particolare di quella demandata al suo comando oltre che agli altri organismi che lei ha citato, intendiamo una difesa principalmente improntata a un attacco caratterizzato da « simmetricità » o possiamo fare riferimento anche a modalità di attacco che trovano nel *web* o comunque nello strumento della *cyber* un'espressione del terrorismo di matrice islamista ?

Inoltre, è demandata a questi strumenti anche la difesa dal terrorismo e dalle modalità che a oggi questo attua, non soltanto per, ahimè, attaccare i Paesi occidentali e organizzare gli attacchi, ma anche – ed arrivo alla seconda domanda – per organizzare il reclutamento in Occidente, come è stato messo in luce da queste ricerche ?

Vi è un ruolo delle strutture e dei vostri comandi anche nella lotta al terrorismo e, in caso affermativo, in che misura ? Vi è una collaborazione da questo punto di vista con le Forze di polizia del nostro Paese e con quelle degli altri Paesi occidentali ?

ANTONINO MOSCATT. Io mi permetto in premessa, non per piaggeria, di rivolgere – a nome del Gruppo, ma penso anche a nome di tutta la Commissione a lei Generale e alle Forze armate, un ringraziamento per il lavoro che state svolgendo in questi giorni e in queste ore nei luoghi in cui si stanno verificando le tragedie legate agli eventi sismici ed all'ondata di maltempo, perché il vostro impegno è eccezionale e, al di là della retorica, consente di salvare vite umane. Noi cogliamo l'occasione per ringraziarvi di questo.

Vado subito alle domande e alle riflessioni. Alcune, in realtà, sono state anticipate dai miei colleghi. Lei parlava di circa 500 attacchi al mese, che non sempre vengono fatti da privati, ma anche da Stati e da istituzioni.

In questo caso, che succede ? Noi siamo un'istituzione. Se riceviamo un attacco da un certo Stato o da una certa regione, che succede ? Come ci si approccia alla vicenda ? Che cosa si fa ? Qual è il rapporto diplomatico che si crea con Stati che ufficialmente fanno degli attacchi ?

Lei ha poi parlato anche di approccio sinergico. Al di là delle esperienze avviate durante le missioni, ci sono altri campi d'azione in cui si sta provando a testare questo approccio sinergico o in questo momento si testano solo nel caso in cui vi siano le missioni ?

Quando ci sono le missioni o in altri campi, si riesce a salvaguardare la proprietà dei nostri dati, dei nostri « segreti » ? Dico questo pur sapendo che, più sinergia si crea, più si riesce a combattere il fenomeno del terrorismo e maggiore è la sicurezza.

Mi ricollego adesso alla vicenda della formazione. Io immagino che oggi vi sia la necessità di creare una classe di intelligenze che siano capaci di affrontare bene il fenomeno e di supportare le forze della Difesa in tal senso.

Abbiamo visto quali sono le prospettive (il *cyber range*, il *cyber lab*), ma fino a ora come si è proceduto ? Quali forze si utilizzeranno, da ora a quando si creeranno questi strumenti, per garantire i processi che sono in corso ?

Infine, abbiamo visitato anche delle imprese private che ponevano delle questioni rispetto alla gestione degli acquisti. In alcuni casi, si seguono dei tempi che sono tempi normali per gli acquisti di alcuni programmi. Nel caso di specie, in questo settore, quando è concluso l'appalto e vi è la consegna dei programmi, probabilmente quei programmi sono per certi versi già superati. Nello stesso tempo, in alcuni casi vi è una parcellizzazione degli acquisti, quindi magari un pezzo di rete viene gestito da una determinata società e un altro sistema viene gestito da un'altra società.

Non c'è il rischio in questo caso di non essere realmente efficaci, o comunque di dare il nostro *know how* e i nostri dati riservati a più aziende, che magari non godono del segreto di Stato ? Siamo certi che, essendo in mano loro, le chiavi del nostro sistema siano al sicuro ?

Infine, il collega Lacquaniti ha dato uno spunto molto interessante. In questo periodo si parla molto di anti-radicalizzazione. Rispetto alla sicurezza cibernetica, quali strumenti sono stati messi in atto su questo settore ?

CLAUDIO GRAZIANO, *Capo di Stato Maggiore della difesa*. Sicuramente le minacce più rilevanti sono quelle che provengono dal terrorismo internazionale e dalle attività svolte da ISIS, quindi la Difesa deve essere rivolta verso qualsiasi tipo di attacco.

Dopodiché, gli aspetti sul territorio nazionale e gli aspetti relativi all'*intelligence* specifica sono di competenza del Ministero degli interni e degli organismi di sicurezza. In questo caso, noi offriamo e diamo collaborazione, in base alle norme, agli accordi, agli aspetti interministeriali e interdisciplinari della situazione.

Nelle operazioni, come abbiamo detto, c'è una responsabilità diretta dei comandi militari, dei comandi multinazionali o dei comandi NATO a cui partecipiamo.

D'altra parte, come è noto, esistono dei livelli di sicurezza: il segreto nazionale, relativamente alla trattazione di documentazioni e aspetti nazionali; il segreto NATO, per le attività che vengono svolte su reti NATO; il segreto di coalizione, perché per esempio in Iraq si opera attraverso le attività di coalizione.

Ci sono, dunque, attività ad alta classifica, ma certamente il controllo delle reti cibernetiche e il lavoro della rete cibernetiche sono aspetti essenziali della lotta al terrorismo.

Gli attacchi su tutta la rete della NATO riportati dal Segretario generale NATO sono circa 500. Come ho detto prima, è difficile che portino una firma; quindi è difficilissimo risalire all'origine effettiva. Tuttavia, se sono particolarmente strutturati, la deduzione è che vengano da un Paese.

D'altra parte, non è di mia competenza, ma lo abbiamo visto recentemente con gli ultimi problemi relativi alle critiche sulle elezioni presidenziali americane. Ci sono delle disinformazioni o delle informazioni. Io non le conosco, ma evidentemente stiamo operando in un settore in cui un attacco particolarmente strutturato che cerca le reti, che cerca le origini delle forze, ha una determinata deduzione, mentre uno che cerca di operare nell'ambito terrorismo ne ha un'altra.

Comunque, ci sono degli appositi organismi di analisi su questo settore. In caso di attacco sul *network* della difesa, viene immediatamente attivato il Nucleo interministeriale situazione e pianificazione (NISP) per operare tutte le correzioni. Quando viene rilevato un attacco, viene portato a questi nuclei di sicurezza cibernetica interministeriali, in modo che tutti siano informati e possano operare insieme per risolvere il problema, mantenendo quell'approccio sinergico di cui abbiamo detto, che è l'elemento centrale e di perfezionamento di attività di questi tempi.

Ci sono dei gruppi di lavoro permanenti per individuare queste attività e vi sono taluni soggetti. Per esempio, io ho citato il generale Palmieri, che in questo momento è il responsabile per la difesa della realizzazione delle proposte concrete, degli interventi, dei progetti, delle reti, delle attività e di tutta la parte programmatica di sviluppo dei sistemi. Il generale collabora con il reparto informazione e sicurezza, per l'acquisizione, per esempio, di software e per altri argomenti.

È qui presente anche il generale Vestito, dell'Aeronautica militare, che è il responsabile del nucleo iniziale del Comando CIOC, che è quello che ha il raccordo fra la parte C4, di acquisizione, di preparazione per situazioni di studio e anche di formazione (perché sono specialisti in comunicazione) e la parte informazioni, per dare vita a questa struttura che, come in tutte le cose, collaborerà con gli altri aspetti.

La formazione è un aspetto essenziale. In questo momento noi ci avvaliamo dei tecnici a disposizione e di quelli che hanno acquisito molta esperienza con le missioni internazionali e NATO. Sono essenzialmente gli ufficiali, i sottufficiali e i militari che vengono dal settore delle comunicazioni dell'Esercito, della Marina e dell'Aeronautica, quindi hanno svolto specifici studi e hanno specifiche lauree nel settore.

Ovviamente un aspetto essenziale è che ci avvaliamo anche di ditte e di società civili, che sicuramente hanno più facilità nell'avere i cervelli, ossia quelli che studiano questi sistemi, che sono difficilmente sviluppabili interamente in ambito Difesa, e con cui bisogna cooperare.

Nell'acquisizione di tutti questi *software* è importante che ci sia la possibilità di controllo degli organi di sicurezza e degli organi istituzionali. Per quanto riguarda le imprese nazionali, questo probabilmente è più agevole, però si opera anche in ambito internazionale, seguendo il codice di appalto e le sue connesse procedure.

Queste cose, comunque, si svilupperanno nel tempo. Probabilmente dovrebbero aumentare le attività di controllo di sicurezza per chi fa appalti in questo specifico settore e su questo specifico argomento.

Ad ogni modo, essendo un dato tecnico, se c'è bisogno, mi riservo di fornire qualche dettaglio in più, chiedendo a coloro che fanno il contratto e che controllano che vengano segretate le informazioni.

CARLO GALLI. Generale, nel ringraziarla per la sua esposizione, le voglio chiedere un commento, se è possibile, su un'impressione che ho avuto, che potrebbe essere sbagliata.

Quando sono stati mostrati i diagrammi dei diversi livelli, sia gerarchici sia funzionali, relativi alla questione della *cyber* difesa nel nostro Paese e sono stati paragonati agli analoghi diagrammi di altri Paesi, mi è parso che i nostri fossero molto più complicati e prevedessero un numero di livelli gerarchici e operativi superiore.

Vorrei sapere se questo nasce da una semplificazione che avete operato nella costruzione di queste lastrine a scopi dimostrativi o se, invece, la mia impressione è fondata sull'esperienza e sulla realtà, cosa che io non posso sapere ?

LUCA FRUSONE. La mia domanda è collegata alla formazione e, in particolare, al momento prima, quello del reclutamento. Quando abbiamo visitato il Comando C4 ci siamo resi conto che c'è un apporto notevole di ditte esterne per il *know how* e per la risorsa umana da prestare a queste attività. Vorrei sapere se, al riguardo, ha intenzione di creare una sorta di percorso.

Inoltre, considerando che formare delle persone è comunque un percorso lungo e dispendioso, vorrei sapere se ha intenzione di creare un canale specifico per il reclutamento all'esterno di persone che magari già di loro hanno delle capacità e che possono essere inserite in questo discorso.

Ho visto, ad esempio, che quest'anno la Marina ha sperimentato un percorso particolare per i Comsubin, creando un canale più attento a queste esigenze.

Infine, oltre al reclutamento, vorrei sapere cosa si prevede per la fuoriuscita, cioè se c'è anche un progetto che riguardi le persone che, per qualsiasi motivo, dopo aver ottenuto una certa esperienza e lavorato in determinati settori, si ritrovano al di fuori e, quindi, paradossalmente potrebbero loro stessi costituire una minaccia.

DINO SECCO. Vorrei fare alcune domande abbastanza semplici. L'Esercito è un'organizzazione che è molto estesa nel territorio, con tante ramificazioni, dove passano milioni di informazioni e di dati. Sono necessarie delle dorsali. Queste dorsali sono di proprietà dello Stato italiano o sono proprietà di privati italiani o stranieri ?

Ci sono dei macchinari per difendere questi nostri sistemi. Di solito sono di due scuole: israeliani o americani. Noi quali abbiamo scelto ?

Infine, vorrei sapere se è vero che una parte del nostro sistema qualche anno fa è stato venduto all'esercito turco.

CLAUDIO GRAZIANO, *Capo di Stato Maggiore della difesa*. Sono state poste domande molto interessanti e stimolanti. Inizio dalle lastrine, dicendo che sono semplificate, anche se questo non risponde completamente alla domanda.

Io credo che il nostro Paese, dal punto di vista del sistema di sicurezza e difesa, abbia fatto grossi passi avanti. Non voglio fare pubblicità, ma io vedo che per la difesa e la sicurezza spesso ci collochiamo davanti

ad altri Paesi. Secondo me, ciò è vero, per esempio, nella cooperazione fra le forze di sicurezza e le Forze armate, nella tutela del territorio e negli interventi di pubblica calamità.

Nell'ambito della *cyber security* qualcosa deve essere fatta – verrà proposta e verrà fatta – al fine di semplificare la struttura, fermo restando che dalla nuova struttura si vede che, al di là del livello di indirizzo politico del CISR, a livello tecnico devono partecipare i tecnici specifici.

A prescindere dalla responsabilità, che è in corso di definizione, sulla gestione generale della minaccia *cyber* specialmente sul territorio nazionale e, quindi, della responsabilità della sicurezza in generale, alcuni di questi Paesi (Gran Bretagna e Stati Uniti) hanno maturato probabilmente una maggiore esperienza *cyber* nel passato. Erano in possesso di norme legislative che gli permettevano a priori determinate operazioni nel mondo *cyber* e nel mondo generale della sicurezza, in cui noi ci siamo sviluppati nell'ambito del rispetto del nostro dettato costituzionale.

Questo è fondamentale: bisogna operare nell'ambito delle norme vigenti e nel rispetto delle leggi. Nel rispetto delle leggi, individuiamo la proposta migliore. Dopodiché, in modo armonico, attraverso il Governo e i sistemi parlamentari, se ci saranno alcune proposte di miglioramento e di semplificazione, verranno sicuramente presentate.

Devo, però, dire che secondo me una chiave importante del successo delle relazioni sono i rapporti di cooperazione interministeriale che esistono attualmente fra Difesa, Ministero degli interni e Ministero degli esteri.

Cito un esempio semplice come quello dell'ospedale di Misurata. La dislocazione dell'ospedale per scopi umanitari a Misurata ha coinvolto tutti gli organi che ho citato, perché sono state fatte negoziazioni diplomatiche, sono stati presi contatti con i servizi, sono stati inviati uomini e navi, c'erano dei sistemi di sicurezza e di avvistamento che coordinavano il movimento, dei sistemi di comunicazione che aggiornavano costantemente il comandante interforze e il Capo di Stato Maggiore Difesa, che minuto per minuto prendevano da spazi sicuri le decisioni e indirizzavano.

Chiaramente su tutto questo c'è un ampio spazio di miglioramento. Trarre ammaestramento da altri Paesi non è mai sbagliato, tenendo presenti anche le capacità nazionali.

Le dorsali, che sono la Rete numerica nazionale e i ponti radio, sono della Difesa. Si tratta di reti in fibra ottica che interessano tutto il territorio nazionale comprese le isole e utilizzano principalmente sistemi nazionali della Leonardo o devoluti a raggruppamenti temporanei di imprese nazionali.

Sul fatto che siano principalmente di origine israeliana o americana onestamente non so rispondere. Per ciò che concerne la Turchia, gli ultimi materiali che abbiamo fornito alla Turchia sono gli elicotteri *T129*. Onestamente, non so se ci sono altre attività, però sicuramente mi posso informare.

Quanto al percorso di formazione, è sicuramente come afferma l'onorevole Frusone. In fondo – questo è un aspetto importante – il fatto che spesso abbiamo avuto successo nelle operazioni, che molti comandanti in operazioni vengano dalle Forze armate italiane si deve al fatto che l'abilità e la capacità dei singoli militari a operare derivano dai percorsi.

Bisognerà fare dei percorsi specifici, come li abbiamo fatti per la conoscenza delle lingue e per altri settori, e prevedere il reclutamento anche sulla base di capacità specifiche, mettendo delle norme per facilitare l'ingresso. Non solo i Comsubin, ma tutte le forze speciali hanno dei canali di formazione e di reclutamento principali, perché si tratta di uno strumento che possiamo paragonare a quello cibernetico, molto delicato, da reclutare, da mantenere, da addestrare e che si usura velocemente.

Per ciò che concerne lo scambio all'esterno, io sono addirittura favorevole. Io non vedo nulla di pregiudizievole se uno che abbia acquisito capacità all'interno della Difesa e del mondo cibernetico poi possa entrare nel comparto privato, mantenendo da un lato il giovane nelle Forze armate e

dall'altro fornendo un materiale sicuro allo strumento industriale. Dobbiamo aiutarli e facilitarli.

Dopodiché, vigilare che non rappresentino a loro volta un nemico è una nostra capacità. Mi solleva il fatto che credo che l'Italia sia il Paese che ha meno *foreign fighter* in assoluto. Altri Paesi nel mondo hanno un problema gigantesco, mentre noi non ce l'abbiamo.

Preparare delle persone che fanno un'esperienza di qualche anno nelle Forze armate e che poi, attratte giustamente da un compenso più elevato, possano andare da un'altra parte e costituire un'osmosi e un nostro riferimento è una cosa che ricerchiamo in tutte le Forze armate. I nostri specialisti, dopo un certo tempo, vanno nell'industria della difesa. Queste industrie, oltre a fornirci magari il pacchetto di protezione informatica, ci forniscono anche il personale che conosciamo e che, quindi, ci dà sicurezza, creando un'osmosi in generale per il bene del Paese.

Oserei dire che mi trova favorevole e che anzi dovrà essere parte di questo percorso.

PRESIDENTE. Ringrazio ancora il Generale Graziano per le cose che è venuto a dirci, che sicuramente saranno molto utili per concludere la nostra indagine conoscitiva. Ci riserviamo eventualmente di chiederle ulteriori dettagli, magari per iscritto, se dovesse servire a comporre la relazione conclusiva.

Dichiaro conclusa l'audizione.

La seduta termina alle 15.40.

Licenziato per la stampa
il 24 maggio 2017

STABILIMENTI TIPOGRAFICI CARLO COLOMBO

ALLEGATO

STATO MAGGIORE DELLA DIFESA
Stato Maggiore Difesa - Ufficio Capo di Stato Maggiore
"La Difesa e il mondo della Cyber Security"
Audizione da parte della 4ª Commissione Difesa
Generale Claudio GRAZIANO
Capo di Stato Maggiore della Difesa
Roma, 25 gennaio 2017

OBIETTIVO DELL' AUDIZIONE

Stato Maggiore Difesa - Ufficio Capo di Stato Maggiore

Illustrare:

- l'attuale organizzazione e capacità di *Cyber Defence* della Difesa;
- le future evoluzioni organizzative nel settore militare delle *Cyber Operations*;
- La costituzione del Comando Interforze per le Operazioni Cibernetiche.

AGENDA
Stato Maggiore Difesa - Ufficio Capo di Stato Maggiore
1 Analisi della minaccia
2 Quadro normativo vigente
3 Attuale capacità *Cyber Defence*
4 Evoluzione verso *Cyber Operations*
5 Il progetto Comando Interforze per le Operazioni Cibernetiche (CIOC)
6 Considerazioni finali
3 di 24

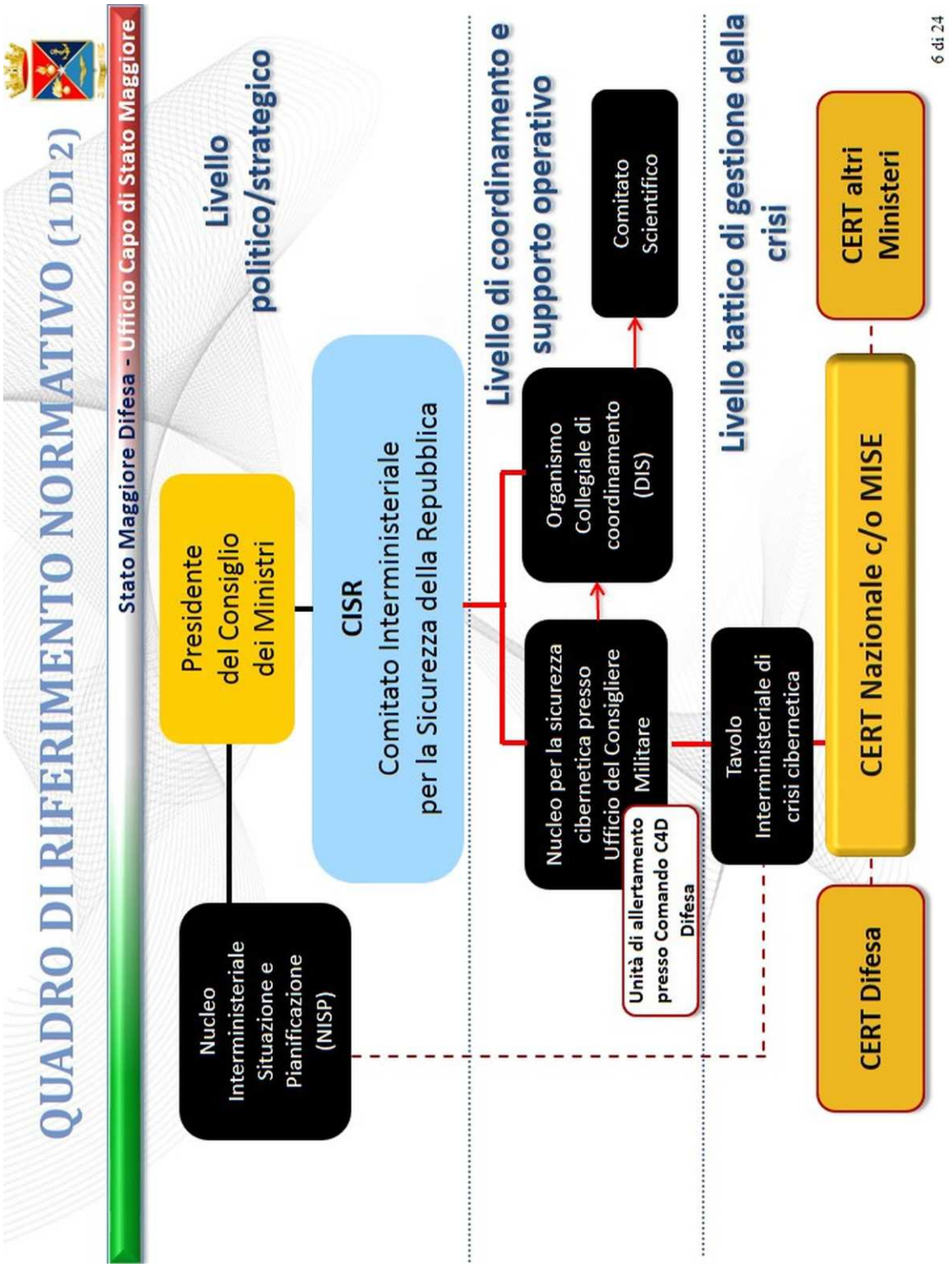
ANALISI DELLA MINACCIA (1 DI 2)

- Rapida evoluzione e crescente rilievo in proporzione alla "dipendenza informatica" dei Paesi

- Attori statuali, non-statuali e senza identità
- Diretta incidenza su settori militari, come le operazioni (Comando e Controllo)
- L'elevato livello tecnologico militare è anche una vulnerabilità
- La NATO chiede come elemento essenziale la sicurezza informatica e la protezione cibernetica

ANALISI DELLA MINACCIA (2 DI 2)

Stato Maggiore Difesa - Ufficio Capo di Stato Maggiore

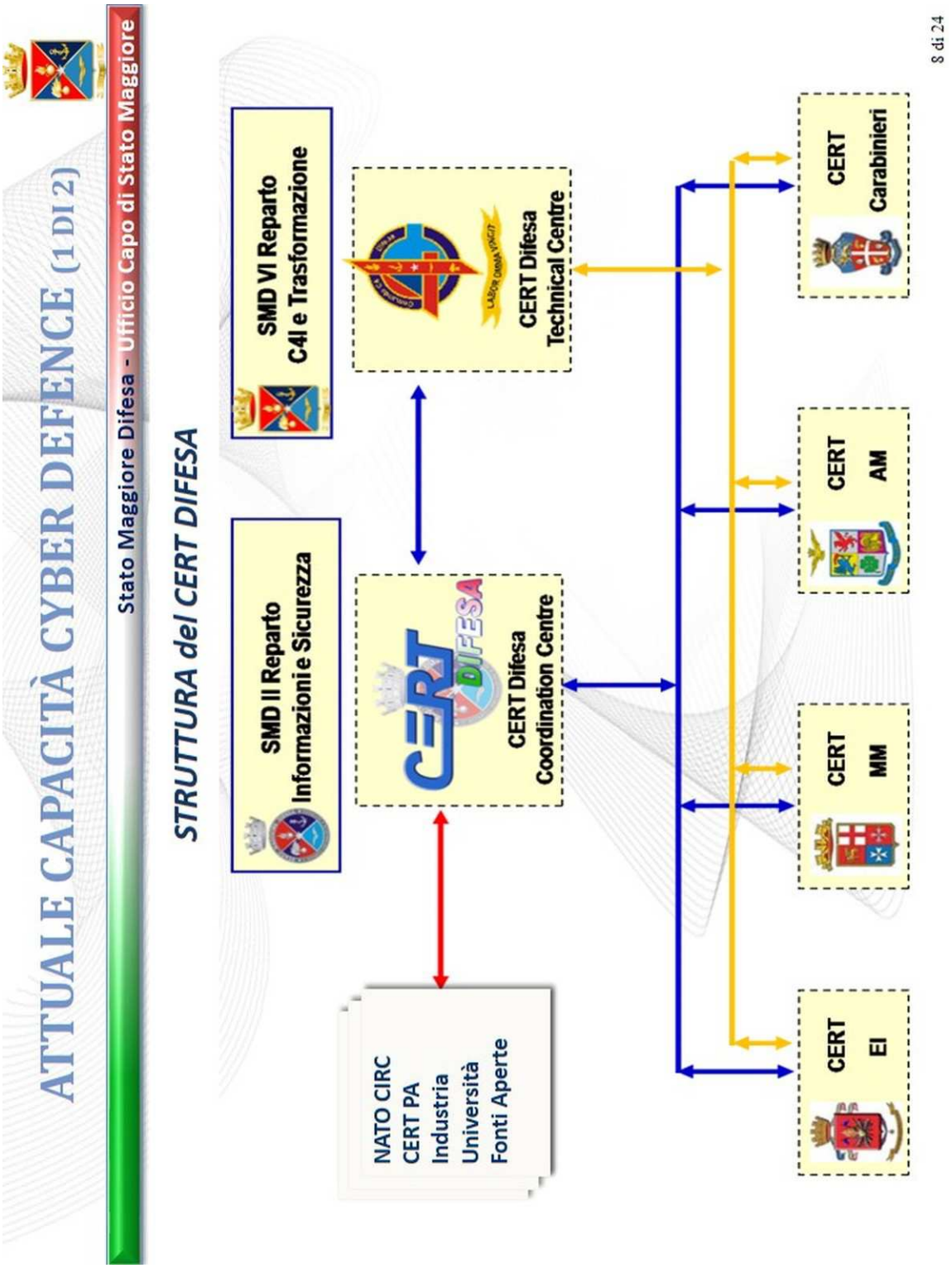

QUADRO DI RIFERIMENTO NORMATIVO (1 DI 2)
Stato Maggiore Difesa - Ufficio Capo di Stato Maggiore
Livello politico/strategico
Presidente del Consiglio dei Ministri
CISR
Comitato Interministeriale per la Sicurezza della Repubblica
Nucleo Interministeriale Situazione e Pianificazione (NISP)
Livello di coordinamento e supporto operativo
Organismo Collegiale di coordinamento (DIS)
Comitato Scientifico
Nucleo per la sicurezza cibernetica presso Ufficio del Consigliere Militare
Unità di allertamento presso Comando C4D Difesa
Livello tattico di gestione della crisi
Tavolo Interministeriale di crisi cibernetica
CERT altri Ministeri
CERT Nazionale c/o MISE
CERT Difesa
6 di 24

QUADRO DI RIFERIMENTO NORMATIVO (2 DI 2)

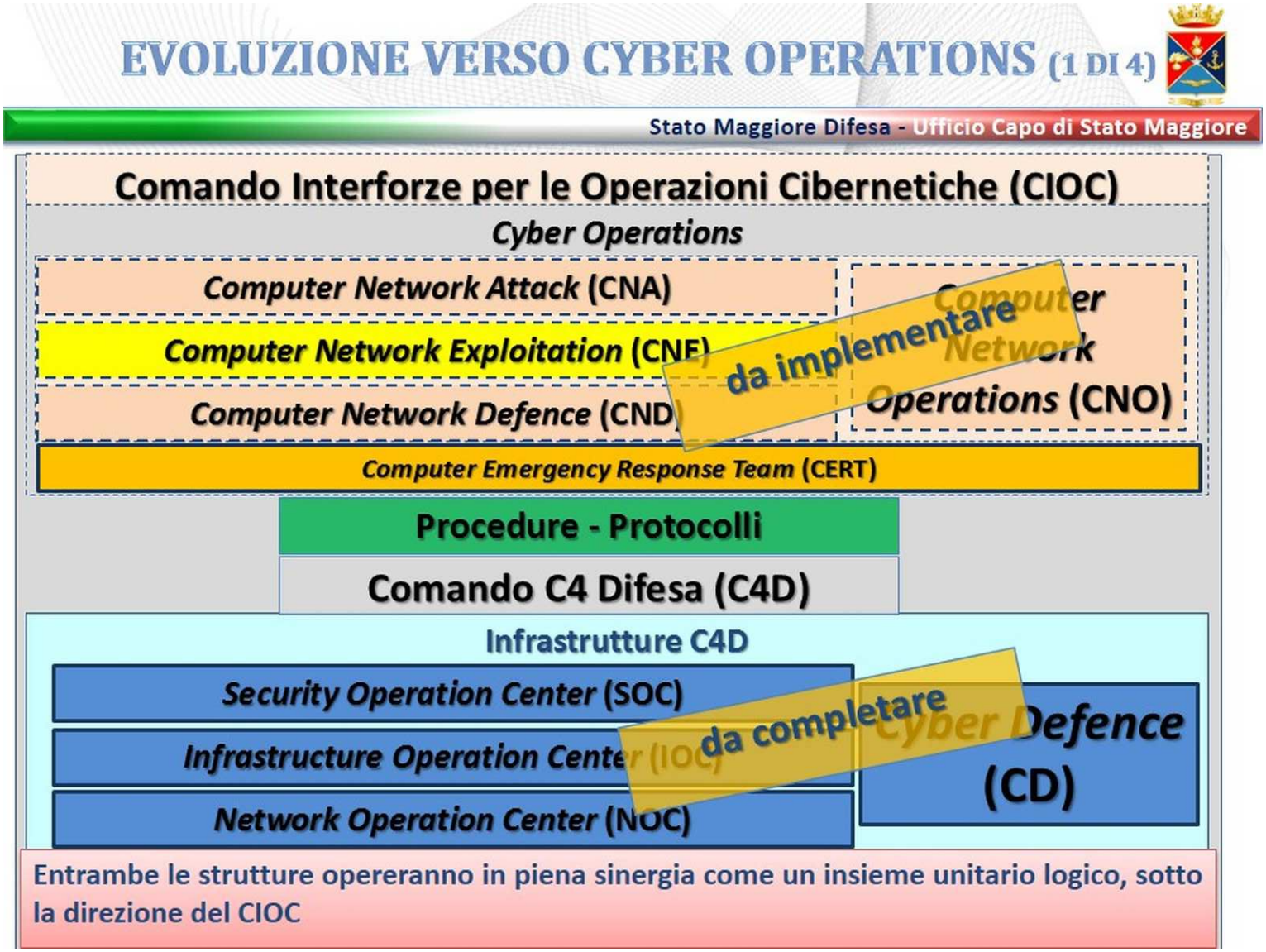
Stato Maggiore Difesa - Ufficio Capo di Stato Maggiore

DPCM 27 GENNAIO 2014

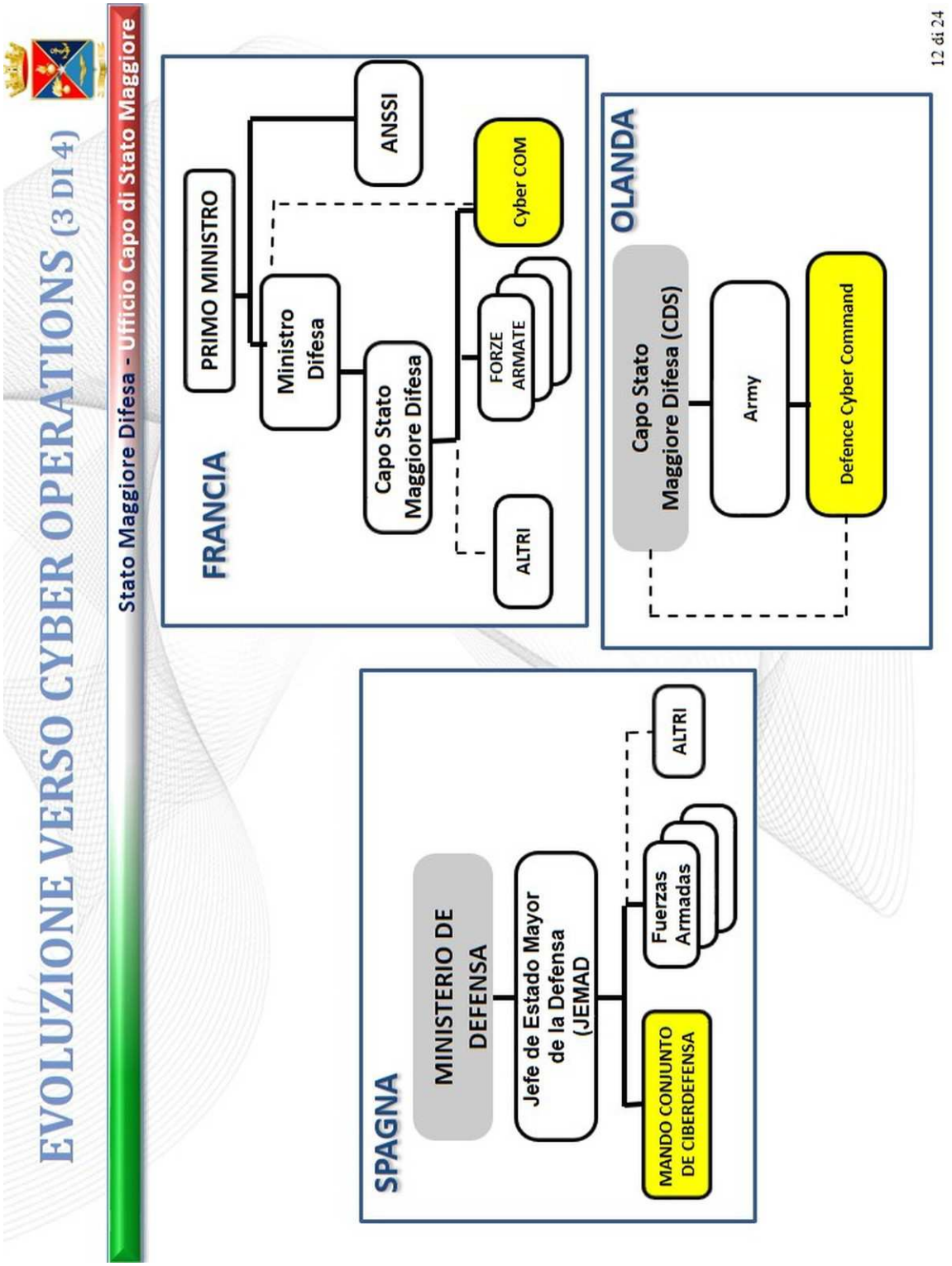
STRATEGIA NAZIONALE PER LA SICUREZZA CIBERNETICA


ATTUALE CAPACITÀ CYBER DEFENCE (1 DI 2)
Stato Maggiore Difesa - Ufficio Capo di Stato Maggiore
STRUTTURA del CERT DIFESA
SMD VI Reparto
C4I e Trasformazione
SMD II Reparto
Informazioni e Sicurezza
CERT Difesa
Technical Centre
CERT Difesa
Coordination Centre
NATO CIRC
CERT PA
Industria
Università
Fonti Aperte
CERT
Carabinieri
CERT
AM
CERT
MM
CERT
EI
8 di 24

ATTUALE CAPACITÀ CYBER DEFENCE (2 DI 2)
Stato Maggiore Difesa - Ufficio Capo di Stato Maggiore
Comando Interforze per le Operazioni Cibernetiche (CIOC)
Cyber Operations
WORK IN PROGRESS
Computer Emergency Response Team (CERT)
Procedure - Protocolli
Comando C4 Difesa (C4D)
Infrastrutture C4D
Security Operation Center (SOC)
Infrastructure Operation Center (IOC)
Network Operation Center (NOC)
da completare
Defence
(CD)

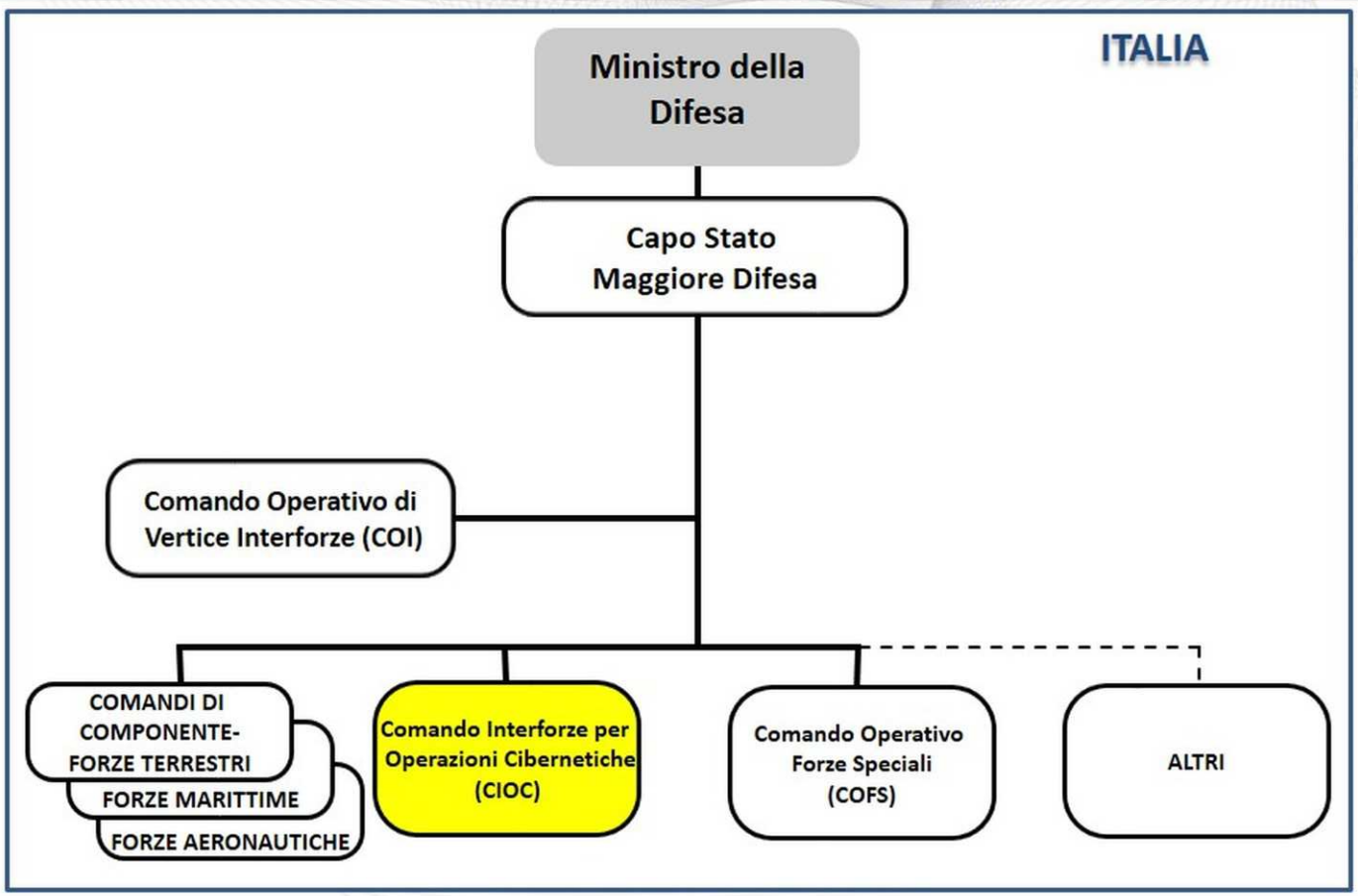

EVOLUZIONE VERSO CYBER OPERATIONS (1 DI 4)
Stato Maggiore Difesa - Ufficio Capo di Stato Maggiore
Comando Interforze per le Operazioni Cibernetiche (CIOC)
Cyber Operations
Computer Network Attack (CNA)
Computer Network Exploitation (CNE)
Computer Network Defence (CND)
Computer Network Operations (CNO)
da implementare
Computer Emergency Response Team (CERT)
Procedure - Protocolli
Comando C4 Difesa (C4D)
Infrastrutture C4D
Security Operation Center (SOC)
Infrastructure Operation Center (IOC)
Network Operation Center (NOC)
da completare
Cyber Defence (CD)
Entrambe le strutture opereranno in piena sinergia come un insieme unitario logico, sotto la direzione del CIOC

EVOLUZIONE VERSO CYBER OPERATIONS (2 DI 4)
Stato Maggiore Difesa - Ufficio Capo di Stato Maggiore
STATI UNITI
PRESIDENTE
SEGRETARIO DI STATO
GENERAL CHIEF OF STAFF
USSTRATCOM
USCYBERCOM
DIR NSA/ CHCSS
REGNO UNITO
PRIMO MINISTRO
Office of Cyber Security & Infoassurance
Segretario di Stato per gli Esteri e gli affari del Commonwealth
Government Communications Headquarter (GCHQ)
MOD
Joint Cyber Unit JCU
11 di 24


EVOLUZIONE VERSO CYBER OPERATIONS (3 DI 4)
Stato Maggiore Difesa - Ufficio Capo di Stato Maggiore
12 di 24
FRANCIA
PRIMO MINISTRO
Ministro Difesa
ANSSI
Capo Stato Maggiore Difesa
Cyber COM
FORZE ARMATE
ALTRI
OLANDA
Capo Stato Maggiore Difesa (CDS)
Army
Defence Cyber Command
SPAGNA
MINISTERIO DE DEFENSA
Jefe de Estado Mayor de la Defensa (JEMAD
Fuerzas Armadas
ALTRI
MANDO CONJUNTO DE CIBERDEFENSA

EVOLUZIONE VERSO CYBER OPERATIONS (4 DI 4)

Stato Maggiore Difesa - Ufficio Capo di Stato Maggiore



13 di 24

IL PROGETTO CIOC (1 DI 4)

Stato Maggiore Difesa - Ufficio Capo di Stato Maggiore

Lo "spazio cibernetico" è un dominio artificiale (anche detto quinta dimensione) che pervade gli altri 4 domini tradizionali (Terrestre, Marittimo, Aereo, Spaziale).

Caratterizzato da:

- **Mancanza di geo-specificità;**
- **Limitate capacità di attribuzione.**

Richiede un quadro dottrinale chiaro e proceduralmente normato per operare anche in contesti interconnessi e/o federati.


IL PROGETTO CIOC (2 DI 4)
Stato Maggiore Difesa - Ufficio Capo di Stato Maggiore
15 di 24
COC
CIOC

IL PROGETTO CIOC (3 DI 4)

Stato Maggiore Difesa - Ufficio Capo di Stato Maggiore

Organizzazione

IL PROGETTO CIOC (3 DI 4)

Stato Maggiore Difesa - Ufficio Capo di Stato Maggiore

Organizzazione

Info/Infrastrutture

IL PROGETTO CIOC (3 DI 4)

Stato Maggiore Difesa - Ufficio Capo di Stato Maggiore

Organizzazione

Info/Infrastrutture

Cyber Lab

Cyber Range

IL PROGETTO CIOC (3 DI 4)
Stato Maggiore Difesa - Ufficio Capo di Stato Maggiore
Organizzazione
CIOC
Area Capacitiva
Area Operativa
PERSONALE
LOGISTICA
DOTTRINA
OPERAZIONI
PIANIFICAZIONI
ADDESTRAMENTO
ASSETTI
CYBER OPERATIONS
COC
Combat Service Support
Combat Support
SALA OPERATIVA 24/7
CONSULENZA LEGALE
PUBBLICA INFORMAZIONE
COORDINAMENTO
Info/Infrastrutture
Personale
WATCH OUT. HACKERS!
NATO CYBER DEFENCE
Cyber Lab
Cyber Range
CYBER ATTACK
19 di 24

IL PROGETTO CIOC (4 DI 4)

Stato Maggiore Difesa - Ufficio Capo di Stato Maggiore

Programmi per l'operatività del CIOC con risorse dedicate:

- ✓ Info-Infrastruttura del CIOC
- ✓ Potenziamento protezione info-dominio A.D.
- ✓ Assetti per la pianificazione e gestione delle operazioni *cyber*
- ✓ *Cyber Operational Picture* (CyOP)
- ✓ *Cyber Range e Cyber Lab*
- ✓ ...

CONSIDERAZIONI FINALI (1 DI 3)

Stato Maggiore Difesa - Ufficio Capo di Stato Maggiore

- ✓ La minaccia cibernetica è concreta e reale, esiste già da tempo, e si sta sempre più evolvendo (virus Stuxnet, Anonymous, etc.);

- ✓ Le unità della Difesa operano in scenari ed ambienti sempre più digitalizzati, nei quali la minaccia cibernetica sarà sempre più presente;

- ✓ **Implementazione** del Comando Interforze per le Operazioni Cibernetiche (**CIOC**), progetto prioritario per la Difesa;

CYBER COMMAND

CONSIDERAZIONI FINALI (2 DI 3)

- ✓ **Impegni Difesa**, in linea con gli **obiettivi** definiti in ambito Nazionale, **Europeo** (Direttiva NIS) e **NATO** (*Cyber Defence Pledge);*

- ✓ **Summit Varsavia**: *"…, attraverso la nostra promessa di rafforzare la Cyber Defence, ci siamo impegnati a far evolvere la difesa cibernetica delle nostre infrastrutture e dei nostri network nazionali, come importanza prioritaria. Ogni Alleato onorerà la propria responsabilità nel migliorare la resilienza ed abilità a rispondere rapidamente ed efficacemente ad attacchi cyber, includendo anche contesti ibridi…"*;

- ✓ Orientamento NATO verso il criterio del ***"No Compliance… No Partecipation"***.

CONSIDERAZIONI FINALI (3 DI 3)

Stato Maggiore Difesa - Ufficio Capo di Stato Maggiore

La Difesa, nell'ambito delle capacità cyber che sta generando sia per proteggere i suoi sistemi sia per pianificare e condurre operazioni militari nel dominio cyber, in linea con il quadro normativo vigente, è, come di consueto, a disposizione del Paese, pronta a rendere disponibili in ogni momento le proprie capacità attuali e quelle future nel campo della Cyber Security per concorrere alla crescita della capacità cibernetica della Nazione.


STATO MAGGIORE DELLA DIFESA
Stato Maggiore Difesa - Ufficio Capo di Stato Maggiore
"La Difesa e il mondo della Cyber Security"
Audizione da parte della 4ª Commissione Difesa
Roma, 25 gennaio 2017
Generale Claudio GRAZIANO
Capo di Stato Maggiore della Difesa
24 di 24