

**COMMISSIONE IV
DIFESA**

RESOCONTO STENOGRAFICO

INDAGINE CONOSCITIVA

4.

SEDUTA DI MARTEDÌ 9 MARZO 2016

PRESIDENZA DEL PRESIDENTE **FRANCESCO SAVERIO GAROFANI**

INDICE

	PAG.		PAG.
Sulla pubblicità dei lavori:		Audizione del Comandante del Centro <i>Intelligence</i> interforze, Generale di brigata aerea Giandomenico Taricco:	
Garofani Francesco Saverio, <i>Presidente</i> ...	3	Garofani Francesco Saverio, <i>Presidente</i> .	16, 19, 22 24, 25, 26, 28
INDAGINE CONOSCITIVA SULLA SICUREZZA E LA DIFESA NELLO SPAZIO CIBERNETICO		Artini Massimo (Misto AL-P)	24, 25
Audizione del Capo del VI Reparto (Sistemi C4I e Trasformazione) dello Stato maggiore della Difesa, Ammiraglio di divisione Ruggero Di Biase:		Boldrini Paola (PD)	25
Garofani Francesco Saverio, <i>Presidente</i> .	3, 13, 14, 16	Taricco Giandomenico, <i>Comandante del Centro Intelligence interforze</i>	16, 19, 24, 26
Artini Massimo (Misto AL-P)	13	ALLEGATI:	
Di Biase Ruggero, <i>Capo del VI Reparto (Sistemi C4I e Trasformazione) dello Stato maggiore della Difesa</i>	3, 13, 14	<i>Allegato 1:</i> Presentazione dell'Ammiraglio Di Biase: Capacità di cyber defence della Difesa	29
		<i>Allegato 2:</i> Presentazione del Generale Taricco: Dominio cibernetico: prospettive per lo strumento militare	57

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-UDC): (AP); Sinistra Italiana-Sinistra Ecologia Libertà: SI-SEL; Scelta Civica per l'Italia: (SCPl); Lega Nord e Autonomie - Lega dei Popoli - Noi con Salvini: (LNA); Democrazia Solidale-Centro Democratico (DeS-CD); Fratelli d'Italia-Alleanza Nazionale: (FdI-AN); Misto: Misto; Misto-Alleanza Liberalpopolare Autonomie ALA-MAIE-Movimento Associativo Italiani all'Estero: Misto-ALA-MAIE; 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 (Unione Sudamericana Emigrati Italiani): Misto-USEI.

PAGINA BIANCA

PRESIDENZA DEL PRESIDENTE
FRANCESCO SAVERIO GAROFANI

La seduta comincia alle 14.10.

Sulla pubblicità dei lavori.

PRESIDENTE. Avverto che la pubblicità dei lavori della seduta odierna sarà assicurata anche attraverso l'attivazione di impianti audiovisivi a circuito chiuso e la trasmissione televisiva sul canale satellitare della Camera dei deputati.

Audizione del Capo del VI Reparto (Sistemi C4I e Trasformazione) dello Stato maggiore della Difesa, Ammiraglio di divisione Ruggero Di Biase.

PRESIDENTE. L'ordine del giorno reca, nell'ambito dell'indagine conoscitiva sulla sicurezza e la difesa nello spazio cibernetico, l'audizione del Capo del VI Reparto (Sistemi C4I e Trasformazione) dello Stato maggiore della Difesa, Ammiraglio di divisione Ruggero Di Biase.

Saluto e ringrazio l'Ammiraglio per essere qui presente e do il benvenuto anche al Generale Taricco, che sarà protagonista dell'audizione che seguirà. Ricordo che dopo l'intervento introduttivo dell'Ammiraglio darò la parola, come di consueto, ai colleghi che volessero proporre domande od osservazioni. Poi l'Ammiraglio sarà tanto cortese da replicare.

Prego, Ammiraglio.

RUGGERO DI BIASE, *Capo del VI Reparto (Sistemi C4I e Trasformazione) dello Stato maggiore della Difesa*. Grazie, signor presidente e onorevoli. Intanto vor-

rei esprimere l'onore di essere qui davanti a questa Commissione per poter illustrare quali sono le attuali capacità che il comparto Difesa ha acquisito nella settore della *cyber defence* e della sua organizzazione.

Ho voluto strutturare l'agenda nel seguente modo.

All'inizio farei un cenno al quadro normativo di riferimento e alla struttura nazionale preposta alla difesa cibernetica per il nostro Paese, per poi evidenziare come l'organizzazione della Difesa si inserisce in tale struttura nazionale.

Passerei, quindi, alle attività finalizzate allo sviluppo della capacità di *cyber defence* del comparto Difesa, accennando in particolare al programma cardine — che noi denominiamo programma *Cyber Defence Capability* — per dare anche un'idea di attività che, ancorché complementari, sono fondamentali per garantire la crescita capacitiva in questo delicato e nuovo settore.

Concluderei poi con un'idea su un altro progetto, altrettanto importante. Non è un progetto della Difesa, ma interministeriale, tuttavia alla Difesa è stato affidato il compito di progettare una Rete interministeriale di gestione delle crisi cibernetiche. Ci siamo presi ben volentieri questo *task* e stiamo affrontando la progettazione.

Passando al quadro normativo di riferimento, l'atto di riferimento è rappresentato dal decreto del Presidente del Consiglio dei ministri del 24 gennaio 2013, che costituisce la direttiva recante « Indirizzi per la protezione cibernetica e la sicurezza informatica nazionale ». Da questo atto è disceso il Quadro strategico nazionale, redatto sempre in un'ottica interministeriale, a guida della Presidenza del Consiglio dei ministri. Tale documento stabilisce di fatto

la *vision* e gli obiettivi strategici che si intendono conseguire in questo settore specifico.

A discendere, è stato redatto il Piano nazionale per la protezione cibernetica e per la sicurezza informatica, che stabilisce le aree su cui in particolare occorre focalizzare l'impegno per garantire non solo una crescita capacitativa, ma — aggiungo io — anche una crescita culturale e soprattutto su cui costruire quelle sinergie fra le Istituzioni e la pubblica amministrazione preposte a condurre quest'attività con il settore privato, l'industria privata, i *provider* che operano nel settore dell'*Information and Communication Technology* e il mondo accademico, in maniera tale che la risposta nazionale possa essere costruita per rispondere in maniera efficace ed efficiente all'esigenza.

Passando alla struttura nazionale preposta alla difesa cibernetica, sul piano organizzativo-funzionale possiamo dividerla in tre livelli. Il primo livello è quello politico-strategico, che si incentra sulla Presidenza del Consiglio dei ministri, alle cui dipendenze c'è il Comitato interministeriale per la sicurezza della Repubblica e che si avvale del Nucleo interministeriale di situazione e pianificazione (NISP). Quest'organismo in particolare è preposto alla gestione e, quindi, al coordinamento di qualsiasi situazione di crisi nazionale.

Al di sotto del livello politico-strategico si inserisce il livello di supporto operativo. Questo livello è incentrato sul Nucleo di sicurezza cibernetico, che è stato creato di recente con il citato decreto del Presidente del Consiglio dei ministri 24 gennaio 2013. Il nucleo ha funzioni di coordinamento e di scambio informativo, sempre in un'ottica interministeriale, ed è preposto a gestire situazioni di crisi precipue nel settore della *cyber defence*. Una volta che ci si ritrova in una situazione di crisi, ovviamente si attiva anche il NISP, il livello superiore.

Il Nucleo di sicurezza cibernetica ha dei forti legami con il Dipartimento delle informazioni per la sicurezza, che rappresenta l'organo collegiale che a tutto tondo si occupa di *intelligence* e di sicurezza nel

nostro Paese. Essi adottano uno scambio continuo di informazioni e un'attività di coordinamento per gestire insieme situazioni di crisi nel settore cibernetico.

A *latere* c'è un organo consultivo di natura tecnico-scientifica che offre la propria attività di consulenza alle due strutture che costituiscono il livello di supporto operativo.

In seno al Nucleo di sicurezza cibernetica è stato istituito un Tavolo interministeriale per le crisi cibernetiche. Si tratta di un organo di raccordo, che ha funzione di collante di tutta l'attività che il livello tecnico-operativo svolge.

Tale livello si basa sui *Computer Emergency Response Team* (CERT) che ogni singolo Dicastero si è ritagliato. Il principale di tali centri è quello nazionale, che è stato realizzato in seno al Ministero dello sviluppo economico. Esso ha, in particolare, funzioni di coordinamento verso i *provider* che operano nel settore ICT, verso l'industria nazionale e verso le Istituzioni preposte a tutelare le infrastrutture critiche della nazione. Il CERT della Pubblica amministrazione è preposto a tutelare la sicurezza delle infrastrutture dei Dicasteri e, quindi, delle Istituzioni dello Stato ed è realizzato insieme all'Agencia per l'Italia digitale.

La Difesa si è realizzata il proprio CERT e, quindi, apporta il suo contributo non solo informativo, ma anche consuntivo laddove necessario, in un'ottica sempre interministeriale, in maniera tale da contribuire in caso di situazioni di emergenza e di crisi cibernetica.

Passerei adesso a illustrare l'organizzazione del CERT Difesa. Quest'organismo si articola su due pilastri fondamentali. Il primo è denominato CERT *Coordination Center* ed è realizzato in seno al II Reparto dello Stato maggiore della Difesa, il Reparto informazioni e sicurezza, mentre la componente tecnico-operativa, che prende il nome di CERT *Technical Center*, è realizzata in seno al Comando C4 Difesa, dipendente dal VI Reparto dello Stato maggiore della Difesa. Il Comando C4 Difesa in particolare è l'organo preposto alla gestione tecnico-operativa di tutti gli

assetto e di tutti i sistemi di *Information and Communication Technology* del comparto Difesa e, quindi, del Dipartimento.

Queste due anime insieme svolgono attività di indirizzo, coordinamento e informazione verso gli analoghi organi costituiti presso le Forze armate. Ogni singola Forza armata si è realizzata il suo CERT. Noi operiamo in maniera coordinata con la funzione del CERT interforze, sovrapposto agli altri non in termini organici, ma funzionali. Infatti, in caso di situazioni di crisi, il CERT Difesa assume il coordinamento delle attività da porre in essere.

Più in particolare, il compito del CERT Difesa è quello di prevenire la minaccia cibernetica, rilevare le attività di natura malevola e reagire agli incidenti informatici. Più nello specifico, il CERT *Coordination Center* svolge attività di informazione e di allertamento anche a scopo di prevenzione e collabora e condivide informazioni con i corrispondenti CERT nazionali e internazionali.

In particolare, il CERT internazionale con cui ci relazioniamo è quello della NATO, che va sotto il nome di *NATO Computer Incident Response Capability* (NCIRC). L'ultima funzione è quella di supportare il CERT *Technical Center* con attività di analisi in caso di evento cibernetico.

Il CERT *Technical Center* è, invece, preposto a prevenire, rilevare e contenere sul piano tecnico-operativo gli incidenti informatici. Tale centro, peraltro, coordina e supporta l'azione dei CERT di Forza armata in caso di emergenza cibernetica.

Ho parlato del CERT Difesa e ho detto che si configura nell'organizzazione del Comando C4 Difesa. È il nostro organo, se vogliamo, tecnico-operativo nella condotta e gestione quotidiana di tutti gli assetti di *Information and Communication Technology* ed è configurato all'interno di questo comando.

Questo comando in particolare articola le sue funzioni su tre pilastri fondamentali. Uno è l'area del *networking*, ossia l'area gestionale dell'intera infrastruttura di rete. Nell'area del *networking* opera il

Network Operation Center. Un'altra area fondamentale è quella dei servizi informativi, sia di natura gestionale, sia di natura operativa, ovvero la gestione dei *data center* che ospitano questi servizi, che attraverso il sistema di *networking* della rete vengono erogati agli utenti. Il tutto avviene in una cornice di sicurezza atta a garantire l'applicazione delle *policy* di settore in materia di sicurezza e a dare attuazione a quelle misure cosiddette di *information assurance* e *cyber defence*.

In particolare, in quest'area opera il *Security Operation Center* (SOC), che è preposto a garantire servizi di sicurezza finalizzati alla protezione dell'infrastruttura ICT del comparto e a rilevare ogni forma di anomalia di natura di sicurezza su tale infrastruttura. In quest'area si colloca il CERT TC, che garantisce i servizi di sicurezza finalizzati alla prevenzione, alla reazione e al contenimento di incidenti informatici.

Passerei adesso al quadro capacitivo, a che cosa la Difesa ha già di fatto conseguito in termini capacitivi e a che cosa sta pianificando come ulteriore crescita capacitiva. Il programma cardine è quello che ho già menzionato nell'elencare i punti dell'agenda, cioè il programma cosiddetto *Cyber Defence Capability*.

Innanzitutto, disporre di capacità di *cyber defence* significa essere in grado di espletare funzioni a tutto tondo di prevenzione e di protezione della propria infrastruttura. Si tratta di proteggerla e prevenire incidenti informatici, di essere in grado di rilevare situazioni in cui l'attività malevola ha avuto effetto e, quindi, è riuscita a penetrare nella propria infrastruttura, di disporre di strumenti di analisi per comprendere la complessità dell'evento e la tipologia dei *malware* e, quindi, di riuscire a reagire e a contrastare la minaccia. Se, conseguentemente, quest'attività malevola ha avuto effetti dannosi sull'infrastruttura, occorre avere la capacità di ripristinare prontamente la stessa, in modo tale che possa continuare a erogare i servizi istituzionali.

Lo scopo di questo programma è proprio quello di accrescere le capacità del

CERT TC e di proteggere le infrastrutture ICT della Difesa. Sto parlando di un dominio non classificato, cioè della porzione di rete aperta alla rete pubblica e a Internet.

Che cosa significa proteggere da attività di natura malevola? Significa proteggere da tutte quelle attività mirate a sottrarre informazioni e dati, a compromettere la loro integrità o addirittura a negare i servizi in rete.

Come vogliamo accrescere queste capacità? Attraverso l'acquisizione di strumenti idonei per prevenire, proteggere, rilevare, condurre analisi, reagire a eventi cibernetici ed essere in grado di ripristinare i servizi a seguito di incidente informatico. Questo è lo scopo principale del programma cardine della Difesa già avviato.

Ci tengo a sottolineare che il modello capacitivo a cui ci siamo riferiti e, quindi, il nostro requisito operativo, si è basato su un *framework* capacitivo che la NATO ha già adottato per costruire la propria capacità di *cyber defence*, ossia il NATO *Computer Incident Response Capability* (NCIRC), come ho prima accennato. Questo è il nostro modello di base. Non abbiamo inventato nulla, non ci siamo mossi in maniera autonoma, bensì abbiamo adottato un modello già validato nel contesto dell'Alleanza e ben provato. Questo è diventato il modello di riferimento per definire il nostro requisito operativo posto a base di questo programma.

Passiamo adesso allo sviluppo temporale del programma. Per ovvi motivi di natura finanziaria non abbiamo potuto imbastire il programma in un'unica soluzione e abbiamo preferito dividerlo in due fasi. Una prima fase, cosiddetta *Cyber Defence Capability* fase 1, è mirata alla realizzazione di una Capacità operativa iniziale (IOC), per poi, con un approccio a spirale incrementale, costruire sulle capacità iniziali e, quindi, portare a finalizzazione questa capacità con una seconda fase, la cosiddetta *Cyber Defence Capability* fase 2, mirata a conseguire la Capacità operativa finale (FOC).

Il requisito è stato redatto nel 2011 e nello stesso anno è stato portato a contrattualizzazione. All'inizio del 2012 è stata avviata la fase di realizzazione di questa Capacità operativa iniziale, che è stata poi conseguita, nel rispetto della tempistica, nel 2013. Il programma sarebbe dovuto poi proseguire con l'avvio della seconda fase nel 2014 per conseguire la Capacità finale nel 2016. Va da sé che queste capacità non si fermano, non hanno un capolinea, ma vanno fatte evolvere e vanno potenziate in relazione all'evoluzione della minaccia. Questo comunque sarebbe un processo continuo e continuativo.

Dove siamo oggi? La fase 1, come ho detto, si è conclusa nei tempi previsti e ha mirato a soddisfare i requisiti minimi basilari per consentire - io dico - una sufficiente, ma in termini anche significativi, capacità di *cyber defence*. Nel contesto è stata creata anche una *control room* presso il Comando C4 Difesa, nell'infrastruttura di sicurezza del Comando C4 Difesa, operante tutti i giorni, 24 ore su 24, con una capacità di fusione di tutti i dati provenienti dalle sonde che operano sull'infrastruttura di rete. Se mi consentite, parlerei anche un po' con termini tecnici: si tratta di sonde di *intrusion detection* e di *intrusion prevention*, di strumenti di capacità di analisi del traffico e, quindi, dei pacchetti *Internet Protocol* che transitano sulla rete.

Tutte queste informazioni poi, attraverso vari strumenti, vengono correlate in maniera tale da presentare la cosiddetta *Cyber Operational Picture*, sulla base della quale poi si prendono le decisioni e si decide di attuare le misure di contrasto alla minaccia da parte del personale preposto. In un certo senso aiuta la funzione di comando e controllo anche in questo settore.

La fase 2 avrebbe dovuto partire nell'esercizio finanziario 2014, ma, per il quadro finanziario non favorevole, purtroppo non è stato possibile avviarla nei termini stabiliti. Tuttavia, per non fermare la macchina, che nel frattempo era partita, e quindi per non fermare il processo di

crescita e di realizzazione di questa capacità - con una certa lungimiranza, devo dire - i vertici militari hanno comunque garantito un finanziamento, ancorché parziale, ma significativo, che ha consentito di continuare l'impresa con una fase cosiddetta di evoluzione, mirata soprattutto a consolidare le capacità acquisite.

Le licenze, le *appliance* vanno rinnovate e questo è un costo. Se non si vuole tornare indietro, bisogna rinnovare quanto già acquisito. Comunque, attraverso questo ulteriore minimo finanziamento, si è riusciti anche a potenziare e adeguare tecnologicamente lo strumento già acquisito e a renderlo più idoneo alla minaccia che nel frattempo evolve.

È interessante, poi, confrontare col *framework* capacitivo NATO del NCIRC le capacità che oggi abbiamo già acquisito attraverso la fase 1 del programma e la fase di evoluzione successiva. Nella *slide* denominata «Programma Cyber Defence Capability - Situazione attuale (CDC 1 + CDC EVO)» ciò che è indicato in verde è tutto quello che abbiamo conseguito totalmente. Ciò che è indicato in marrone chiaro è quello che abbiamo conseguito parzialmente, ma sottolineo comunque in maniera adeguata e sufficiente per garantire un determinato livello di risposta alla minaccia cibernetica.

In attesa di poter avviare l'importante fase 2 del programma, abbiamo dunque fatto tesoro dell'esperienza che abbiamo nel frattempo maturato con il nostro personale e con la nostra organizzazione per tener conto dell'evoluzione della minaccia - forse, poi, il Generale Taricco esplicherà tale aspetto molto meglio di me - sempre più persistente, sofisticata e complessa.

Abbiamo approfittato, quindi, di questo stallo del programma per poter riprogettare la fase 2, rivederne per bene il requisito e far sì che fosse allineato alle nuove forme di minaccia e alla nuova complessità della minaccia. Il nuovo requisito è in via di finalizzazione. Saremo pronti a breve ad avviare l'impresa. L'impresa è posta in alta priorità. È in attesa di finanziamento, ma è certamente una

delle imprese a più alta priorità nell'ambito della pianificazione dello Stato maggiore della Difesa.

Se riusciamo a partire quest'anno con un finanziamento spalmato su di un triennio, dovremmo essere in grado a fine 2018 di conseguire la *Final Operational Capability* di questa capacità di cui ci auspichiamo che il comparto Difesa possa disporre così come è stata pianificata.

In sintesi, quali sono gli obiettivi che la Difesa intende conseguire con la seconda fase di questo programma? Ovviamente, il consolidamento del livello di operatività già acquisito, un ulteriore adeguamento dell'attuale infrastruttura di protezione al crescente livello della minaccia - questo significa potenziare e adeguare sul piano tecnologico gli strumenti e i sistemi di prevenzione, protezione e rilevazione degli eventi - un'analisi che sarà fondamentale per cercare di capire la tipologia e la complessità dei *malware* e capacità di reazione e di *recovery* dall'infrazione nel caso in cui l'incidente abbia avuto i suoi effetti.

Contestualmente, sempre nell'ottica del risparmio, questa volta con riferimento a risparmio sull'esercizio e sul funzionamento nel tempo, abbiamo visto che crescendo e, quindi, aggiungendo sistemi, molto spesso questi ultimi espletano funzioni che si sovrappongono. Vorremmo anche condurre una razionalizzazione di tutto ciò che è stato realizzato, in maniera tale da evitare sovrapposizioni di funzioni e, quindi, risparmiare nell'esercizio. Questi strumenti vanno rinnovati in termini di licenza e vanno tenuti aggiornati sul piano tecnologico. La razionalizzazione deve portare un risparmio sul funzionamento nel tempo.

Abbiamo voluto inserire in questa impresa anche un'ulteriore attività, che mira a irrobustire ulteriormente la protezione di natura *cyber* nel dominio classificato. Per dominio classificato intendo le reti classificate, che per la Difesa sono reti chiuse, ma la minaccia è anche interna. Pertanto, la capacità di *cyber defence* serve sicuramente a proteggere l'infrastruttura dall'interno.

La complessità degli attuali *malware* è tale da operare anche in modalità *air-gap*. Se uno per sbaglio usa un dispositivo come una penna su una macchina di un dominio classificato — non dovrebbe farlo, ma se inavvertitamente lo facesse — può portarsi dei virus che operano in maniera *air-gap*. Si inseriscono, cioè, nel dominio classificato e poi, attraverso l'inserimento di un'ulteriore chiavetta, senza che l'utente se ne accorga, caricano su questo supporto informazioni classificate all'insaputa dell'utente che riporta la chiavetta in un dominio non classificato, aperto alla rete pubblica. Automaticamente, attraverso dei *link* di comando e controllo, questi dati verrebbero esfiltrati.

In questo dominio noi attuiamo tutte le *best practice* del caso e preveniamo questa tipologia di incidente con strette misure di sicurezza. Questo per dire che la minaccia cibernetica è talmente complessa che addirittura c'è la possibilità, attraverso *malware* che operano in modalità *air-gap*, di violare anche eventualmente i domini classificati. Non è il nostro caso, perché conosciamo bene l'argomento. Sappiamo esattamente quali sono le stringenti misure da adottare in questo dominio e ci comportiamo di conseguenza.

Abbiamo approfittato di questa impresa anche per portare avanti un progetto fondamentale. Anche qui stiamo in un certo senso copiando la NATO. La NATO sta lanciando nel nuovo *headquarter* la cosiddetta *Business One*. Che cosa è la *Business One*? L'Ottanta per cento delle informazioni classificate è di natura riservata. Anziché andare ad appesantire e creare maggiori problematiche al dominio classificato, si sta cercando di fare in modo di trattare informazioni anche di natura classificata, solo fino a « riservato », ossia al primo gradino delle classifiche di segretezza, sull'infrastruttura di Intranet aperta alla rete pubblica. Ciò con opportune compartimentazioni e misure di sicurezza che consentano di separare l'informazione classificata fino al livello « segreto » dall'informazione non classificata. Questo agevola di fatto l'attività lavorativa.

In estrema sintesi, gli obiettivi della *Cyber Defence Capability* fase 2 del programma sono quelli di consolidare le capacità già acquisite e di continuare nell'auspicato processo di crescita capacitiva.

Sempre con riferimento al *framework* capacitivo NATO, alla fine del programma di fatto andremo a realizzare molte delle capacità che la NATO ha già realizzato. Una minima parte rimane realizzata non in maniera totale, ma per noi sufficiente. Abbiamo tenuto fuori le attività relative a una *active cyber defence*, di natura un po' più offensiva, perché tutto questo farà parte di altri processi di crescita costruttiva che vedrete con il Generale Taricco. Ripeto, quello che si andrà a realizzare — il famoso comando *cyber* della Difesa, che dovrà poi condurre operazioni a tutto tondo di *network operation* — si dovrà dotare anche di strumenti che consentano di espletare funzioni di natura più attiva, più di *exploitation*. Pertanto, la parte *cyber defence* ha un po' trascurato questa componente capacitiva.

Volevo anche portare all'attenzione di questa onorevole Commissione quanto abbiamo già investito nel settore della *cyber defence* per acquisire le capacità e quanto è in pianificazione per arrivare al traguardo che ci siamo prefissati. La prima fase, quella con cui abbiamo realizzato la Capacità operativa iniziale, ci ha già impegnati per 4 milioni di euro sui capitoli di ammodernamento e di rinnovamento (A.R.), quindi sulla parte del bilancio relativa all'investimento. Con la fase intermedia di *evolution* abbiamo investito ulteriori 1,2 milioni di euro, sempre sui capitoli di A.R. Sulla parte dell'esercizio invece, attraverso una manutenzione di natura evolutiva, abbiamo voluto adeguare tecnologicamente i sistemi di protezione e, quindi, abbiamo investito altri 1,7 milioni di euro.

Abbiamo in programma per la fase 2 quattordici milioni di euro, sempre sui capitoli di investimento, con un profilo pluriennale per il triennio 2016-2018. Ripeto che si tratta di un'impresa ad alta

priorità. È in attesa di finanziamento, ma è una delle imprese a più alta priorità nell'ambito del comparto.

Dotarsi degli appropriati strumenti è certamente un processo ineludibile e fondamentale, ma lo strumento da solo, per quanto complesso e sofisticato possa essere, ha bisogno della risorsa umana e, quindi, bisogna investire anche sulla risorsa umana. È il binomio strumento-risorsa umana che di fatto costituisce la capacità di *cyber defence*.

La Difesa si è posta questo obiettivo e sta perseguendo la crescita sul piano quantitativo e qualitativo degli organici delle articolazioni preposte all'attività di *cyber defence* nell'ambito del comparto, e lo sta facendo attraverso un processo interno di selezione e formazione del personale, sia militare, sia civile, da qualificare sulla base dei nuovi profili di impiego e *iter* formativi. È già stata svolta una — credo meritoria — attività in tal senso. Abbiamo definito completamente i nuovi profili funzionali di impiego e abbiamo ridefinito tutti gli *iter* formativi.

Disponiamo di due istituti di formazione. Il primo è la Scuola delle telecomunicazioni interforze di Chiavari; l'altro è il CIFI/GE presso il Centro *intelligence* interforze. Questi due organismi formano il nostro personale specialistico.

Un'altra attività fondamentale è l'assunzione diretta di personale civile e militare con appropriate qualificazioni. Non si tratta di prendere del semplice personale, ma di cercare di reclutare personale già in possesso di esperienza pregressa in questo settore e, quindi, già in possesso di una formazione di un determinato livello. Per talune figure specialistiche — ce ne sono tante; ne cito solo qualcuna: per esempio *forensic analyst*, *vulnerability evaluator*, *risk manager*, *penetration tester* — stiamo cercando di conseguire certificazioni specialistiche, sia *in-house*, sia attraverso corsi specialistici offerti da organizzazioni ben presenti nel settore, che sono di riferimento per noi.

Adesso passerei a quell'attività che inizialmente ho definito complementare, ma che è altrettanto importante per conse-

guire la crescita capacitiva nel settore della *cyber*, che è il nostro obiettivo. Uno di questi progetti è *Autonomous System Internet Provider Independent*. Sono parole strane, ma adesso cercherò di spiegarmi meglio e di farvi comprendere di che cosa si tratta.

Per fare questo vorrei innanzitutto darvi un'idea dell'architettura della rete Difesa e di come la stessa sia connessa a Internet. Quando si parla di un'infrastruttura di rete sul piano concettuale, questa si può suddividere in due componenti: la componente fisica, ossia il *networking*, il supporto trasmissivo, la rete fisica e, ovviamente, la componente logica. Stiamo parlando di reti che adottano protocolli IP, a cui tutti ormai siamo abituati.

La componente logica è la componente che consente l'accesso del traffico in rete, la distribuzione del traffico in rete e il *routing* del traffico in rete. Quindi, abbiamo componente logica più componente fisica. Su questa componente giace poi il *layer*, ossia lo strato dei servizi: servizi applicativi, servizi *core*, portali *web* e *e-mail*. Questi si chiamano nel gergo *call service*, accanto ai quali ci sono i sistemi di servizi di natura funzionale, i *functional service*, ossia i sistemi informativi gestionali, i sistemi per gestire la logistica, la sanità e il personale. Attraverso questo *layer* di *networking* vengono erogati i servizi agli utenti. Questa è un po' l'architettura della nostra rete.

Il comparto Difesa condivide il *layer* fisico. La componente fisica è a fattor comune. Abbiamo un'estesa rete in fibra ottica — 13.000 chilometri di fibra sul territorio nazionale; è una delle reti più estese nell'ambito della Pubblica amministrazione — e condividiamo il supporto fisico a fattor comune. L'area di vertice interforze, che include lo Stato maggiore della Difesa e il Segretariato generale, con le singole Forze armate, condivide questo strato di *networking*. Ogni Forza armata è poi organizzata col proprio dominio e ha la sua Intranet.

Le Intranet di Forza armata e l'Intranet dell'area di vertice interforze sono federate in una relazione di *trust* reci-

proca. Pertanto, i servizi vengono condivisi in maniera pienamente interoperabile, come se si trattasse di un'unica rete. L'accesso a Internet oggi avviene per ogni singola Forza armata. Ogni singola Intranet si ritaglia, attraverso operatori commerciali, l'accesso alla rete pubblica, a Internet.

Qual è lo scopo di questo programma dal titolo molto sontuoso, ma in effetti abbastanza semplice? È quello di realizzare l'infrastruttura di accesso diretto, ovviamente a larga banda e ridondato, al *Big Internet*, unico per l'intero comparto Difesa. Abbiamo visto che oggi ogni singola Forza armata nell'area di vertice interforze si ritaglia il suo accesso — lasciatemi il termine — la sua piccola strada provinciale verso Internet. Noi vogliamo, invece, creare l'autostrada verso Internet a fattor comune per l'intero comparto.

In questo scenario il Comando C4 Difesa si va a connettere direttamente con i nodi di accesso nazionale alla grande nuvola Internet, alla cosiddetta *Big Internet*. Questi nodi sono il Namex di Roma e il Mix di Milano. Attraverso questi due centri abbiamo accesso diretto, evitando i *provider*. Il Comando C4 Difesa diventa esso stesso *Internet Service Provider* per l'area di vertice interforze e tutte le Forze armate.

Quali sono i vantaggi di questo progetto? Innanzitutto l'unitarietà di comando e controllo nell'attività di difesa cibernetica: ci concentriamo tutti su quell'autostrada e difendiamo quell'autostrada, anziché disperdere le forze su tante strade provinciali. Questo è, in sintesi, il primo vantaggio.

Le risorse che abbiamo, che non sono ovviamente infinite, verrebbero concentrate a difesa di un unico fronte e sul piano economico si avrebbe una riduzione di costi perché, bypassando i *provider* commerciali e andando a ritagliarsi l'accesso alla rete pubblica di Internet attraverso questi due centri nazionali, i costi sono molto più bassi, a fronte di una maggiore qualità di servizio e di una maggiore disponibilità di banda.

Passando alla tempistica del progetto, va precisato che siamo già partiti. La progettazione è stata già completata. Se ci vengono garantite le risorse, entro il 2016 vorremmo partire per attivare il servizio per l'intera area di vertice interforze, per poi, nel 2017, estendere questo servizio alle Forze armate. Gli oneri finanziari preventivati sono di 2,7 milioni di euro, con un profilo pluriennale, anche qui su un triennio dal 2016 al 2018.

Questo solo per dare l'idea di come la nostra rete si connette in fibra ottica al Mix di Milano e al Namex di Roma. L'architettura finale di accesso della rete Difesa, che noi chiamiamo DIFENET, alla rete pubblica di Internet vede la Difesa diventare un *Autonomous System*, il che significa che ci si svincola dai *provider* e che il *provider* di Internet per l'intero comparto è un ruolo che il C4 Difesa dovrà svolgere.

Con una punta di orgoglio devo dire che la Difesa è stata, nell'ambito delle Istituzioni dello Stato, la prima a chiedere l'iscrizione al RIPE. Oggi il mondo Internet viaggia sull'*Internet Protocol* versione 4, ma nel mondo dell'Internet delle cose c'è sempre più bisogno dell'indirizzamento IPv6. Siamo stati il primo Dicastero a iscriverci al RIPE, che risiede in Olanda, ossia il registro che fornisce i pacchetti di indirizzamento IPv6. Con orgoglio posso dire che il Dicastero della Difesa è il primo in Italia a essersi già dotato dei propri pacchetti di indirizzamento IP.

In tal senso ho già lanciato l'iniziativa verso i dirigenti generali responsabili dei sistemi informatici degli altri Dicasteri, perché svolgo anche questo ruolo: sono dirigente generale responsabile dei sistemi informatici dell'amministrazione Difesa. Nel mio ruolo ho voluto coinvolgere tutti gli altri dirigenti generali per dire che — attenzione — questo Paese deve svegliarsi e andare a chiedere i pacchetti di indirizzamento IPv6.

Probabilmente, da questo punto di vista in ambito nazionale, manca una sala di regia. Ho provato a cercare, nell'ambito della Pubblica amministrazione, chi potesse assumere questa regia, ma non l'ho

trovato. Ci siamo resi, quindi, indipendenti e la Difesa ha adesso ottenuto i propri pacchetti di indirizzamento IP. Sto facendo un'opera di convincimento e di informazione nei confronti dei colleghi, in maniera tale che tutti poi possano farlo. Avendo noi ben note le procedure e, quindi, potendo travasare queste informazioni ed esperienze agli altri, vorrei far sì che la Pubblica amministrazione potesse richiedere per tempo questi indirizzi IP, che saranno fondamentali per un mondo che evolve verso l'Internet delle cose.

Un'altra attività fondamentale è il Piano di *Business Continuity* e di *Disaster Recovery*. Anche qui, che cosa significano *Business Continuity* e *Disaster Recovery*? Ripeto, si tratta di attività complementari, ma senza queste funzioni la risposta alla minaccia *cyber* verrebbe in un certo senso vanificata. Fare *Business Continuity* e *Disaster Recovery* significa disporre di quelle funzioni che costituiscono la capacità dell'infrastruttura ICT di garantire l'erogazione dei servizi istituzionali pur a fronte di eventi disastrosi, anche di natura malevola, ovvero di incidenti informatici dovuti ad attacchi cibernetici. È questa la relazione con il settore della *cyber defence*.

Per ottenere questo, ciò deve tradursi in un processo di riorganizzazione di tutti i *data center* in un unico ambiente di *private cloud*. Noi stiamo introducendo questa tecnologia nei nostri centri di elaborazione dati. Il tutto è predisposto per garantire quella necessaria resilienza atta a evitare soluzioni di continuità nella disponibilità dei servizi. Le risorse di computazione e gli storici devono essere messi a fattor comune per poter garantire il necessario *backup* ai servizi che sono erogati dal comparto.

Anche su questo abbiamo avviato il progetto. Prima del progetto abbiamo redatto un Piano che è stato validato, in termini favorevoli, dall'Agenzia per l'Italia digitale. La prima fase è stata già definita con un progetto esecutivo in corso di avvio. Sto per inviare la lettera di mandato.

La prima fase mira alla razionalizzazione e al consolidamento dei *data center*

dell'area di vertice interforze. Alludo all'area tecnico-operativa dello Stato maggiore della Difesa e delle sue articolazioni e all'area tecnico-amministrativa, ovvero al Segretariato generale, con le sue articolazioni e le sue direzioni generali e le sue direzioni tecniche. Questo in modo da concentrarsi solo su tre centri di elaborazione dati: quello del Comando C4 Difesa in via Stresa, che sarà poi oggetto di visita che la Commissione svolgerà il prossimo 17 marzo; il realizzando CED del Comparto A di Centocelle, che sarà la prossima sede del Segretariato generale (stiamo per attuare il trasferimento del Segretariato da via XX Settembre al Comparto A di Centocelle); e il CED di via Marsala.

Oltre a ciò, l'impresa mira anche a implementare la tecnologia di *private cloud* dei suddetti CED con funzione di *Business Continuity* e *Disaster Recovery*. Gli oneri finanziari per questa prima fase dell'impresa sono stati già garantiti — ripeto, sto per inviare la lettera di mandato alla Direzione tecnica, TELEDIFE — anche qui con un profilo pluriennale 2016-2018.

La fase 2, invece, è finalizzata alla realizzazione e alla convergenza dei *data center* delle Forze armate. Vogliamo portare nel *private cloud* unico della Difesa anche i *private cloud* che nel frattempo le Forze armate singolarmente si stanno realizzando. Vogliamo creare un'unica infrastruttura di *private cloud* predisposta per garantire ai servizi anche funzioni di *Business Continuity* e *Disaster Recovery*. L'impresa sarà l'occasione anche per reingegnerizzare quei vecchi sistemi *legacy* che sono stati costruiti su vecchie tecnologie informatiche, per poter poi consentire agli stessi di operare in una nuova infrastruttura di tipo *cloud*.

La seconda fase dell'impresa è in pianificazione e dovrebbe richiedere circa 10 milioni di euro, anche qui con un profilo pluriennale triennale 2018, 2019 e 2020.

Nella prima fase metteremo, dunque, i tre CED dell'area di vertice interforze in un unico *private cloud*, con *Disaster Recovery* e *Business Continuity* reciproci di tutti i servizi. La seconda fase sarà l'in-

clusione nel *private cloud* unico della Difesa anche dei singoli *private cloud* che le Forze armate si stanno realizzando.

Passerei all'ultimo argomento, il progetto della Rete interministeriale di gestione delle crisi cibernetiche. Posso dirvi con fierezza che il Nucleo di sicurezza cibernetica - il Nucleo di sicurezza cibernetica è il secondo livello, quello operativo - ha affidato alla Difesa il compito di presentare un progetto di realizzazione di una rete robusta che potesse garantire lo scambio di informazioni e, quindi, dare continuità alle comunicazioni in uno scenario di crisi cibernetica, laddove vengono meno le reti e le infrastrutture dei Ministeri della Pubblica amministrazione.

Poter disporre di un sistema di comunicazione ben protetto, robusto, ridondato e sicuro, perché «*up to S*», ossia di classifica di segretezza S, in grado di garantire lo scambio di informazioni e, quindi, di far sì che si possa attuare quella necessaria azione di comando e controllo e di coordinamento dell'attività di reazione è fondamentale e vitale, altrimenti resteremmo senza comunicazione.

Lo studio di fattibilità è stato richiesto alla Difesa in virtù del fatto che la Difesa dispone già di una complessa rete di comunicazione, la DIFENET, e che probabilmente - dico anche questo con un pizzico di orgoglio - è il Dicastero che ha maggiore esperienza nella gestione di reti di natura classificata. Per questo motivo è stato richiesto a noi.

La soluzione ipotizzata è quella di ospitare i nodi che dovranno erogare i servizi presso i *data center* della Difesa, utilizzare la connettività DIFENET, che già in parte serve un determinato numero di Dicasteri e di organismi interessati che siedono al Nucleo di sicurezza cibernetica e sono già raggiunti dalla nostra rete - per una questione di risparmio, ovviamente - e completare la connettività mediante il *leasing* di circuiti dedicati. Non si tratta di servizi, ma di circuiti, proprio di connettività fisica, che verrebbe poi equipaggiata con sistemi proprietari per garantire che il tutto sia sotto un determinato controllo di sicurezza.

Gli oneri previsti sono 3 milioni di euro. C'è poi il mantenimento nel tempo per il funzionamento di questa infrastruttura, che comporta un minimo costo di 350 mila euro per anno. Stiamo cercando di definire le modalità di finanziamento di questa impresa, ossia se farla con un unico finanziamento a cura della Presidenza del Consiglio dei ministri o se ogni Dicastero poi si finanzia la propria porzione di rete.

Dobbiamo anche definire le procedure di acquisizione e la struttura di *governance* sia dal punto di vista tecnico, sia dal punto di vista operativo, sia dal punto di vista della sicurezza. Lo stiamo facendo in concorso, perché la responsabilità è della Presidenza del Consiglio dei ministri.

Passo ora ad illustrare la possibile evoluzione di questa rete. Nasce come rete di gestione delle crisi cibernetiche, ma l'idea è quella di farla evolvere come rete di gestione delle crisi nazionali in sostituzione dell'attuale vecchia rete. Anche qui si tratta di un salto tecnologico della rete di gestione delle crisi nazionali. Questo potrebbe essere il nucleo che può garantire questa capacità nel futuro.

Le due *slide* denominate « Rete interministeriale di gestione delle crisi cibernetiche » vi danno un'idea dei Dicasteri o comunque degli organismi e delle Istituzioni - quelli in verde - che sono già serviti dalla nostra rete Difesa, con un certo risparmio. Quelli rossi dovranno essere serviti attraverso *leasing* di connettività fisica.

Con questo avrei concluso la mia parte della presentazione. Questa è oggi la capacità dell'organizzazione attuale. L'idea della Difesa è quella di costituire il comando preposto a condurre le operazioni cibernetiche, non solo *cyber defence*, ma *computer network operation*.

In tal senso, a fine estate dello scorso anno è stato già istituito il nucleo iniziale di formazione di questo comando, il cui acronimo è CIOC. C'è una *timescale* abbastanza definita. Il processo si deve sviluppare secondo questa tempistica. Entro il 2016 dovrebbe già conseguire una determinata capacità operativa iniziale, do-

tandosi anche degli strumenti per arrivare poi alla capacità finale entro il 2017. Su tali aspetti, tuttavia, si soffermerà più diffusamente il Generale Taricco nell'audizione che si svolgerà subito dopo.

Con questo, signor presidente, ho concluso la mia presentazione.

PRESIDENTE. Grazie. Autorizzo la pubblicazione in allegato al resoconto stenografico della seduta odierna della *slide* della presentazione (*vedi allegato 1*). Do la parola ai deputati che intendano intervenire per porre quesiti o formulare osservazioni.

MASSIMO ARTINI. Questa volta, presidente, mi permetta di essere, purtroppo, un po' più lungo, perché la presentazione dell'Ammiraglio è stata ampia, ma ha suscitato tutta una serie di domande e di dubbi. Anche rifare il punto è piuttosto complesso.

Innanzitutto è interessante vedere come la pianificazione non manchi. La parte di pianificazione e di previsione rispetto al mondo cibernetico - ovvero quelle attività che ci portano anche a dover contrastare da un punto di vista tecnico - è ampia e strutturata. Non mancano le definizioni. Per me, Ammiraglio, è fondamentale sapere quali siano le reali capacità, non tanto quelle attuali. Non la prenda assolutamente come una critica. In realtà, voglio veramente comprendere il livello attuale e ciò che ci aspetta di qui al futuro.

Ieri abbiamo ascoltato il professor Politi, che ci ha riferito che la NATO, per implementare la dimensione *cyber* ha speso 58 milioni di euro. Facendo la somma di quello che è stato messo a regime fino adesso, non si arriva a 14 milioni, se non ho calcolato male.

RUGGERO DI BIASE, *Capo del VI Reparto (Sistemi C4I e Trasformazione) dello Stato maggiore della Difesa.* Sono di più.

MASSIMO ARTINI. Sì, ma per creare tutta la struttura. La domanda che mi

faccio è la seguente: o siamo stati estremamente bravi nel risparmiare su questo tipo di sistema, oppure che cosa effettivamente non si è potuto implementare per carenza di impegno finanziario?

In particolare - questo è un po' il percorso che mi interessa scoprire rispetto a questa indagine conoscitiva - vorrei comprendere chi sono quelli che effettivamente operano. Non le chiedo il numero, perché non vorrei che fosse un'informazione classificata, ma è opportuno comprendere in una struttura come la Difesa, che è ben espressa sia dal punto di vista di struttura di rete, sia di nodi che deve gestire, quali sono le persone che vanno effettivamente a operare nella parte di CERT. Sicuramente - non l'ho presente, ma lo posso supporre - ci saranno dei livelli gerarchici più bassi, oltre al livello di Forza armata, ma l'idea è comprendere chi sia realmente operativo e chi realmente diriga questa attività.

Perché? Perché la *slide* che mostrava il concetto NATO è effettivamente complessa. Occorre comprendere se, come tutti i concetti NATO, sia realmente implementabile, perché effettivamente nella realtà è difficile andare a implementare questo tipo di lavori.

Mi domando, quindi, come punto primo, se le risorse ci abbiano permesso di raggiungere delle capacità che, in caso di effettivo attacco, ci danno la possibilità di rispondere e se effettivamente occorra prendere la consapevolezza che questo è l'unico mondo che ci si prospetta davanti e che, quindi, occorre investire in maniera massiccia, mettendoci anche molto più denaro di quello che lei ha indicato.

Ho apprezzato moltissimo la *slide* in cui vi sostituite come *Internet Service Provider* per i servizi della Difesa. È un concetto intelligente di ridondanza. Preferirei avere un terzo nodo di connessione che non averlo.

Mi domando, però - mi scusi, presidente, se sono un po' lungo, ma devo argomentare questo punto - che tipo di rapporto hanno questi sistemi che andiamo a implementare rispetto al privato

che mi implementa il *private cloud*, la parte di ridondanza, la parte di sistemi, la parte di infrastruttura. Poiché la parte di *hardware*, al netto della logica, mi preoccupa abbastanza, sono preoccupato da quella parte di *leasing* per la connessione delle altre strutture. Per esempio, in questo contesto che tipo di interazione c'è con aziende italiane e non italiane? Penso alla Selex a Chieti, che è un'azienda che sfruttiamo in maniera robusta.

Un'altra domanda riguarda sempre la parte di infrastruttura di *stack* di rete. Quando ha parlato dell'introduzione della *Business One*, un concetto NATO che viene replicato qui dentro, mi sono chiesto chi sviluppi quel tipo di privatizzazione della rete, ossia di VPN, e chi ne abbia la sovranità. Qualora fosse la NATO a svilupparlo, mi domando se ci sia la possibilità per l'Italia di fare customizzazioni sulla parte di privatizzazione o meno, altrimenti la nostra sovranità anche in quel caso se ne può andare.

Le domande sono mirate sulla parte di effettiva sovranità e di reale controllo della situazione e su quanto finanziamento sarebbe necessario per terminare e non per il 2020. Il *private cloud* di tutta la Difesa dovrebbe terminare nel 2020, ma con le programmazioni finanziarie che abbiamo, la preoccupazione è che si vada al 2024. Sono quattro anni. Se penso a come erano i *data center* quattro anni fa e a come sono adesso, vedo che a livello di capacità di *storage* e di trasferimento dati, c'è stata un'evoluzione pazzesca. Questo se l'implementazione fosse fatta adesso. Prevedere fra quattro anni un aggiornamento sarebbe l'opportunità migliore.

Quello che mi preoccupa, infine — e concludo — è la parte che probabilmente affronterà il Generale Taricco, ossia quel settore di *active defence* che è attualmente non implementato. Se, però, la Gran Bretagna ha investito 650 milioni di dollari in questo settore, ci sarà un motivo. Su questo e anche sulla capacità di essere padroni dello sviluppo del *software* che

tipo d'azione si vuole andare a fare? Probabilmente risponderà il Generale Taricco su questo.

PRESIDENTE. Do la parola all'Ammiraglio per la replica.

RUGGERO DI BIASE, *Capo del VI Reparto (Sistemi C4I e Trasformazione) dello Stato maggiore della Difesa*. Provo a fornire una risposta alle domande, estremamente articolate. Partirei dalla NATO. È vero, la NATO ci ha investito oltre 50 milioni di euro. Ovviamente, ho riportato solo le attività principali, ma poi c'è tutta un'attività di accordi *enterprise* per sostituire i prodotti *software* eccetera.

Abbiamo già presentato un Piano perché cerchiamo anche noi di avere accesso ai fondi che il Presidente Renzi mette a disposizione per questo settore. Il nostro Dicastero si è già presentato con una lista delle attività che riteniamo fondamentali per conseguire una crescita capacitiva nel settore, che non riguarda solo la *cyber defence*, ma anche le *cyber networking operation*.

Dunque, le idee ci sono, anche in termini di quello che vogliamo realizzare e di quanto vorremmo investire. Ovviamente le cifre non si discostano tanto da quelle della NATO.

La NATO, peraltro, ha tutta la componente di *active defence* che noi, allo stato attuale, non abbiamo ancora considerato.

Faccio notare, peraltro, che Finmeccanica è stata la società che ha realizzato la *NATO Computer incident response capability* (NCIRC), con molte difficoltà iniziali, perché la NATO chiedeva anche delle cose che tecnologicamente ancora non erano presenti sul mercato. Queste sono state le difficoltà che la nostra industria ha incontrato nel realizzare questa capacità. Alla fine lo ha fatto con un po' di ritardo, come avviene in tutti i programmi, ma non è andata molto in là e ha fatto una buona impresa.

Abbiamo realizzato la *Cyber defence capability 1* (CBC1). Siamo andati in gara e l'ha vinta la Selex, oggi Finmeccanica. Di fatto, la prima parte della capacità è stata

realizzata dalla stessa industria che ha operato nel contesto NATO. Io confido che la seconda fase sarà un'altra impresa condotta con l'industria nazionale, se non altro a livello di *system integrator*.

Ovviamente, come lei ben sa, molti di questi prodotti sono stranieri. In Italia si produce ben poco in questo settore strategico. Forse un'attenzione andrebbe rivolta alla piccola e media industria, che probabilmente ha le potenzialità per potersi esprimere nel settore. Noi dovremmo sicuramente sfruttare meglio la piccola e media industria a supporto dei grandi *system integrator*.

Vengo ora al *cloud*. Noi abbiamo già implementato la virtualizzazione. Adesso quello che stiamo cercando di fare è lo strato di orchestrazione. I servizi oggi non risiedono su macchine singole, come il vecchio paradigma « applicativo-servizio-server dedicato ». Oggi la nostra infrastruttura è già « virtualizzata » e, quindi, i servizi sono ospitati su un'infrastruttura che si ritaglia la quantità di capacità computazionale e di capacità di *storage* in funzione dell'esigenza del singolo applicativo.

Quello che noi vogliamo fare è l'orchestrazione, cioè mettere insieme tutti i pilastri di virtualizzazione, in modo tale da creare il *private cloud*. Noi parliamo solo di *private cloud*, perché non vogliamo andare a esporre fuori i nostri servizi. Per noi è fondamentale rimanere in casa, per questo si parla di *private cloud*.

Le Forze armate contestualmente non stanno aspettando me, ma si sono già organizzate con il loro *private cloud*. Quello che vogliamo fare è un processo, ecco perché è articolato su un certo numero di anni. Ovviamente vanno garantiti i finanziamenti, ma la pianificazione è stata fatta e prevede queste attività.

Quello che vogliamo fare è razionalizzare anche tutto l'assetto dei Centri elaborazione dati (CED) delle Forze armate e avere un unico *private cloud*, in maniera tale che i servizi della Marina possano essere « backuppati » — uso un termine di

derivazione anglosassone — in un'altra infrastruttura, a prescindere da quale essa sia.

Infatti, il mondo del *private cloud* di fatto in un certo senso è agnostico rispetto a dove risiede il servizio, che può risiedere da per tutto. Questo è quello che vorremmo realizzare.

Un processo di virtualizzazione di tutte le nostre infrastrutture di calcolo è già partito da tempo e, ovviamente, i nostri servizi già sono ospitati in infrastrutture « virtualizzate ».

Quello che bisogna realizzare adesso è lo strato di orchestrazione, ovvero la funzione di *business continuity and disaster recovery*. Infatti, oggi noi ci garantiamo soltanto il *backup* dell'applicativo e il *backup* dei dati, ma questo non è sufficiente. Noi dobbiamo far sì che, se l'infrastruttura è affetta da un incidente informatico, anche di natura malevola nel contesto *cyber*, gli stessi servizi automaticamente, secondo le logiche di *business continuity and disaster recovery*, possano essere erogati in tempo reale da un'altra qualsiasi delle infrastrutture CED messa in *cloud*.

Io sottolineo il fatto che noi dobbiamo valorizzare molto la piccola e media industria nazionale. Abbiamo bisogno di queste realtà; ne conosciamo un certo numero molto brave. Noi le abbiamo ingaggiate, perché ovviamente, nel definire i nostri requisiti operativi, noi ci confrontiamo con queste piccole realtà.

Ad esempio, noi ci confrontiamo con TIM e con Finmeccanica, per uno scambio di idee. Dopodiché, una volta che noi abbiamo definito in maniera autonoma il requisito, si va in gara e vinca il migliore, ma sempre nel contesto industriale nazionale.

A proposito dei numeri operativi, come ho sottolineato nella presentazione, noi possiamo dotarci dei migliori strumenti, siano essi navi, carri armati, o aerei, però è l'uomo che è preposto a condurre questi mezzi. È fondamentale il binomio tra lo strumento e l'uomo che lo conduce.

Se io mi doto di uno strumento di analisi altamente sofisticato e l'uomo non

lo sa usare, ho vanificato lo sforzo, ho investito, ho acquisito una capacità notevole, che può dare tanto, ma l'uomo non la sfrutta per quello che potenzialmente quel *software* può darmi.

Per questa ragione, noi ci stiamo concentrando molto sulla formazione del personale. Innanzitutto va selezionato. Si sta pensando di fare bandi di concorso per reclutare il personale con determinati profili. Questo è fondamentale. Per formare una persona in questo settore ci vogliono anni e anni. Se io devo reclutare un giovane ufficiale e poi lo devo formare in dieci anni, di fatto non mi serve. Io dovrei essere in grado di selezionare, attraverso bandi di concorso — lo abbiamo già fatto internamente e lo faremo esternamente per il personale civile — degli ingegneri, dei dottori laureati in informatica, persone che hanno già un'esperienza lavorativa nel settore specifico, per portarli nel nostro contesto istituzionale.

Per il reclutamento del personale militare vogliamo mettere nei bandi di concorso determinate qualificazioni, in maniera tale che si possa selezionare gente che ha già gli *skill* appropriati, da cui partire per formare degli alti specialisti.

PRESIDENTE. Grazie, Ammiraglio. Dichiaro conclusa l'audizione.

Audizione del Comandante del Centro *Intelligence* interforze, Generale di brigata aerea Giandomenico Taricco.

PRESIDENTE. Avverto che la pubblicità dei lavori della seduta sarà assicurata anche attraverso l'attivazione di impianti audiovisivi a circuito chiuso e la trasmissione televisiva sul canale satellitare della Camera dei deputati.

L'ordine del giorno reca, nell'ambito dell'indagine conoscitiva sulla sicurezza e la difesa nello spazio cibernetico, l'audizione del Comandante del Centro *Intelligence* interforze, Generale di brigata aerea Giandomenico Taricco.

Do la parola al Generale Taricco per lo svolgimento della sua relazione.

GIANDOMENICO TARICCO, *Comandante del Centro Intelligence interforze*. Grazie, presidente, per avermi offerto l'opportunità di venire a parlare in questa autorevolissima sede di un argomento sicuramente fondamentale per lo strumento militare.

La mia presentazione sarà leggermente diversa, anche perché innanzitutto non sono bravo come l'Ammiraglio Di Biase, ma anche perché vorrei affrontare la problematica in un'altra prospettiva. Spero che non siate tutti esperti come l'onorevole Artini, perché in tal caso potreste trovare la mia presentazione troppo semplice.

Voglio cercare di fare ordine e di fornire alcune risposte in un mondo che spesso non è così amichevole o *user friendly*. Siamo grandi consumatori di strumenti informatici, ma spesso non apprezziamo fino in fondo quello che c'è dietro e, anziché governare un mondo che diventerà sempre più delicato per la nostra società e per la nostra vita quotidiana, finiamo per subirlo.

Fatta questa premessa, vedremo rapidamente alcuni aspetti, soprattutto nell'ottica dell'esigenza dello strumento militare di operare in questo nuovo (per modo di dire) dominio, che ormai sta crescendo e sta diventando sempre più parte integrante della vita di tutti, compreso lo strumento militare.

Faccio un'ulteriore premessa, giusto per stabilire una terminologia comune e alcuni concetti comuni. È un mondo complesso; per comprenderlo, secondo me, bisogna fare un po' d'ordine. In genere si considera il mondo a tutto tondo. In realtà, si può distinguere.

Io ho usato un codice di colori per concettualizzare. Nella *slide* denominata « Spettro di capacità cyber » la parte gialla è quella di cui ha parlato principalmente l'Ammiraglio Di Biase, che è connessa alla gestione di una rete. Mentre una volta per avere un servizio bastava avere un computer e un modem e andare in rete, adesso non è più così. Per gestire una rete, bisogna avere un'architettura complessa e in particolare per

proteggerla si deve mettere in piedi una serie di predisposizioni, che consentano di mantenerla accessibile e funzionante e soprattutto di evitare che qualche esterno ci entri anche se non è voluto. Quello è il mondo giallo.

Quello che emerge è il mondo che io ho evidenziato in blu, che è quello a cui ha accennato poc'anzi l'Ammiraglio: il *computer network operation*. Si tratta di un mondo emergente, che utilizza questo sistema cibernetico - uso un termine autarchico, non la terminologia inglese - in maniera diversa, con le stesse identiche strutture.

I due mondi convivono, ma in realtà per certi aspetti sono separati. Come sono separati? Normalmente, quando parliamo di una rete, noi vi associamo la nuvola, che è il concetto classico del mondo informatico. La nuvola è una rete. Se la rete è chiusa, non ci sono porte, è facile da proteggere. Essendo chiusa, non si dà accesso e, quindi, è facile garantire la protezione.

Tuttavia, non potendola tenere chiusa, perché si deve interagire con il mondo esterno, si espongono dei servizi. Espo- nendo dei servizi, si aprono delle porte. In quel momento nascono i problemi.

Fisicamente l'apertura delle porte si va a collocare, come vedete, non più nel mondo giallo, ma nel mondo blu. Andando nel mondo blu, deve cambiare l'approccio.

Nel mondo giallo principalmente c'è una problematica di difesa fisica. Prima avete visto che c'erano una serie di misure, che andavano da elementi di politica (procedure, modi di fare) a elementi di prevenzione e protezione fisica, con i cosiddetti *firewall* e con i cosiddetti antivirus. Si passa a una vera e propria interazione attiva per difenderla.

La *computer network defense* (CND) diventa un'attività comune tra i due mondi, che è utile sicuramente per il mondo giallo, ma è altrettanto utile per il mondo blu. Chiaramente prevede, non più una protezione fisica, ma un'interazione attiva dell'uomo, per fare in modo che quel mondo giallo venga protetto.

Quando passiamo nelle *computer network exploitation* (CNE) e nei *computer network attack* (CNA) - uso i termini tecnici - entriamo in un mondo ancora più complesso, dove diventiamo dei veri e propri attori e andiamo a casa degli altri.

Andiamo a casa degli altri perché, per poterci difendere, non basta più difendere il fortino. Per diventare efficaci, tramite le *computer network exploitation*, si deve capire cosa fanno gli avversari o i *competitor*, a seconda del dominio in cui siamo. Se siamo nel mondo commerciale, possono essere dei *competitor* commerciali. Se siamo nel mondo della difesa, possono essere delle realtà statuali che in qualche maniera decidono di confrontarsi e non lo fanno con le regole normalmente accettate dai Paesi democratici, ma lo fanno in altra maniera e, quindi, nasce il problema.

Chiaramente la differenza tra l'*exploitation* e l'*attack* è sottile: mentre nell'*exploitation* si è nella rete, ma si rimane invisibili, nell'attacco si provoca un effetto.

L'esempio classico, che tutti conosciamo, è Stuxnet, cioè l'attacco compiuto in Iran per fermare la produzione di uranio impoverito. Tramite un attacco informatico, fecero un danno fisico, che bloccò la produzione, quindi ottennero un effetto. Quello è il classico esempio di un attacco fatto tramite la rete.

Questa è la premessa. Chiaramente - come potete vedere nella *slide* «Cyber Security - Spettro di Capacità» - il mondo giallo e il mondo blu, che sono già una realtà complessa, si affiancano ad altri due mondi, che sono quello del crimine, codificato in rosso e quello delle infrastrutture critiche in verde.

Le infrastrutture critiche sono le infrastrutture a fattor comune, quelle che tutti devono usare, che per un Paese rappresentano una risorsa essenziale per poter far funzionare la rete, qualunque sia il giocatore, che sia il Ministero della difesa o qualunque altro, compreso il mondo delle imprese private.

Passiamo ai giocatori sotto un profilo di minaccia. Nella *slide* « Piano del conflitto cibernetico » abbiamo due assi. Nell'asse orizzontale, che principalmente ricade nel mondo giallo, abbiamo come nemico il *cyber crime*. Ormai il *business* viene fatto in rete, quindi per uno che ha intenzioni cattive è un'ottima occasione di fare *business* e di riuscire a lucrare soldi, rubando dalla carta di credito a tutto quello che si può immaginare.

L'altro attore è l'attivismo, che è un giocatore che usa la rete. È una forma di protesta. Usando la rete, cercano di mandare dei messaggi e di portare avanti delle campagne che spesso sono di protesta.

Questo è pericoloso, ma non è il più pericoloso. Il più pericoloso è quello dell'asse verticale, dove abbiamo il mondo blu delle operazioni. In quest'asse il confronto avviene tra realtà statuali che usano la rete come un vero e proprio campo di battaglia, perché è estremamente efficace, morbido e invisibile, e spesso si riesce a vincere senza mai arrivare nel *computer network attack*, ma restando solo nella parte dell'*exploitation*.

Come ho detto poc'anzi, il giallo appartiene a tutti; è un mondo che chiunque opera (civile, militare o privato) deve affrontare, se vuole essere competitivo nella società attuale.

Il mondo verde è quello trasversale. È il mondo del cosiddetto « *enabler* », il facilitatore dell'infrastruttura critica.

Il rosso chiaramente è fondamentale per perseguire le attività criminali e così via.

Il blu attualmente è quello meno sviluppato in Italia e che dobbiamo invece affrontare, perché altrimenti rischiamo di restarne fuori o di subire in maniera del tutto passiva gli attacchi che vengono compiuti regolarmente da realtà statuali.

Faccio alcune considerazioni rapide. La debolezza dell'ambiente *cyber* risiede nel fatto che questo ambiente è cresciuto a macchia di leopardo. Questo chiaramente comporta una mancanza di standardizzazione e di scelte condivise e, quindi, una debolezza intrinseca della rete.

Esiste una limitata sensibilità in Italia sull'argomento. Spesso lo si sottovaluta e non se ne capisce l'importanza. Poc'anzi parlavamo di risorse finanziarie; in seguito riprenderemo il tema. Secondo me, finché non riusciamo a farne capire l'importanza, è anche difficile creare il consenso per investire in questo settore. Occorre far percepire che investire in questo settore crea sicurezza per davvero, crea crescita economica, benessere ed economia per il Paese. Finché non si riesce a far capire questo, difficilmente si riesce a ottenere l'obiettivo.

Sulla scena internazionale il *know-how* non è condiviso; chi ha la capacità la nasconde. Se si esamina il caso Snowden sotto tanti aspetti, si vedono anche gli investimenti fatti e le capacità degli Stati Uniti, che fanno la differenza in termini di competitività sul mercato mondiale.

Chiaramente poche risorse, se non vengono sfruttate in modo razionale e con delle scelte condivise, rischiano di restare delle gocce in un deserto.

Dopo questa premessa, che poi riprenderemo, illustriamo perché è importante per la difesa l'attività nello spazio cibernetico.

Come ho detto poc'anzi, la rete ha tre livelli. Il primo è quello fisico, composto, nel caso di questa aula, dai computer, dalla rete *wireless*, dai telefoni e dalle stesse telecamere, perché ormai hanno una tecnologia tale per cui si può mettere tutto in rete. Fanno tutti parte del dominio fisico.

Il dominio logico sono i *database* e i dati. Le nostre enciclopedie e le nostre biblioteche sono in rete. La conoscenza è in rete, in *database* organizzati in maniera più o meno logica.

L'ultimo *layer* e il più importante è quello cognitivo, cioè l'interazione dell'uomo con la rete. L'uomo chiaramente fa la differenza, perché rende la rete imprevedibile. La stessa persona può avere più identità, a seconda delle modalità d'interazione.

Questi tre elementi creano il cosiddetto « mondo cibernetico ». Questo non è a sé stante, ma è trasversale; entra in ogni

aspetto della vita; non ha confini geografici. Un concetto importantissimo è la dimensione temporale: se si perde tempo, non basta lo stesso tempo per recuperare, ma ci vuole il triplo o il quadruplo delle risorse, perché ogni ritardo che si fa in questo dominio ha aspetti e impatti che vanno ben oltre. Se si perde un anno, per compensare si deve mettere il triplo o il quadruplo delle risorse, e non è detto che ci si riesca.

Un altro aspetto importante è il problema dell'attribuzione: non è possibile sapere chi e che cosa. Questo chiaramente crea un grandissimo vantaggio per chi svolge attività criminali o attività statuali.

Ad esempio, nel confronto Stati Uniti-Cina, gli Stati Uniti hanno formalmente accusato la Cina e quest'ultima ha detto: « Fatemi vedere dove sta scritto. Anch'io sono oggetto di attacco di attività cibernetiche. Come fate a dire che sono io? » In effetti, non è possibile dire in maniera evidente che certe cose sono state fatte da una certa realtà.

Semplificando, spesso c'è ancora la cultura secondo cui l'informatica si riassume in due concetti: una diversa macchina da scrivere e un sistema diverso di scambiarsi posta. In realtà, non è così. Di fatto, ha stravolto tutti, il nostro modo di lavorare, il nostro modo di vivere.

Chiaramente per l'ambiente militare è la stessa cosa. Aver messo in rete non solo in termini di servizi tipici, ma anche in termini di sistemi d'arma (gli aerei, le navi, i carri armati, i centri di comando) tutti gli strumenti, è un grandissimo vantaggio, perché significa avere un'efficacia operativa decisamente superiore.

Infatti, in tempo reale si riesce a controllare quello che succede, quindi in termini di comando e controllo si riesce in qualsiasi momento a tenere il *trigger* e il capo può decidere effettivamente se usare la forza. Questo è fondamentale per lo strumento militare.

Chiaramente, però, questo è un motivo di forza, ma è anche un motivo di debolezza, perché mettere tutto in rete comporta che la rete diventa oggetto d'attacco da parte del nemico, ma analogamente noi

possiamo usare la rete come strumento di offesa nel caso in cui si decida di farlo. Dunque, c'è una rete doppia.

È una vera dimensione a sé stante, come il classico difensore militare nella dimensione terrestre, nella dimensione navale e nella dimensione aerospaziale. Adesso c'è un'altra dimensione, che è quella cibernetica, che è a sé stante, ma è anche trasversale ad altre.

Chiaramente, come ogni cosa, il computer può essere un'arma; l'arma di per sé non è pericolosa, ma dipende dall'utilizzo che se ne fa. Può essere usata per minacciare, come strumento di deterrenza o per uccidere. La stessa cosa varrà per il computer.

Ovviamente il computer, visto in questi termini, deve essere gestito, perché lo stesso computer con cui si lavora non può essere utilizzato anche come arma, per una serie di motivazioni, che adesso non abbiamo il tempo di approfondire. Chiaramente deve essere gestito a parte, ma diventerà a tutti gli effetti una vera e propria arma, che potrà essere utilizzata anche in maniera efficace.

Spesso noi trattiamo la problematica *cyber* solo per alcuni aspetti e la vediamo come una problematica di reato di violazione della *privacy*, ma in realtà è uno strumento militare per certi aspetti. Se lo si considera uno strumento analogo all'aereo, al cannone e alla nave, con le regole previste, con cui l'autorità politica e il Parlamento decidono dove deve essere usata, può essere utilizzata come qualsiasi altra tipologia di arma, in modo analogo ai carri armati, alle navi e agli aerei. Questo è importante.

PRESIDENTE. Con le regole d'ingaggio.

GIANDOMENICO TARICCO, *Comandante del Centro Intelligence interforze*. Con le regole d'ingaggio, si può usare tranquillamente questa come tutte le altre armi.

L'aspetto importante è che, per poterlo fare, bisogna avere informazioni, *intelligence*, perché se non si sa dove sparare è difficile. Anche un'arma tradizionale pre-

senta lo stesso identico problema. Le stesse identiche problematiche che ci sono per altre tipologie di armamento varranno per il computer. L'*intelligence* diventa fondamentale. È necessario percepire anche per il settore cibernetico l'importanza dell'*intelligence* e creare un patrimonio informativo che ci consenta di utilizzarlo ai fini che decidiamo di perseguire.

Per far capire l'equiparazione, quando parliamo di sicurezza fisica, mettiamo delle barriere e delle telecamere; la *cyber defense* è la stessa identica cosa nel mondo cibernetico. Quando facciamo una scorta armata di un convoglio, quindi una protezione fisica con l'uomo, facciamo delle *computer network defense* di cui parlavo prima. Analogamente faremo la stessa cosa nell'*intelligence* con il *computer network exploitation* quando facciamo sorveglianza con sistemi *signal intelligence* (SIGINT), *communication intelligence* (COMINT) e così via. Quando facciamo degli attacchi fisici, perché decidiamo di fare soppressione di difese nemiche o attacchi, facciamo qualcosa simile a quello che nel mondo cibernetico facciamo con il *computer network attack*. Il concetto è lo stesso.

La difesa sicuramente fa la parte gialla, che abbiamo visto prima, di cui ha parlato in maniera molto estesa l'Ammiraglio Di Biase. Accanto a quella, dobbiamo fare una difesa attiva, attraverso una vera e propria capacità, non solo di usare strumenti fisici, ma anche di diventare degli attori attivi, ovvero di fare *penetration test* e analisi forense, cioè analizzare gli effetti malevoli che succedono.

Se noi pensiamo, non solo la Difesa, ma anche le altre amministrazioni o qualsiasi altra realtà, di poterci difendere dagli attacchi utilizzando soltanto i tipici strumenti che vanno dall'antivirus al *firewall*, non saremo mai vincenti, perché lo sviluppo tecnologico della minaccia è sempre aggiornatissimo.

L'antivirus, per quanto possa essere efficace, riconosce le minacce di sei mesi o un anno prima. Il nemico attacca con delle tecniche e delle tattiche che sono aggiornatissime e, quindi, probabilmente,

come spesso succede, quando qualcuno entra nella rete non ce ne accorgiamo, perché l'antivirus non riconosce quel tipo di tattica, sulla base di quello che c'è, essendo già vecchio.

In quel caso non si può comprare. Per riuscire a difendersi, bisogna svilupparsi da soli quelle conoscenze che consentono di riconoscere la minaccia. Come lo si fa? Lo si fa in maniera attiva, filtrando e studiando ogni giorno gli eventi, per capirli, sulla base di correlazioni. Infatti, una certa azione fatta sulla rete è un attacco, non è un'azione normale.

Chiaramente l'*intelligence* è fondamentale. Bisogna avere dei dati di archivio per essere in grado di capire l'evoluzione della minaccia, giorno per giorno, in base a quello che succede.

Ovviamente occorre costruire un ordine di battaglie *cyber*, perché, se dobbiamo decidere di fare degli attacchi, dovendo farlo sul nemico, dobbiamo sapere quest'ultimo che tipo di organizzazione ha e dove poter eventualmente attaccare nel caso in cui si decida di farlo.

Passo rapidamente agli aspetti organizzativi. Nella *slide* « Riferimenti principali » è raffigurato il quadro normativo che ha già tracciato l'Ammiraglio Di Biase, a cui si aggiungono delle nostre direttive interne.

C'è un concetto importante riguardante la NATO, della quale abbiamo parlato in maniera estensiva. La NATO tratta soltanto la parte gialla, ma non la parte blu. La parte blu è sensibile e non è trattata in un contesto multilaterale o multinazionale, per cui su quell'argomento non si fanno discussioni a livello NATO.

L'organizzazione attuale è descritta nella *slide* « Competenze Cyber — Situazione attuale ». Da questa organizzazione, dove vogliamo andare? Col codice giallo e blu, vediamo chi fa cosa in questo momento, tra la Difesa e il comparto per l'informazione e la sicurezza della Repubblica, che è un giocatore fondamentale nel quadro normativo-organizzativo, dove in questo momento abbiamo delle interazioni.

Principalmente, come vedete, l'attività è rivolta al mondo giallo, mentre il mondo blu è parzialmente svolto dal reparto dove attualmente presto servizio io, ovvero il II reparto del Centro *Intelligence* interforze. In seguito vedremo in maniera minimale cosa abbiamo fatto. Chiaramente lavoriamo in stretto coordinamento, come previsto dalla legge n. 124 del 2007 e dai relativi regolamenti applicativi, con il comparto per l'informazione e la sicurezza della Repubblica.

Nella *slide* « Organizzazioni nazionali attuali » ci sono i giocatori con cui interagiamo: a sinistra ci siamo noi e a destra c'è il Ministero degli interni. Sia con il settore Centro nazionale anticrimine informatico per la protezione delle infrastrutture critiche (CNAIPIC) sia con il settore Ministero delle poste e delle telecomunicazioni, abbiamo una stretta correlazione. Infatti, quando scopriamo giocatori, che magari sono dei criminali, che agiscono sulla nostra rete, chiaramente informiamo tempestivamente gli organi preposti per farlo. Allo stesso modo, concorriamo con il CNAIPIC alla difesa delle infrastrutture critiche, che è fondamentale, in quanto comunque, mettendoci tutti assieme, non saremmo mai sufficienti per gestire un mondo così complesso.

Passo ad alcune considerazioni veloci. Ribadisco che la *cyber* non è solo una questione di gestione delle reti. In realtà, si basa su due pilastri: il mondo giallo e il mondo blu. Cercheremo di mettere assieme quei due mondi in quel comando di cui parleremo tra poco.

Le *computer network operation* sono sensibili. Come ho detto poc'anzi, a livello NATO non se ne parla. A maggior ragione, non se ne parla in termini generali, perché, essendo una tecnologia sensibile, che dà un grande vantaggio, ogni investimento e ogni pezzo di conoscenza viene protetto, perché svelarlo comporterebbe un grande danno economico.

Snowden, oltre a tutti i problemi che ha creato, ha bruciato investimenti tecnologici americani, perché, una volta che uno

rivela la capacità, automaticamente l'altro adotta una contromisura e, quindi, l'investimento è vanificato.

Abbiamo già citato i percorsi formativi. Non esiste una scuola dove si può comprare. I percorsi formativi devono essere creati *ad hoc* sulla specifica esigenza, innanzitutto perché, come ho detto prima, sicuramente serve un *background*. Abbiamo bisogno di alcuni ingegneri, ma abbiamo bisogno anche di operai. Noi dobbiamo formare il personale in tempi rapidi e consistenti con l'esigenza, con dei percorsi che riescano a dare alle persone specifiche conoscenze per il lavoro che devono svolgere. Non tutti devono essere superesperti; servono probabilmente delle conoscenze di settore che, messe assieme, fanno un *puzzle* che si combina e, quindi, dà una certa capacità. Noi le abbiamo sviluppate internamente.

Arrivo alle conclusioni. Abbiamo sviluppato il percorso formativo, che sta funzionando ed è quello che ci ha consentito di diventare degli *enabler*, come affermava poc'anzi l'Ammiraglio Di Biase.

Quando ci siamo confrontati con altri dicasteri, abbiamo scoperto che il personale che abbiamo addestrato noi è risultato molto competitivo e molto utile anche per loro, per capire cosa stesse succedendo.

Abbiamo implementato una capacità di *cyberlab* a Ponte Galeria, che è fondamentale sia per formare che per addestrare il personale.

È stata condotta un'attività esercitativa specialistica. Spesso si fanno esercitazioni in ambiente internazionale, ma sono edulcorate, ovvero si svolgono a livello procedurale, perché in realtà la volontà di condividere certe conoscenze, facendo delle attività pratiche, non c'è. Pertanto, le attività reali si svolgono solo sull'ambiente nazionale. È difficile trovare il consenso per fare un'esercitazione in ambiente multinazionale, perché chiaramente ciò significa svelare capacità che spesso non si vogliono condividere o che, una volta condivise, perdono di efficacia.

PRESIDENTE. Non esistono alleati in questo.

GIANDOMENICO TARICCO, *Comandante del Centro Intelligence interforze*. Non esistono alleati, purtroppo questa è la dura realtà, o meglio ci sono alleati finché l'obiettivo è comune, mentre quando l'obiettivo non è più comune automaticamente diventiamo amici ma competitivi. Questa è la differenza. In realtà, la grande battaglia è principalmente economica e, quindi, siamo tutti alleati, ma siamo anche tutti competitivi, perché ognuno comunque vive di competizione. Questa è la regola di fondo.

Abbiamo impostato delle capacità di pronto intervento, che ci consentono di affrontare in maniera più efficace la difesa, non fermandoci alla parte gialla, ma avendo una buona capacità anche di operare in *computer network defense* e, quindi, di avere un ruolo attivo in termini di analisi forense, ovvero ricostruire quello che è successo, verificare la robustezza delle reti e cercare di fare *reverse engineering*.

L'*intelligence* è sempre un processo a rovescio: noi partiamo da quello che è successo e cerchiamo di ricostruire il punto di partenza. Si tratta di un'attività difficile, che deve essere svolta anche in questo settore. Capendo come uno ha agito, si riesce anche ad adottare la contromisura per evitare che questo possa ripetersi.

Abbiamo impostato dei programmi di acquisizione di sistemi di supporto per la parte blu. Non voglio citare i numeri, perché altrimenti la relazione diventerebbe troppo lunga e troppo pesante.

Abbiamo avviato soprattutto un'attività di formazione, che è la cosa più importante. Io dico sempre che le risorse finanziarie sono fondamentali, perché senza di esse non si riesce a ottenere il risultato, ma è più importante l'uomo. Se bastasse avere il denaro, tutti avrebbero questa capacità. In realtà, nessuno ha questa capacità, perché i soldi sono una parte del problema, ma non sono quella fondamentale. La parte fondamentale è rappresen-

tata dall'uomo e dalle sue capacità di utilizzare in una certa maniera queste risorse e questa tecnologia.

Il percorso formativo lo abbiamo sviluppato *in house* concettualmente, cercando di capire le competenze che servivano e costruendo dei moduli addestrativi, che abbiamo acquisito a pezzetti, mandando le persone fuori, mettendole assieme, facendo un percorso che è diventato consistente, per dare una capacità completa alle persone.

Per ciò che concerne le attività iniziali, siamo in grado di cominciare a sviluppare un ordine di battaglia *cyber*, che si può fare anche soltanto sul mondo aperto, senza chissà quali attività sofisticate, solo andando con metodo in tutti i settori esposti. Le formazioni esposte correlate già forniscono molte informazioni e comunque sono utili. È un'attività che si può svolgere anche da casa propria e che, fatta con metodo e sapendo cosa cercare, può diventare efficace.

Abbiamo sviluppato sistemi di pianificazione della condotta di operazioni *cyber*. Se noi immaginiamo la *cyber* come una capacità militare, ne deduciamo che diventerà un'operazione tradizionale, come l'operazione terrestre, l'operazione navale o l'operazione aerea. Pertanto, anche l'operazione *cyber* dovrà avere degli strumenti per poter pianificare.

Abbiamo implementato dei sistemi perimetrali per fare *Computer Network Defence* (CND), dove, a complemento dell'attività di protezione con antivirus e con *firewall*, effettuiamo una vera e propria verifica e filtro in tempo reale di eventuali minacce. Abbiamo formato del personale specialistico e stiamo definendo le procedure operative per acquisire questa capacità.

Senza questa capacità, la Difesa non sarà più competitiva, perché ciò vorrebbe dire restare fuori dal mondo futuro. Infatti, questo tipo di attività diventerà sempre più predominante per lo strumento militare, in quanto è un'attività per certi aspetti efficace ed estremamente *safe*, perché molto spesso non muore nessuno. Si può distruggere un *server*,

ma, non morendo nessuno, si arreca un danno efficace, riducendo al minimo il danno collaterale. Di conseguenza, questo è uno strumento che nel futuro potrà diventare molto efficace, nel momento in cui ci si dovrà confrontare e usare la forza.

Il quadro normativo al momento attuale assegna molte competenze al Sistema di informazione per la sicurezza della Repubblica, ma probabilmente non definisce in maniera sufficiente i compiti della Difesa. Sarebbe opportuno chiarire meglio i compiti della Difesa per agevolare un certo tipo di attività, soprattutto nel settore dell'*exploitation*, che diventa fondamentale per l'efficacia sia della Difesa che di un eventuale attacco.

È necessario valutare un eventuale adeguamento del quadro normativo. I principali alleati lo hanno già fatto in maniera efficace. Chiaramente il Paese di riferimento rimangono gli Stati Uniti, che hanno affrontato sicuramente molto prima degli altri la problematica e lo hanno fatto secondo me in maniera efficace, definendo bene nel settore giallo, nel blu, nel rosso e nel verde chi deve fare che cosa. Lo hanno fatto con una struttura che riesce, nonostante tutto, a essere sinergica e convergente per l'obiettivo comune. Gli aspetti critici di cui parlava l'onorevole Artini, secondo me, sono i veri *gap*, non solo della Difesa, ma a livello nazionale. In un settore come questo non abbiamo capacità nazionali né dal punto di vista *hardware*, né dal punto di vista *software*. Non avere capacità significa subire gli altri, con tutto quello che comporta. Infatti, quando si compra un computer, un *server* o un qualsiasi pezzo dell'architettura di cui parlavo prima, si può comprare anche la porta attraverso la quale chi vuole può estrarre le informazioni.

Quando a casa — dovremmo farlo tutti — installiamo un *software* per poter controllare in remoto il computer di casa, perché ci fa comodo accedervi dall'ufficio, volontariamente apriamo la porta dalla quale può entrare chiunque, sapendoci entrare. Cito un esempio che probabil-

mente conosciamo tutti e che dà un'idea molto concreta di come è complesso questo mondo, se non lo si affronta con metodo.

In realtà, è un mondo come tutti gli altri. Spesso noi facciamo fatica, non conoscendo molta della terminologia usata dall'Ammiraglio Di Biase, perché non abbiamo acquisito quel dizionario di 300-400 parole che magari abbiamo acquisito in altri settori. Forse si acquisirà tra dieci o venti anni, perché da ragazzini, giocando, si acquisisce una terminologia che poi rimane tutta la vita. Magari chi ha la mia età, o è più grande, è cresciuto in un'epoca in cui i computer non erano così diffusi, per cui non ha sviluppato questa terminologia e fa più fatica a capire concetti che non sono difficili ma, messi assieme, diventano complessi. Si fa fatica a capirli, non avendo magari neanche la terminologia per comprendere il termine tecnico a quale concetto si associa.

Le risorse spesso non sono valorizzate e messe a sistema. L'Ammiraglio Di Biase parlava di piccole realtà. Spesso nel mondo cibernetico non servono grandi investimenti, perché principalmente è una questione di capacità dell'uomo. Un uomo può fare la differenza. Chiaramente occorre saper riconoscerlo, valorizzarlo e metterlo in condizione di fare quello che è in grado di fare per il bene complessivo.

Spesso i grandi investimenti, se non c'è l'uomo che ha un reale *know-how* o l'intuito corretto, non portano risultati. Da ciò deriva l'importanza di saper individuare le persone che valgono, riuscire ad attrarle e metterle in condizione di poter operare in questo settore.

Al reclutamento abbiamo accennato poc'anzi. In Difesa, nonostante tutto, non siamo ancora così bravi, non solo noi. Anche confrontandoci con gli altri Paesi, emerge che spesso l'esigenza portava a individuare persone con una certa struttura fisica e con una certa muscolatura, perché era più che altro una questione fisica. Probabilmente in futuro non serviranno più quel tipo di persone, o comunque non nel numero con cui le cercavamo prima, ma serviranno persone che magari

sono piccole e portano gli occhiali, ma sono bravissime a usare la tecnologia. Pertanto, occorre anche una capacità di adattare il reclutamento e valorizzare certe caratteristiche.

Secondo me, il Paese in assoluto più lungimirante è Israele, che ha capito l'importanza di questo settore. Avendo ancora la leva obbligatoria, riesce a filtrare le persone in gamba addirittura al liceo (spesso le persone hanno la maggiore capacità di produzione quando sono molto giovani) dove fanno dei test propedeutici alla visita. Riescono a individuare le persone che sono più portate per questo tipo di mondo e poi cercano di utilizzarle per le capacità che hanno.

Questo è chiaramente un approccio molto efficace, che consente di costruire nel tempo, in dieci, quindici o vent'anni, una squadra molto forte, che poi riesce a distribuirsi dappertutto, come deve avvenire nel mondo cibernetico. Avere delle persone competenti, valorizzate e sfruttate significa avere dappertutto gente che è in grado di interagire e di dare consistenza ed efficacia al processo.

Il *procurement* è un altro aspetto molto importante. La tecnologia è molto veloce e spesso i processi con cui noi compriamo materiali sono troppo lenti, per cui, da quando noi definiamo l'esigenza a quando il contratto va in esecuzione, compriamo cose che sono già obsolete. Non riusciamo a essere abbastanza veloci. Avere un processo di acquisizione veloce, che consenta di acquisire cose che non sono vecchie, è fondamentale.

Occorre soprattutto saper scegliere cosa comprare. Nella Pubblica amministrazione la regola fondamentale è comprare al massimo ribasso. Spesso comprare al massimo ribasso significa comprare il computer cinese. È probabile che coloro che sono dietro al computer cinese siano scaltri e riescano a venderci, facendoci pagare, lo strumento col quale poi ci ruberanno le informazioni.

È necessaria una standardizzazione e razionalizzazione della spesa, perché saper scegliere secondo concetti condivisi ed efficaci significa dare consistenza a

tutta la struttura e, quindi, renderla più forte. Se dobbiamo difendere la parte gialla, lo si fa avendo una struttura solida ed efficace. Se la struttura non è solida ed efficace, diventa estremamente difficile difenderla.

Le verifiche di sicurezza sono fondamentali, perché consentono di acquisire quella sovranità che nel mondo informatico è sicuramente un elemento di debolezza per l'Italia.

Questa è l'ipotesi su cui stiamo lavorando: la stessa struttura che avete visto prima razionalizzata, dove sicuramente colleghiamo in maniera più solida e reale l'anima gialla e cerchiamo di farla funzionare dovunque opera con un'unica regia, in maniera molto più sincronizzata di quanto lo sia adesso. La parte blu è la seconda gamba del comando cibernetico, per essere capaci e prepararci a svolgere sia operazioni a supporto della Difesa sia operazioni offensive, qualora venisse deciso, in questo nuovo settore emergente.

Il punto di domanda rispetto al Sistema d'informazione per la sicurezza della Repubblica è quello a cui accennavo poc'anzi. Probabilmente nel quadro normativo manca un reale collegamento, per fare in modo che anche la Difesa possa svolgere nel settore dell'*intelligence* il ruolo che serve per poter essere consistente ed efficace.

PRESIDENTE. Grazie Generale. Autorizzo la pubblicazione in allegato al resoconto stenografico della seduta odierna della *slide* della presentazione (*vedi allegato 2*). Do ora la parola ai colleghi che intendano intervenire per porre quesiti o formulare osservazioni.

MASSIMO ARTINI. Presidente, in questo caso evito di fare commenti, non perché non ne voglia fare, ma perché mi sembra che questa presentazione dia un quadro chiarissimo di qual è lo spunto e, nell'ambito dell'indagine conoscitiva — se mi posso permettere — apre l'aspetto relativo alla parte attiva, per quel che è di nostra competenza, oltre alla conoscenza

tecnica. Oggi è stata una giornata relativamente pesante dal punto di vista delle nozioni informatiche.

C'è un discorso normativo che è fondamentale: come faceva presente il Generale Taricco, dal punto di vista della legislazione attuale o comunque dei regolamenti vigenti attualmente, non c'è una definizione chiara dei compiti.

Voglio porre una domanda. Nelle ultime *slide* abbiamo visto la capacità di attacco e di svolgere operazioni, che ovviamente rimangono limitate a quel sistema di test che si compiono internamente, nel senso che non è un qualcosa che può essere distribuito all'esterno, perché questo potrebbe essere un rischio, se non normato.

Il problema è proprio questo: c'è un mondo completamente diverso che, oltre a dover prendere una forma reale, per quanto virtuale nella sua accezione *software*, deve essere previsto dalla normativa.

Dal mio punto di vista, manca una previsione che dia delle garanzie a chi opera in questo mondo, anche funzionali. Infatti, certi tipi di operazioni sono particolari e possono provocare, se non danni collaterali, danni effettivi di un'efficacia impressionante.

Arrivare, non solo ad acquisire competenze, ma anche a poterle mettere in campo, sulla base di una catena di comando che decide, è il passaggio che, per quanto riguarda la parte parlamentare, ritengo essere fondamentale. Si tratta di capire come si norma questo mondo delle *computer network operation* e delle *computer network exploitation*. Il fatto di poter raccogliere informazioni è già un aspetto molto sensibile, anche rispetto alla semplice difesa.

Anche su questo punto dovremmo domandarci che tipo di legislazione stiamo utilizzando per salvaguardare chi opera.

PRESIDENTE. L'onorevole Artini ha ben rappresentato quello che è probabilmente l'oggetto principale di questa indagine conoscitiva e della nostra responsabilità come Commissione difesa. Si tratta

di un problema oggettivamente complicato.

Nell'introduzione lei, Generale, ha correttamente fatto il paragone tra gli strumenti tradizionali di attacco e di strategia militare e questa nuova dimensione, con le caratteristiche che la contraddistinguono: anonimato, riservatezza e segretezza.

Quando parliamo di regole d'ingaggio e di delimitazione del perimetro in cui quest'azione deve svolgersi, abbiamo un problema complicato, anche dal punto di vista giuridico e normativo, a cominciare dal dettato costituzionale, che regola in maniera molto rigida per il nostro Paese la possibilità di attacchi, escludendo la guerra. Questo può rappresentare un pezzo del nuovo conflitto.

MASSIMO ARTINI. Come affermato dal Segretario della NATO Stoltenberg una quindicina di giorni fa a Bruxelles, ormai è riconosciuto dalla dottrina che un attacco cibernetico può far scattare l'articolo 5 dell'alleanza NATO, che è fondamentalmente un'autodifesa, ovvero una difesa da un attacco di guerra.

Pertanto, gli appunti che il presidente faceva sul percorso costituzionale e sul fatto che questo tipo d'attacco sia normativamente previsto come guerra, toccano una serie di aspetti giuridici particolari.

PRESIDENTE. Ringrazio il Generale e gli chiedo la disponibilità, anche nel futuro prossimo, a seguirci in questo tipo di percorso che noi abbiamo appena avviato, sulla base della sua esperienza e delle cose che molto interessanti che oggi ci ha riferito.

Da militare, aiutateci a costruire un quadro normativo in cui inserire in maniera più lineare e trasparente questa nostra missione.

PAOLA BOLDRINI. Sarò molto veloce, anche perché il collega Artini, che è un informatico, conosce molto bene questa materia. Io, invece, mi sono approcciata a questo tema in maniera autodidatta, nel senso che ho imparato man mano. Vorrei porre due o tre domande.

Innanzitutto, lei ci diceva che gli Stati Uniti sono i più evoluti sotto il profilo della difesa cibernetica, forse anche perché la loro storia è molto più lontana nel tempo rispetto alla nostra. Ha citato anche Israele. Vorrei sapere noi, invece, come ci posizioniamo in questa sorta di graduatoria, per capire quanto ancora dobbiamo lavorare.

Inoltre, lei parlava anche dell'acquisizione dei materiali *hardware* e anche *software*. Ovviamente, conoscendo la prassi dell'acquisizione amministrativa pubblica, che avviene attraverso sistemi di acquisizione centralizzati, so che ci sono delle lungaggini che da un certo punto di vista ci proteggono da alcune cose. Provenendo dall'ambiente universitario, so che, ad esempio, le specificità dei laboratori di tipo scientifico non possono essere assecondate dalle richieste di una centralizzazione degli acquisti. Capisco molto bene questa questione.

Eventualmente, normativamente parlando, vista la specificità del vostro lavoro, si potrebbero prevedere delle clausole derogatorie per l'acquisizione. Questa è una riflessione che pongo.

Noi siamo entrati nel progetto dell'Agenda digitale (Strategia dell'Europa 2020), che comprende un allargamento e una programmazione, per diffondere — lo vediamo anche nel nostro Paese — la digitalizzazione di tutti i sistemi.

Proprio ieri, facendo parte della Commissione affari sociali, ho partecipato all'audizione del Garante della *privacy*, durante la quale, oltre al tema della garanzia della *privacy* dei dati, si è affrontato anche il tema della sicurezza dei dati stessi, che sono dati sensibili. Ovviamente da questo non dipende la sicurezza del Paese, ma sicuramente dipende la sicurezza della persona.

Siccome dobbiamo proteggere tutti i dati che sostengono questi flussi, vorrei sapere se nell'Agenda digitale non si potrebbero cercare i fondi — lo diceva anche il Garante della *privacy* — per proteggere i dati che fluttuano dentro al sistema cibernetico.

PRESIDENTE. Do la parola al Generale Taricco per la replica.

GIANDOMENICO TARICCO, *Comandante del Centro Intelligence interforze*. Grazie per le domande, che sono sicuramente molto interessanti e molto pertinenti e mi danno modo di ampliare alcuni temi.

Gli Stati Uniti sono il Paese che ha lanciato la rivoluzione digitale. Avendo lanciato la rivoluzione digitale, automaticamente sono diventati i principali conoscitori, hanno maggiori *expertise* e governano un certo tipo di processo.

È un'opportunità che potevamo avere anche noi, perché è nata grazie a qualche ragazzo, come Bill Gates (li conosciamo tutti). Hanno una squadra di persone che hanno saputo capire l'importanza del settore e lo hanno trasformato. Probabilmente era anche il momento giusto, perché la tecnologia era maturata in una certa maniera e, quindi, certe soluzioni tecnologiche utilizzate potevano fare la differenza.

Avendolo inventato, hanno un vantaggio, che è quello di viaggiare sempre in anticipo rispetto agli altri e di condizionare comunque tutti gli altri.

Come ho detto prima, la problematica più rilevante è che un'ora nel mondo cibernetico non equivale a 60 minuti. Se si perde un'ora, in realtà se ne perdono tre e, quindi, recuperare diventa molto difficile o probabilmente impossibile.

Quindi — mi ricollego alla seconda domanda — non potendoci permettere di sviluppare in maniera autarchica computer e *software*, perché non saremmo competitivi, in quanto la soluzione che avremmo sarebbe comunque scadente rispetto a soluzioni che offrono Paesi che fanno questo da molto più tempo, qual è la bravura?

La bravura è quella di riuscire almeno a controllare ciò che noi acquisiamo e utilizziamo in un certo tipo di struttura pubblica, della Difesa o istituzionale, come hanno fatto gli inglesi, che hanno imposto che qualsiasi pezzo di *hardware* e *software* entri in Inghilterra deve essere completa-

mente trasparente per l'autorità governativa britannica, senza riserve. Chiunque decide di vendere in Inghilterra lo può fare, ma lo fa dando completa visibilità sul progetto, sul funzionamento e sul *software* inserito.

È una decisione molto forte, però in tal modo si riesce a imporsi o almeno a garantire parzialmente la sovranità nazionale in un certo tipo di settore, che diventerà sempre più fondamentale.

A questo proposito, mi collego al tema della digitalizzazione del Paese. Vivremo sempre di più nel mondo digitale, perché è facile, accessibile ed efficace e, quindi, diventerà sempre più parte della nostra vita. Se non riusciamo ad agire in maniera efficace, saremo inconsistenti.

Avendo poche risorse, l'unico modo di farlo è compiere scelte condivise. Quando parlavo di standardizzazione intendevo dire che la struttura nel suo complesso, che è un insieme di pezzi di varia tipologia, deve essere costruita con scelte condivise, secondo precisi requisiti di sicurezza. Facendo certe scelte a monte, si impone automaticamente la sicurezza e non lo si fa a macchia di leopardo.

Spesso è successo che in una certa realtà, privata o pubblica, che fosse un reggimento o uno stormo della difesa oppure un'impresa privata, c'era uno bravo che diceva « ci penso io » e organizzava. Quella persona magari era bravissima, però compiva delle scelte che nella sua logica erano efficaci, mentre in una logica più grande potevano essere nel tempo non così efficaci.

Occorre fare scelte condivise in termini di standardizzazione e di interoperatività e soprattutto mantenerle aggiornate, perché la tecnologia viaggia così veloce che, se non viene aggiornata, automaticamente diventa obsoleta.

Nella nostra rete succede giornalmente che subiamo attacchi informatici, perché non riusciamo ad aggiornare i sistemi.

Faccio un classico esempio: tutti a casa abbiamo ancora un computer XP, che magari funziona ancora, però, messo in una rete, determina una debolezza, perché è un'architettura obsoleta e, quindi, facile

da penetrare. Essendo in rete, diventa una porta facilissima, tramite la quale un soggetto può accedere e poi, una volta che è nella rete, può andare dove vuole. Ricordate la nuvoletta: una volta aperta la porta e entrati, si può navigare. Non cambiare il computer XP perché non si hanno risorse finanziarie significa di fatto creare una debolezza.

Occorre avere la capacità e percepire l'importanza d'investire, mantenendo le cose aggiornate nel tempo.

Chiaramente si può anche decidere di fare scelte come quella dell'India di qualche giorno fa. Non so se avete letto sui giornali che l'India ha deciso di uscire da Windows e da Microsoft e di sviluppare un sistema completamente nazionale indipendente, che la svincola da qualsiasi dipendenza, in questo caso statunitense.

Per fare ciò occorre avere la consapevolezza delle risorse che servono per attuare una scelta del genere. Chiaramente diventa difficile capire se il sistema Italia ha le risorse sufficienti per fare una scelta del genere, ma è un'altra possibilità.

Ovviamente la *privacy* è un tema fondamentale. Nel mondo giallo anche i dati privati devono essere protetti con la stessa efficacia con cui vengono protetti i dati militari della Difesa.

I dati sono importanti. Forse vi ricordate che qualche mese fa è stato riportato sui giornali che negli Stati Uniti sono penetrati e hanno rubato i dati personali. Se hanno i dati del Presidente, possono costruire un patrimonio informativo, con il quale poi lo possono attaccarono.

È chiaro che i dati devono essere protetti. Questo rientra sempre nel mondo giallo. Chi è deputato a gestire i dati personali, che sia una realtà pubblica o una realtà privata, deve essere protetto con una struttura gialla altrettanto efficace e altrettanto aggiornata in maniera costante.

L'Agenda digitale è trasversale. Rientriamo nel discorso di avere un sistema che è in grado di fare scelte condivise, governate e spiegate. Infatti, se le cose vengono spiegate, c'è la percezione dell'importanza e automaticamente è facile sce-

gliere d'investire risorse in questo settore e fare scelte corrette.

Spero di aver risposto a tutte le domande.

PRESIDENTE. La ringrazio ancora, Generale. Credo che prossimamente ci r incontreremo, nell'ambito delle visite che abbiamo programmato di svolgere presso le strutture della Difesa che si occupano di questi temi e, quindi, anche in quella che lei comanda.

Dichiaro conclusa l'audizione.

La seduta termina alle 16.05.

*IL CONSIGLIERE CAPO DEL SERVIZIO RESOCONTI
ESTENSORE DEL PROCESSO VERBALE*

DOTT. RENZO DICKMANN

*Licenziato per la stampa
il 6 maggio 2016.*

STABILIMENTI TIPOGRAFICI CARLO COLOMBO



STATO MAGGIORE DELLA DIFESA

Stato Maggiore Difesa

**Capacità di Cyber Defence
della Difesa
Audizione da parte della 4^a Commissione Difesa**

Roma, 9 Marzo 2016

ALLEGATO 1



SCOPO DELLA PRESENTAZIONE

Stato Maggiore Difesa

**Illustrare alle On. SS.VV. l'attuale
Organizzazione e lo stato dell'arte
delle Capacità di Cyber Defence del
Comparto Difesa**



AGENDA

Stato Maggiore Difesa

- **Quadro normativo e Struttura Nazionale preposta alla Difesa Cibernetica**
 - **Organizzazione Cyber Defence del Comparto Difesa**
- **Le attività finalizzate allo sviluppo della Capacità di Cyber Defence del Comparto Difesa**
 - **Programma «CYBER DEFENCE CAPABILITY»**
 - **Progetto «AUTONOMOUS SYSTEM»**
 - **Piano di «BUSINESS CONTINUITY & DISASTER RECOVERY»**
- **Rete Interministeriale di Gestione delle Crisi Cibernetiche**



Struttura Nazionale di Difesa Cibernetica

Quadro normativo di riferimento

Stato Maggiore Difesa

DECRETO DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI 24 gennaio 2013.
Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale.

Publicato nella G.U. 19 marzo 2013, n. 66.

IL PRESIDENTE DEL CONSIGLIO DEI MINISTRI

Vista la legge 2 agosto 2007, n. 124, recante "Sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto", come modificata e integrata dalla legge 7 agosto 2002, n. 232, e, in particolare, l'art. 1, comma 1, lettera c); visto il decreto del Presidente del Consiglio dei Ministri del 12 settembre 2007, n. 105, recante "Linee guida del Comitato interministeriale per la sicurezza della Repubblica, adottati apposite direttive per rafforzare le attività di informazione per la protezione delle infrastrutture critiche materiali e immateriali, con particolare riguardo alla protezione delle infrastrutture critiche materiali e immateriali, ai sensi del paragrafo 1-bis, al senso del quale il Governo allega alla relazione sulla politica dell'informazione per la sicurezza e sui risultati ottenuti, che presenta annualmente al Parlamento, il documento di sicurezza nazionale, concernente la protezione delle infrastrutture critiche materiali e immateriali e immateriali, nonché alla protezione cibernetica e alla sicurezza informatica;

Visto l'art. 4, comma 3, lett. 4-bis) della citata legge 2 agosto 2007, n. 124, al senso del quale il Dipartimento delle informazioni per la sicurezza coordina le attività di ricerca informativa finalizzate a rafforzare la protezione cibernetica e la sicurezza informatica nazionali;

Visto l'articolo 1 della legge 1° aprile 1981, n. 121;

Visti il decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 2 settembre 2005, n. 188, e il decreto del Presidente del Consiglio dei Ministri 27 settembre 2005, n. 144, recante "Linee guida per la protezione cibernetica", che, all'articolo 7-bis, dispone che, ferme restando le competenze dei Servizi di informazione per la sicurezza, i competenti organi del Ministero dell'Interno assicurano i servizi di protezione informatica delle infrastrutture critiche materiali e immateriali, ai sensi del paragrafo 1-bis, del decreto del Presidente del Consiglio dei Ministri 9 gennaio 2006, con il quale sono state individuate le predette infrastrutture ed è stata prevista l'istituzione del Centro nazionale anticrimine informatico per la protezione delle infrastrutture critiche;

Visti l'art. 14 del decreto legislativo 30 luglio 1999, n. 300, recante "Riforma dell'organizzazione del Governo, a norma dell'articolo 11 della legge 15 marzo 1997, n. 59", che attribuisce, tra l'altro, al Ministero dell'Interno competenze in materia di protezione cibernetica e sicurezza informatica nazionale, e l'art. 2001 che istituisce la Commissione interministeriale tecnica di difesa civile;

DPCM 24/01/2013
«Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale»



QUADRO STRATEGICO NAZIONALE



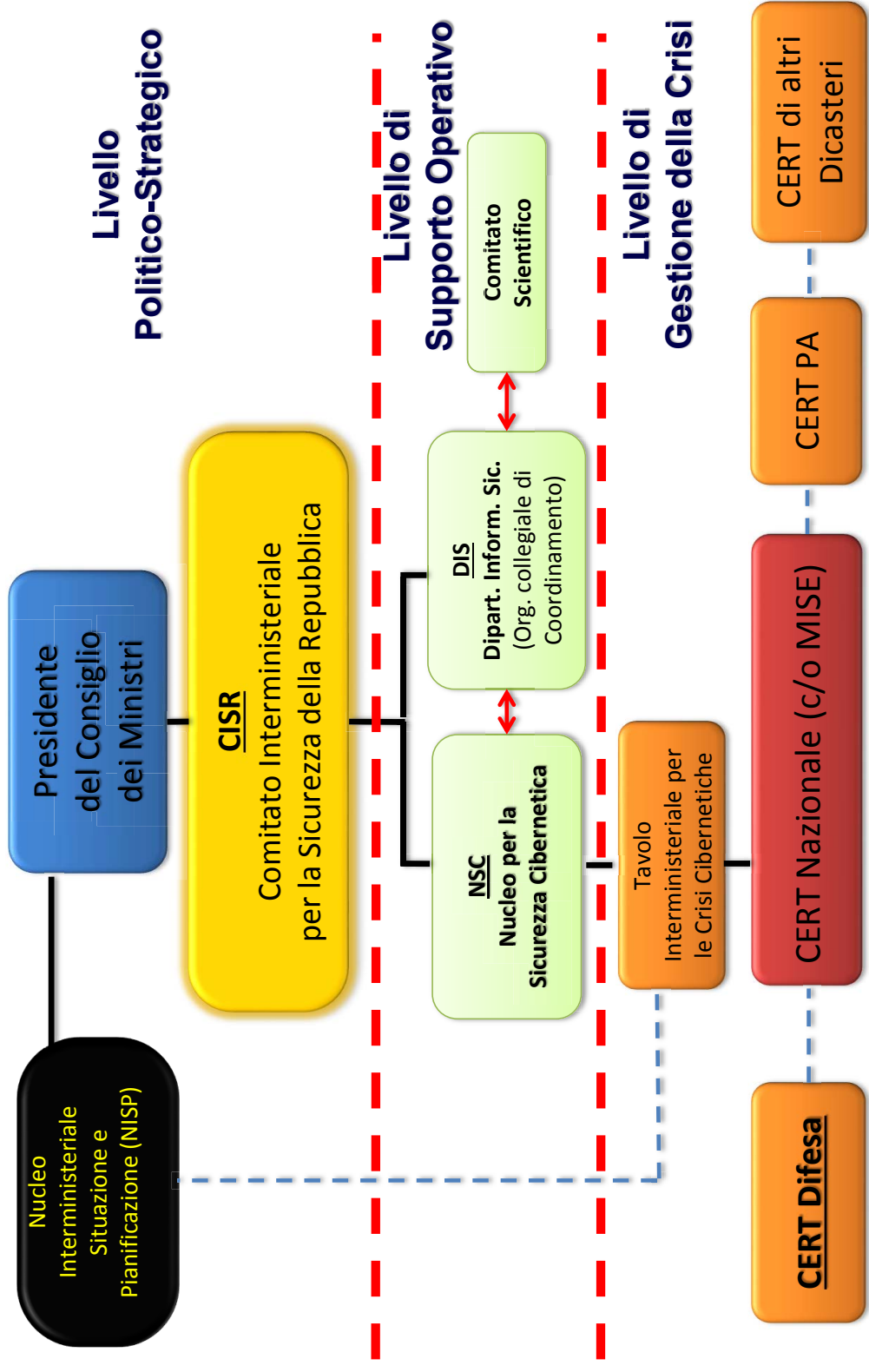
PIANO NAZIONALE



Struttura Nazionale di Difesa Cibernetica

Organizzazione Funzionale

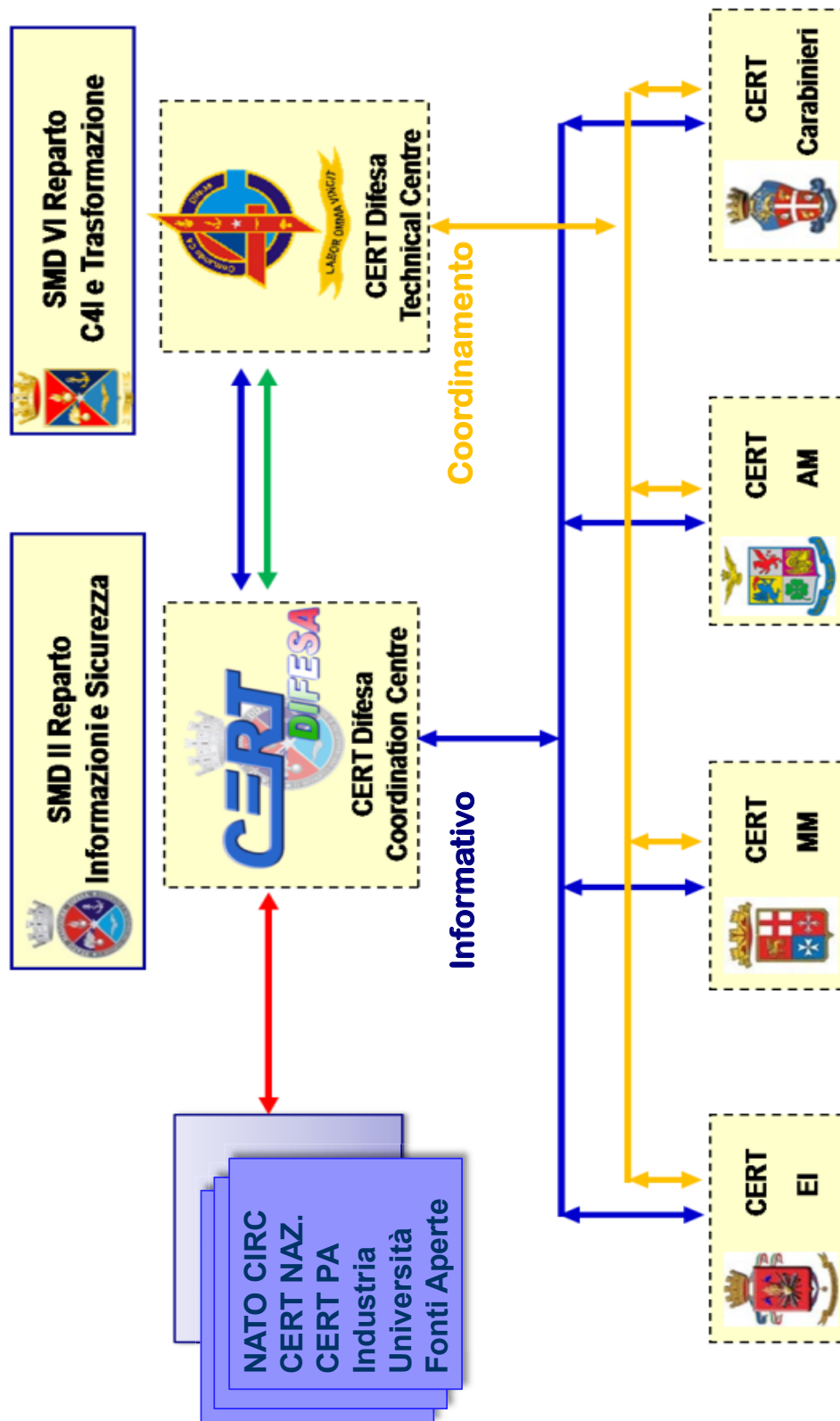
Stato Maggiore Difesa



Struttura di Cyber Defence del Comparto Difesa CERT Difesa



Stato Maggiore Difesa





Struttura di Cyber Defence del Comparto Difesa

Compiti del CERT Difesa

Stato Maggiore Difesa

Il CERT Difesa ha il compito di prevenire la minaccia cibernetica, rilevare le attività di natura malevola e reagire agli incidenti informatici

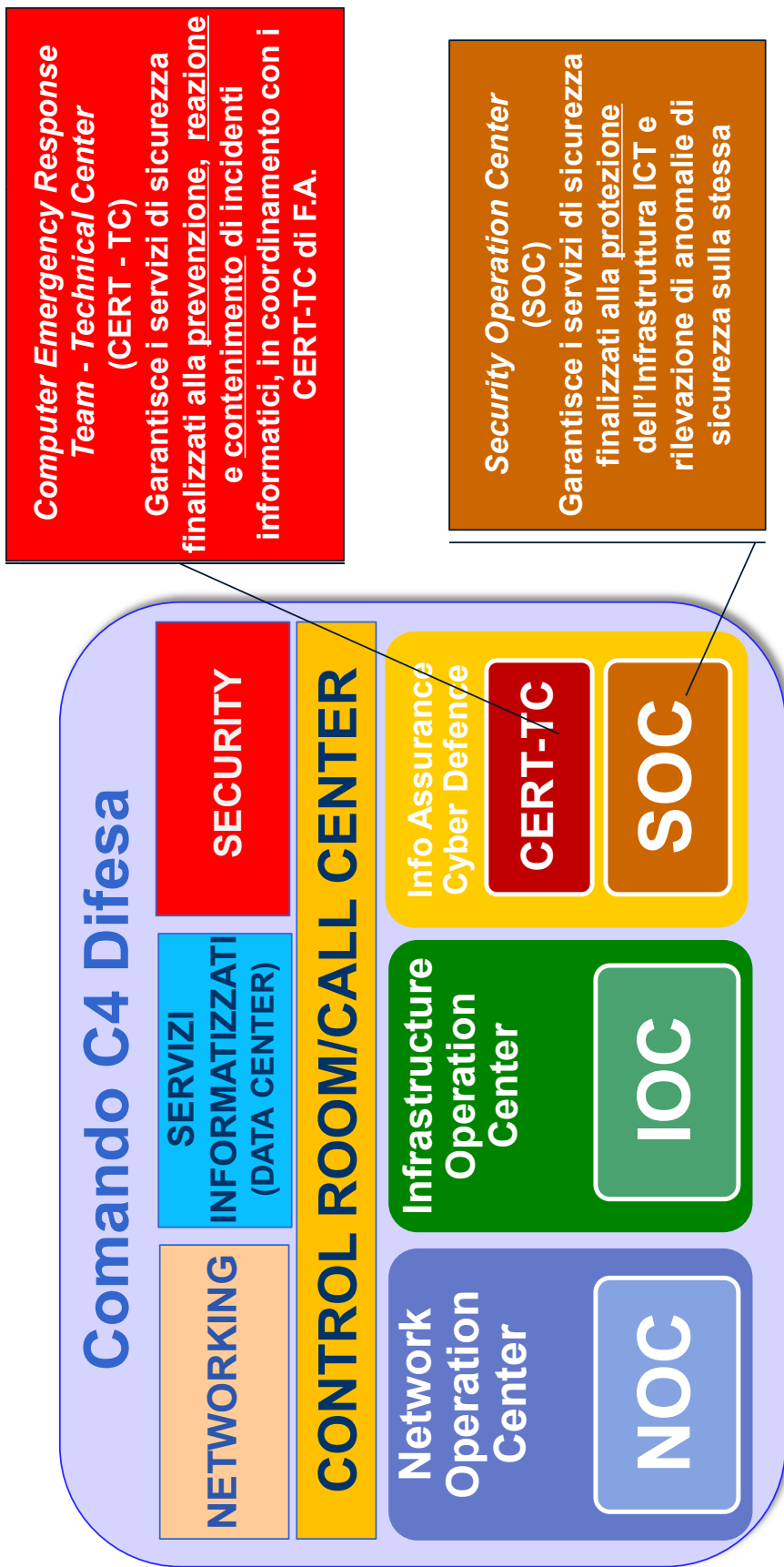
- **II CERT COORDINATION CENTRE (CERT-CC)**
 - svolge attività di informazione e di allertamento anche a scopo di prevenzione
 - collabora e condivide informazioni con i corrispondenti CERT nazionali ed internazionali
 - supporta il CERT-TC con attività di analisi in caso di evento cibernetico
- **II CERT TECHNICAL CENTRE (CERT-TC)**
 - preposto a prevenire, rilevare e contenere, sul piano tecnico-operativo, gli incidenti informatici
 - coordina e supporta l'azione dei CERT di F.A. in caso di emergenza cibernetica



Struttura di Cyber Defence del Comparto Difesa Il CERT TC nell'Organizzazione del C.do C4D

Stato Maggiore Difesa

Struttura operativa funzionale del C.do C4D





QUADRO CAPACITIVO PROGRAMMA "CYBER DEFENCE CAPABILITY"

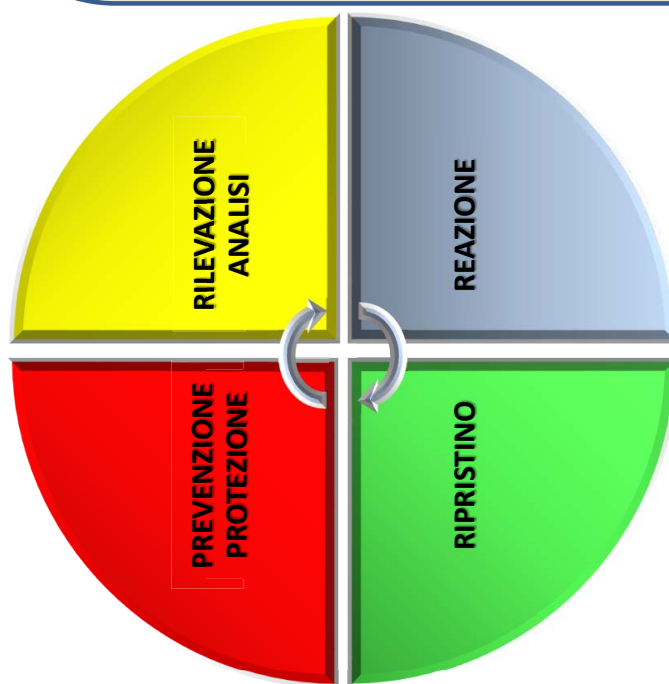
Stato Maggiore Difesa

SCOPO

Accrescere le capacità del CERT-TC di proteggere le infrastrutture ICT della Difesa (aperte ad INTERNET), da attività di natura malevola nel *dominio Cibernetico*:

- sottrazione di informazioni/dati
- compromissione della loro integrità
- negazione dei servizi,

attraverso l'acquisizione di strumenti di **Prevenzione/Protezione**, **Rilevazione/Analisi**, **Reazione** ad eventi «Cyber» e di **Ripristino** dei servizi a seguito di Incidenti Informatici

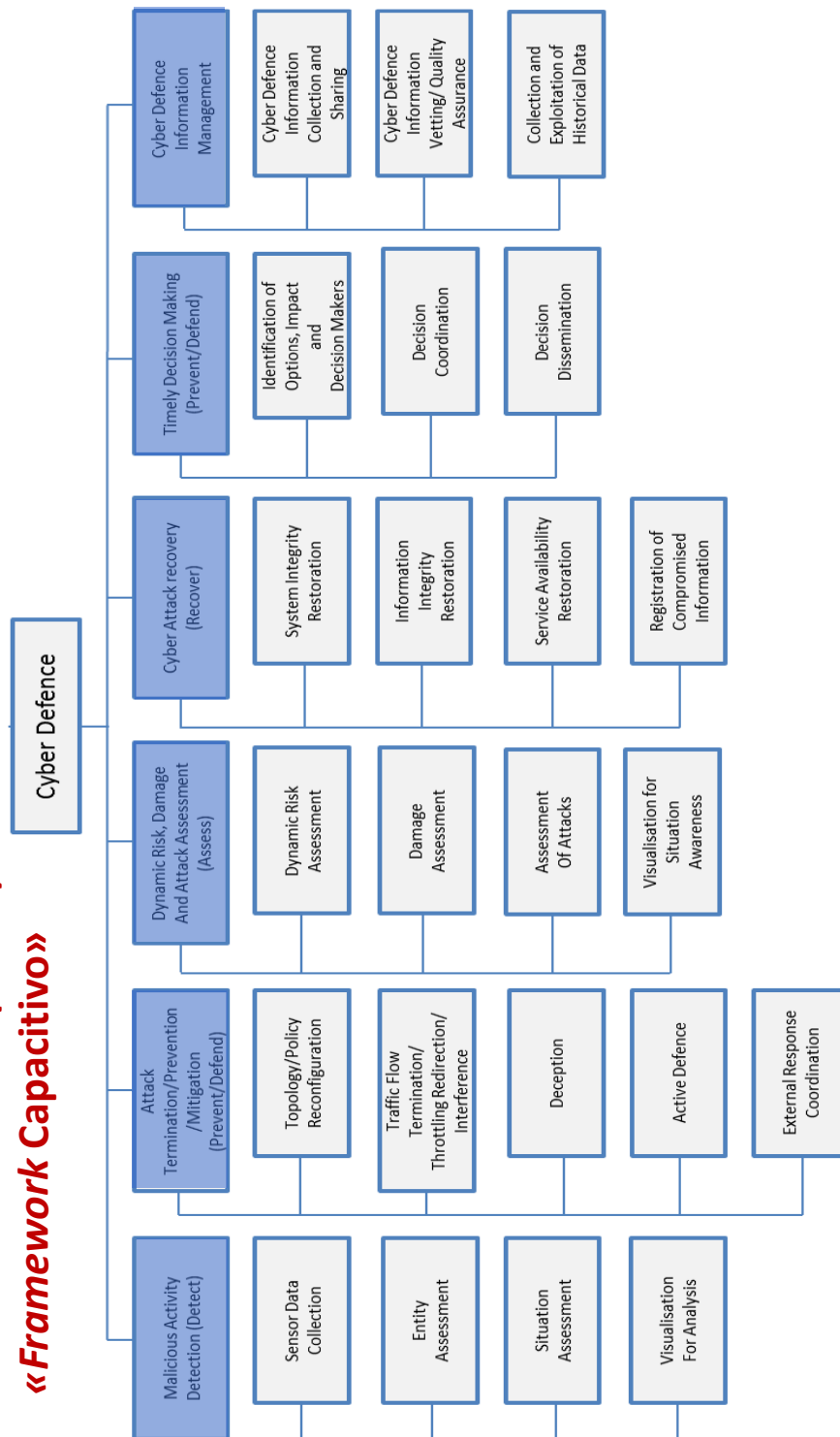




PROGRAMMA "CYBER DEFENCE CAPABILITY" Modello capacitativo di riferimento

Stato Maggiore Difesa

NATO COMPUTER INCIDENT RESPONSE CAPABILITY (NCIRC) «Framework Capacitivo»





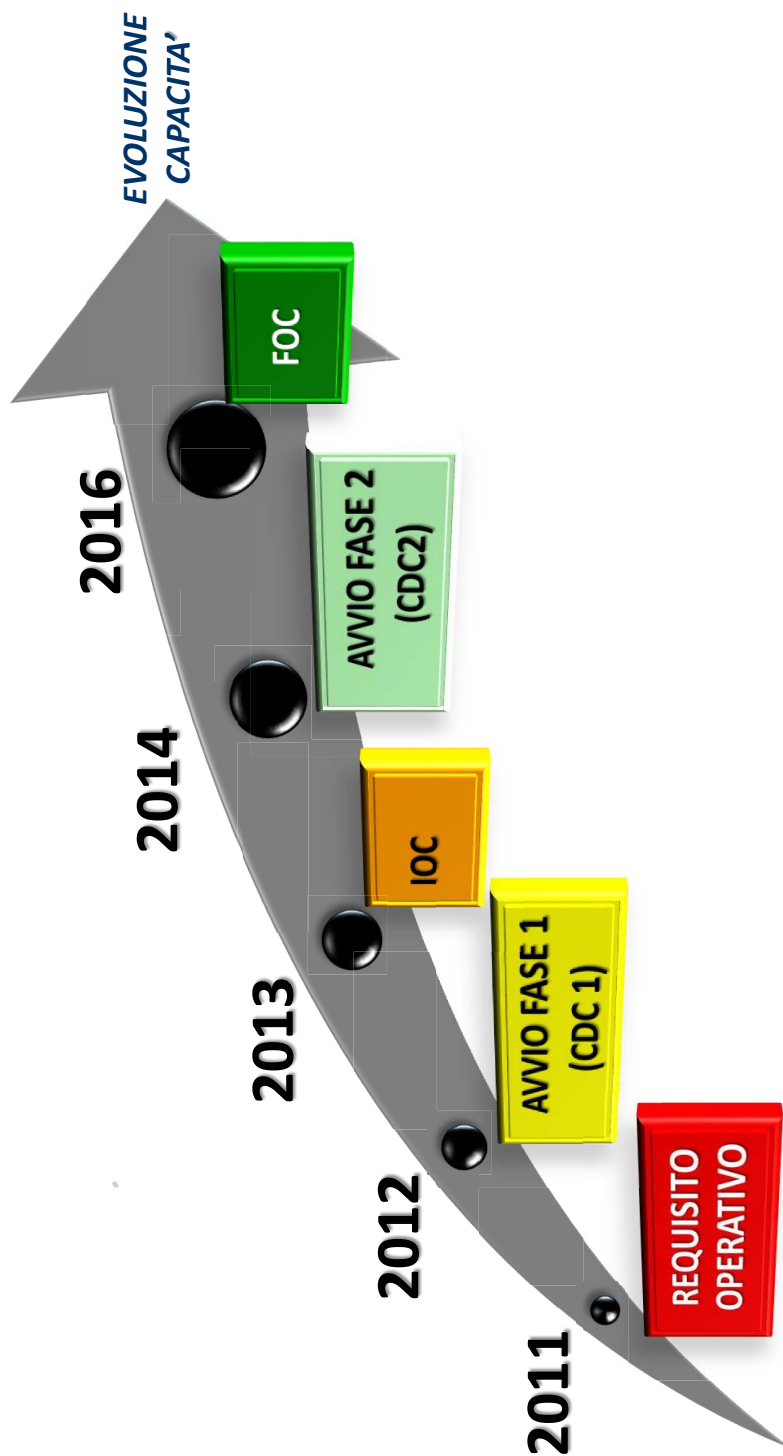
PROGRAMMA "CYBER DEFENCE CAPABILITY"

Sviluppo temporale pianificato

Stato Maggiore Difesa

FASE 1 (CDC 1) - Realizzazione di una Capacità Operativa Iniziale (IOC)

FASE 2 (CDC 2) - Conseguimento della Capacità Operativa Finale (FOC)





PROGRAMMA "CYBER DEFENCE CAPABILITY"

Situazione attuale

Stato Maggiore Difesa

- **FASE 1 (CDC 1): Capacità Operativa Iniziale di Cyber Defence (IOC)**
 - soddisfacimento dei requisiti minimi basilari per garantire una sufficiente capacità di *Cyber Defence*
 - *Control Room* con capacità di fusione dei dati e correlazione degli eventi (*Cyber Operational Picture*), operante H24/7G

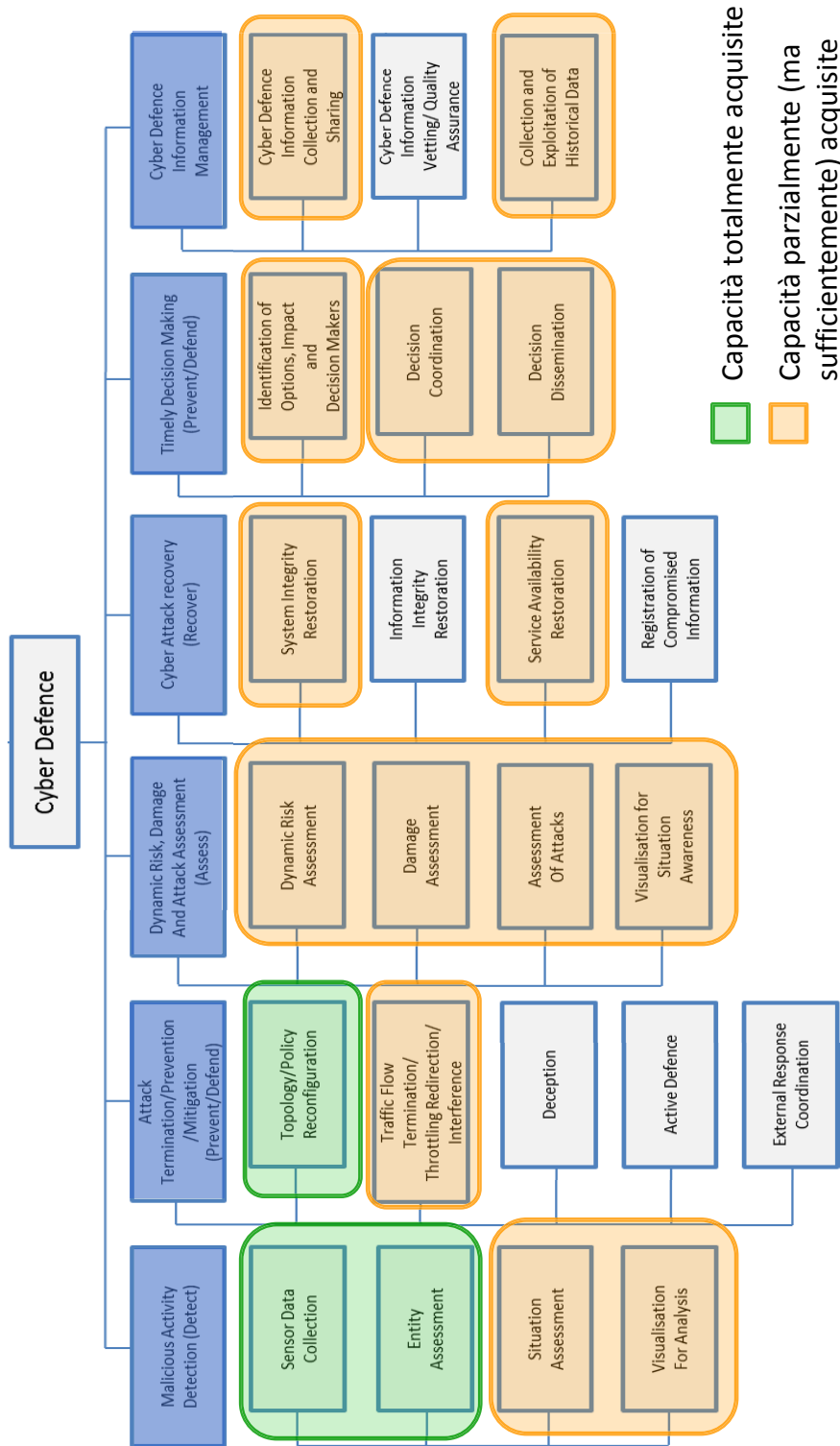
- **FASE 2 (CDC 2): Capacità Operativa Finale di Cyber Defence (FOC)**
 - **procrastinata alla luce del non favorevole quadro finanziario**
 - garantito un finanziamento parziale (Impresa «**CDC EVO**»)
 - consolidamento delle capacità acquisite
 - ulteriore potenziamento/adeguamento tecnologico delle stesse in relazione all'evoluzione della minaccia



PROGRAMMA "CYBER DEFENCE CAPABILITY" Situazione attuale (CDC 1 + CDC EVO)

Stato Maggiore Difesa

Capacità acquisite comparate al Framework Capacitivo NCIRC

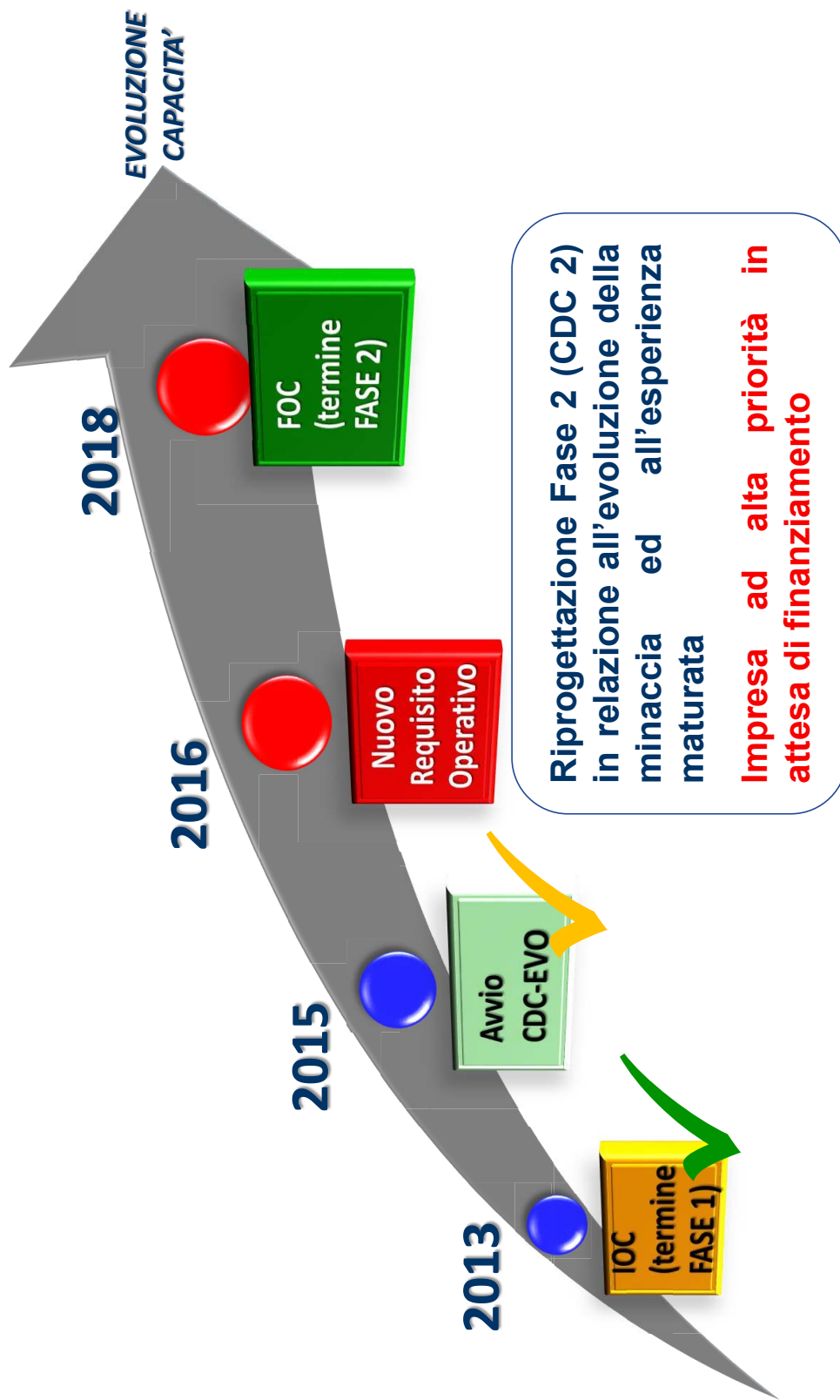




PROGRAMMA "CYBER DEFENCE CAPABILITY"

Nuovo Sviluppo temporale

Stato Maggiore Difesa





PROGRAMMA "CYBER DEFENCE CAPABILITY"

Obiettivi CDC 2

Stato Maggiore Difesa

- **Consolidamento** del livello di operatività già acquisito
- **Adeguamento** dell'attuale infrastruttura di protezione al crescente livello della minaccia
 - potenziamento/adequamento tecnologico degli strumenti/Sistemi di **Prevenzione, Protezione, Rilevamento, Analisi, Reazione e Recovery**
- **Razionalizzazione** architettuale della capacità, nell'ottica di ottimizzare i costi di mantenimento ed esercizio
- **Ulteriore irrobustimento** della protezione Cyber delle Reti classificate
- **Progetto Business WAN** (possibilità di trattare informazioni «up to R» sull'INTRANET non classificata)

**Consolidamento della
capacità acquisita**



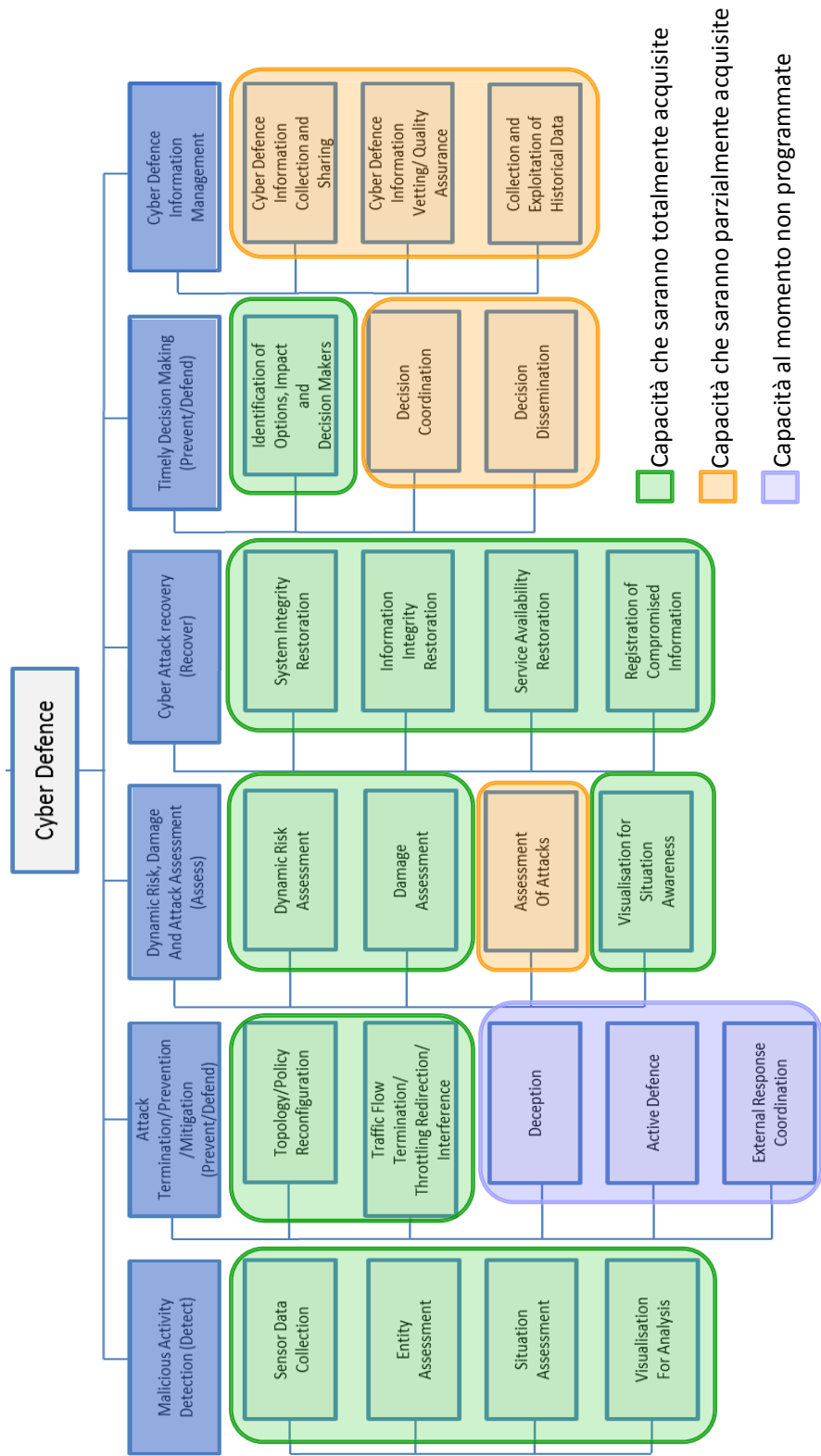
**Indispensabile
Crescita capacitativa**



PROGRAMMA "CYBER DEFENCE CAPABILITY" Capacità' Finale di Difesa (FOC)

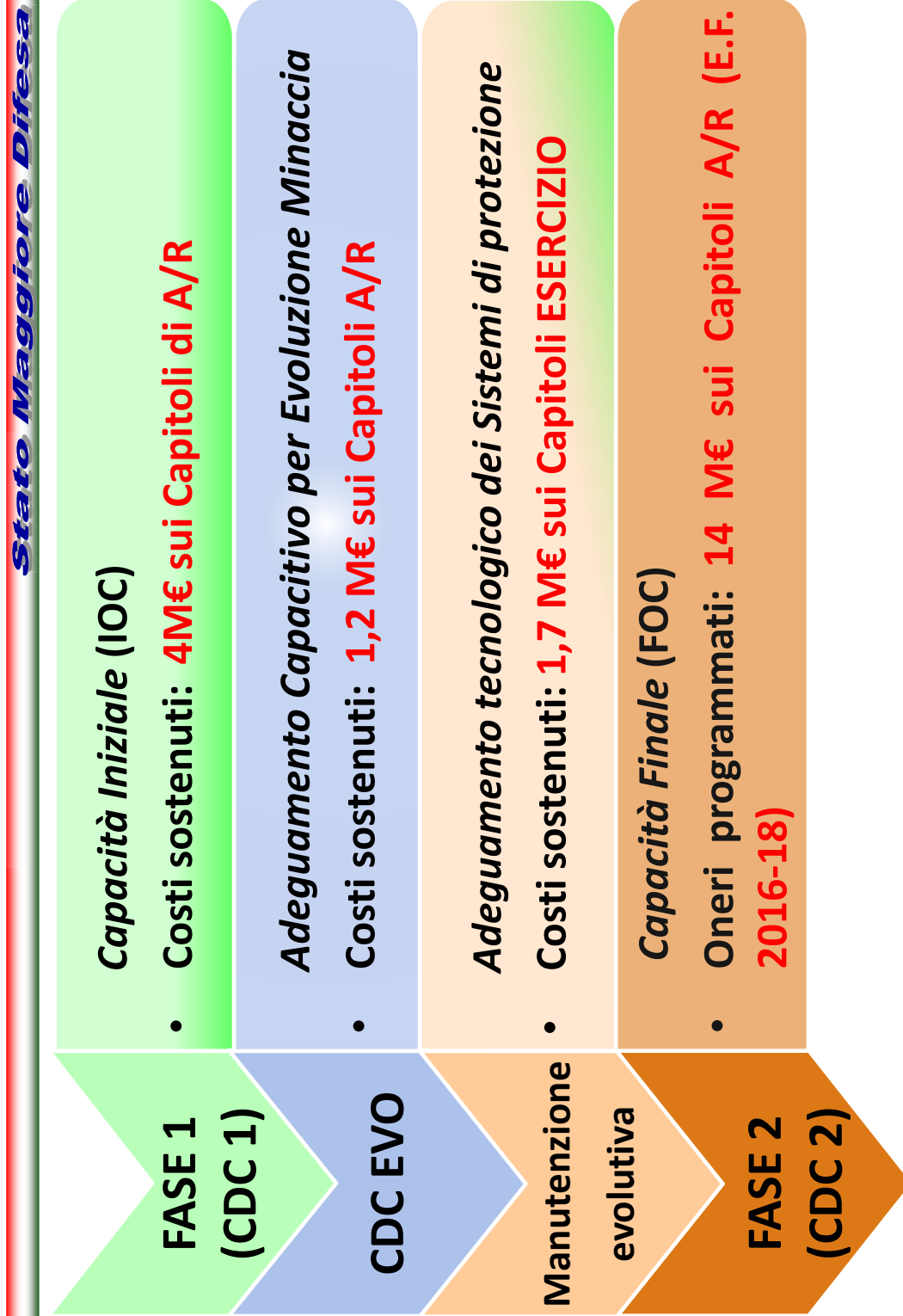
Stato Maggiore Difesa

Capacità che si conta di acquisire al termine del Programma, comparate al Framework Capacitivo NCIRC





PROGRAMMA "CYBER DEFENCE CAPABILITY" Profili finanziari





PROGRAMMA "CYBER DEFENCE CAPABILITY" Risorse Umane

Stato Maggiore Difesa

Proseguire nella crescita (quantitativa e qualitativa) degli organici delle articolazioni preposte alla *Cyber Defence*

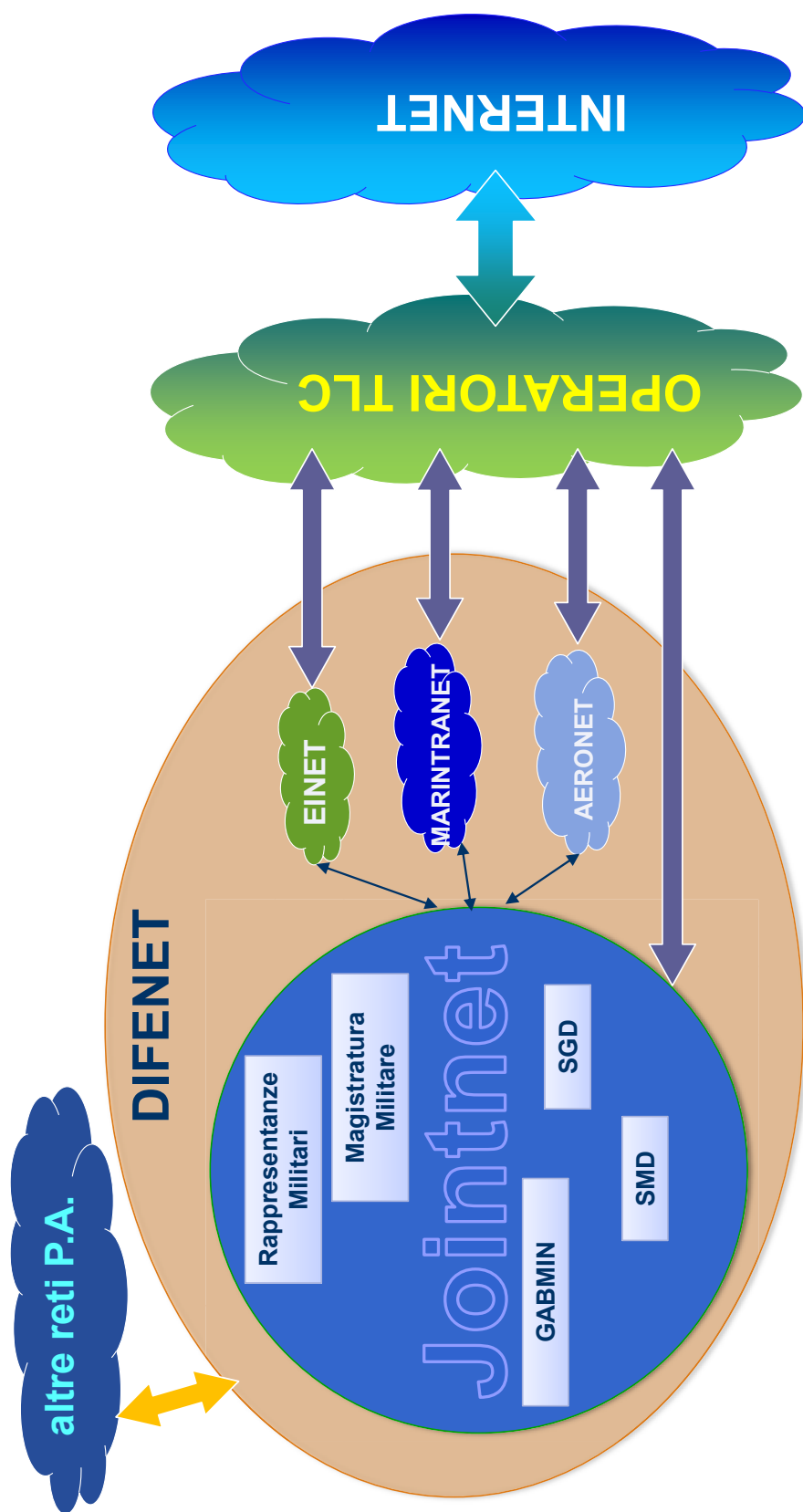
- Processo interno di **«selezione e formazione»** del personale (militare e civile), da qualificare sulla base dei nuovi **«profili d'impiego» ed «iter formativi»**
- **Assunzione diretta** di personale, civile e militare, con appropriate «qualificazioni»
- **Certificazioni specialistiche per peculiari «figure»** (*Forensic Analyst, Vulnerability Evaluator, Risk Manager, Penetration Tester, ecc.*)



**PROGETTO
"AUTONOMOUS SYSTEM – INTERNET PROVIDER INDIPENDENT"**

Stato Maggiore Difesa

Architettura di Rete – connessione ad INTERNET





PROGETTO " AUTONOMOUS SYSTEM – INTERNET PROVIDER INDIPENDENT " SCOPO

Stato Maggiore Difesa

Realizzare l'infrastruttura di accesso diretto (a larga banda e ridondata) al «Big INTERNET», unico per l'intero Comparto

Il Comando C4 Difesa, connesso ai due principali Nodi di accesso nazionale al «Big INTERNET» (NAMEX di Roma e MIX di Milano), assume il ruolo di **INTERNET SERVICE PROVIDER**

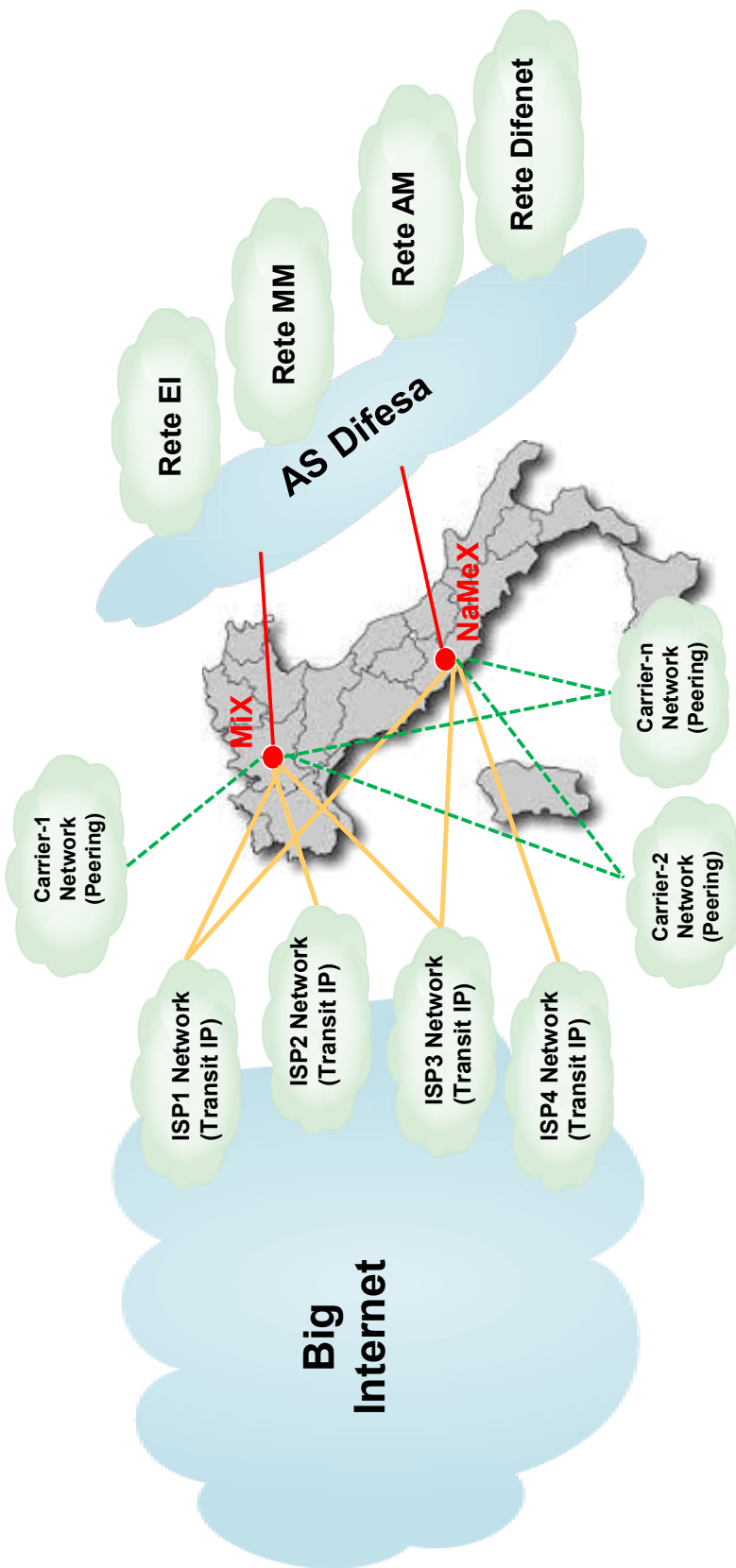
- **Vantaggi**
 - Unitarietà di Comando e Controllo nelle attività di difesa cibernetica
 - Concentrazione della capacità di Cyber Defence su un unico «fronte»
 - Riduzione dei costi di gestione con una migliore qualità del servizio
- **Tempistiche** (progettazione già completata)
 - Entro 2016 - attivazione del servizio per l'Area di Vertice Interforze
 - Entro 2017 - estensione del servizio anche alle F.A.
- **Oneri finanziari**
 - 2,7M€, con profilo pluriennale (E.F. 2016 -18)

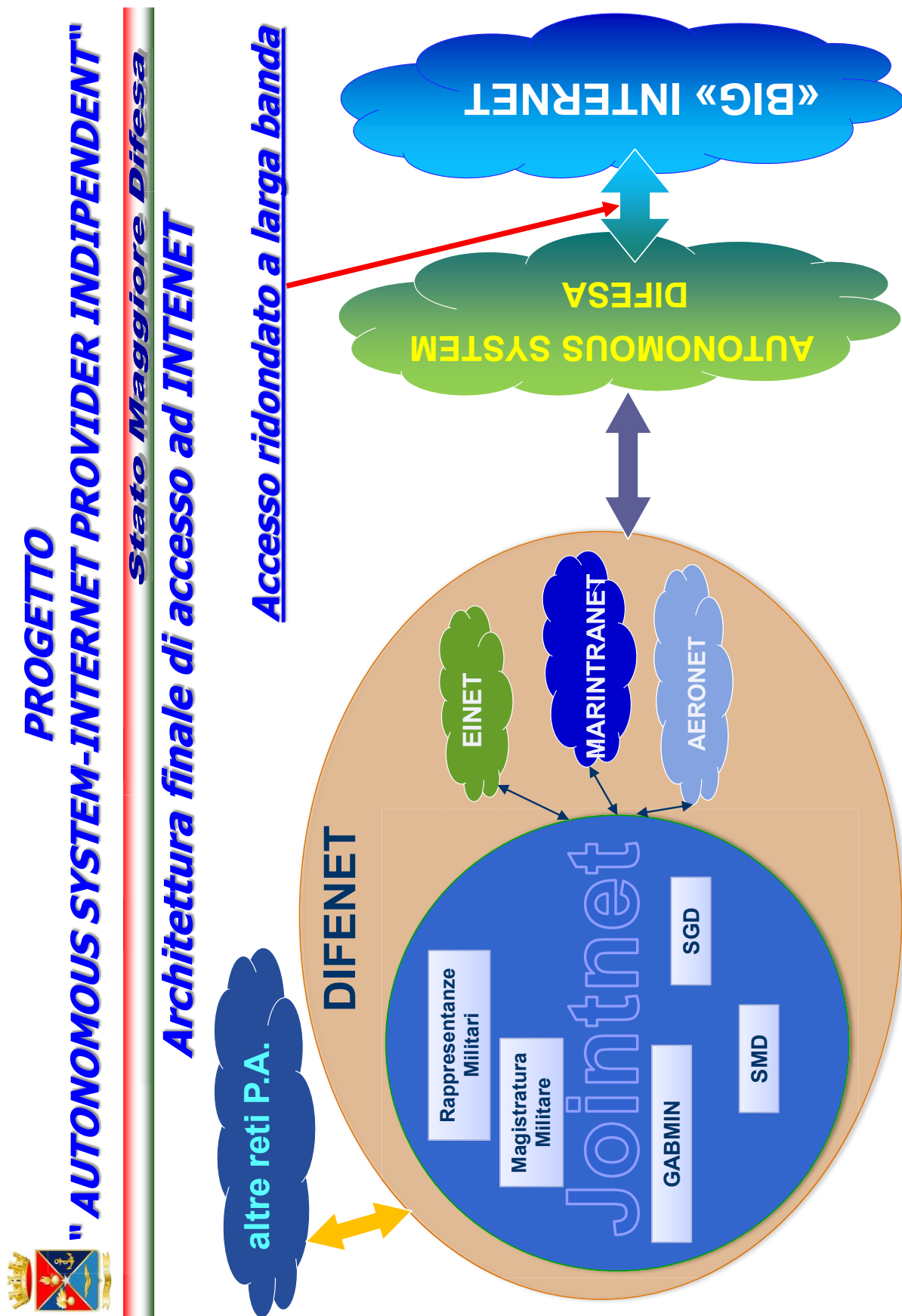


**PROGETTO
"AUTONOMOUS SYSTEM - INTERNET PROVIDER INDEPENDENT"**

Stato Maggiore Difesa

SCHEMA CONNESSIONE AL «BIG INTERNET»





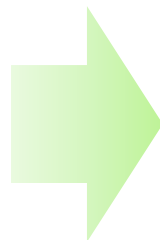


BUSINESS CONTINUITY & DISASTER RECOVERY

Definizione

Stato Maggiore Difesa

Le funzioni di **Business Continuity** e **Disaster Recovery** costituiscono la capacità dell'Infrastruttura ICT di garantire l'erogazione dei servizi istituzionali pur a fronte di eventi disastrosi (anche di natura malevola)



Ciò deve tradursi in un processo di riorganizzazione di tutti i **Data Center** in un ambiente di **Private Cloud**, predisposto per garantire la «**resilienza**» necessaria ad evitare soluzioni di continuità nella disponibilità dei Servizi



BUSINESS CONTINUITY & DISASTER RECOVERY

Fasi del progetto

Stato Maggiore Difesa

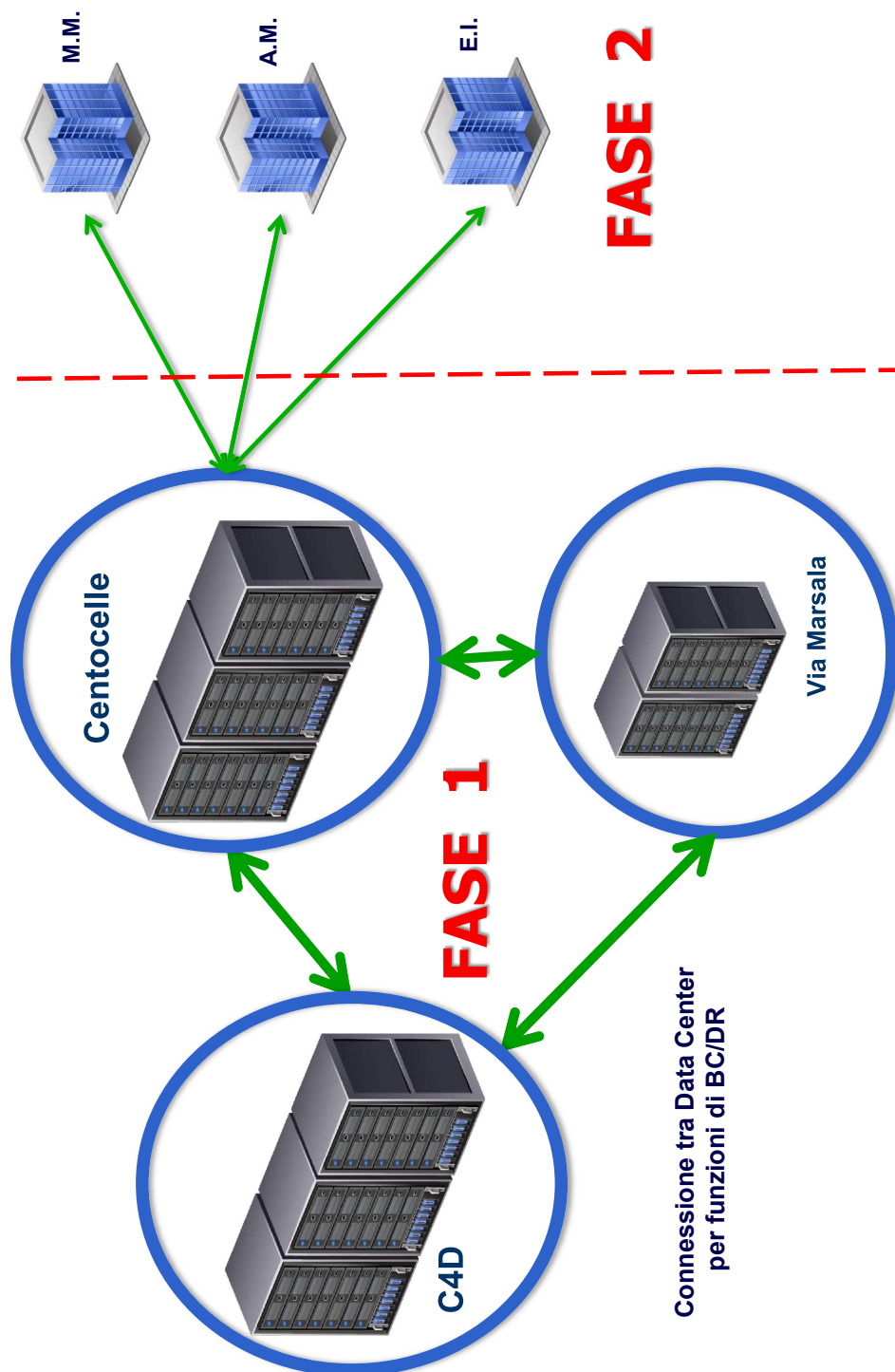
Il Piano articolato in due fasi

- **FASE 1** (già definita in un Progetto, in corso di avvio)
 - **Razionalizzazione e consolidamento** dei Data Center dell'Area Interforze (T/O e T/A), da concentrare sul C.do C4 Difesa, Comparto «A» di Centocelle e sito di Via Marsala
 - **Implementazione della tecnologia di *Private Cloud*** nei suddetti CED, con **funzioni di BC e DR reciproco**
 - **Oneri finanziari: già garantiti per 4 M€, con profilo pluriennale (2016-18)**
- **FASE 2**
 - **Razionalizzazione e convergenza** dei Data Center delle F.A. nel *Private Cloud* unico Difesa e condivisione allargata alle F.A. delle funzioni di BC e DR
 - **Reingegnerizzazione dei Servizi legacy** per poter essere ospitati nella nuova Infrastruttura «Cloud»
 - **Oneri finanziari: circa 10 M€, con profilo pluriennale (2018-20)**

BUSINESS CONTINUITY & DISASTER RECOVERY

Fasi del progetto (rappresentazione grafica)

Stato Maggiore Difesa





RETE INTERMINISTERIALE DI GESTIONE DELLE CRISI CIBERNETICHE

Stato Maggiore Difesa

Costituire una Rete protetta fra la PCM ed i Dicasteri/Organismi partecipanti al *Nucleo di Sicurezza Cibernetica*, finalizzata a garantire lo scambio di informazioni in situazione di crisi cibernetica

- **Studio di fattibilità richiesto alla Difesa**
 - Disponibilità di una rete di trasporto proprietaria (DIFENET)
 - Maggiore esperienza nella gestione di reti classificate
- **Soluzione ipotizzata**
 - Realizzazione dei Nodi di erogazione dei servizi presso i Data Center Difesa
 - Utilizzo della connettività DIFENET per i Dicasteri/Organismi già raggiunti da tale Rete
 - Completamento della connettività mediante *leasing* di circuiti dedicati
 - Oneri previsti per l'Impresa: **3 M€ + 350K€ annui di «Esercizio»**
- **Modalità di finanziamento, procedure di acquisizione e struttura di Governance** in corso di definizione a cura della PCM
- Possibile evoluzione futura quale **Rete Gestione Crisi Nazionale**

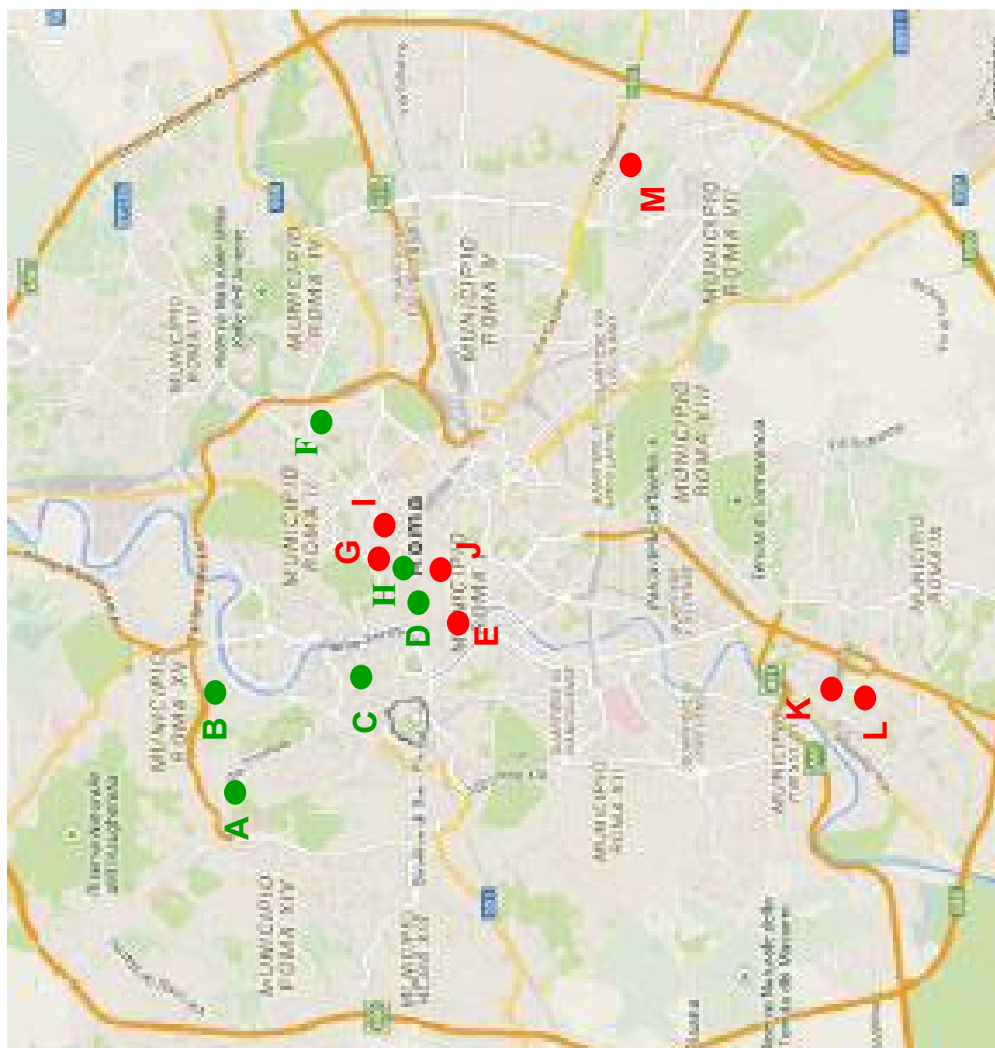


RETE INTERMINISTERIALE DI GESTIONE DELLE CRISI CIBERNETICHE

Stato Maggiore Difesa

Distribuzione geografica

- Siti non raggiunti dalla rete della Difesa
- Siti raggiunti dalla rete della Difesa

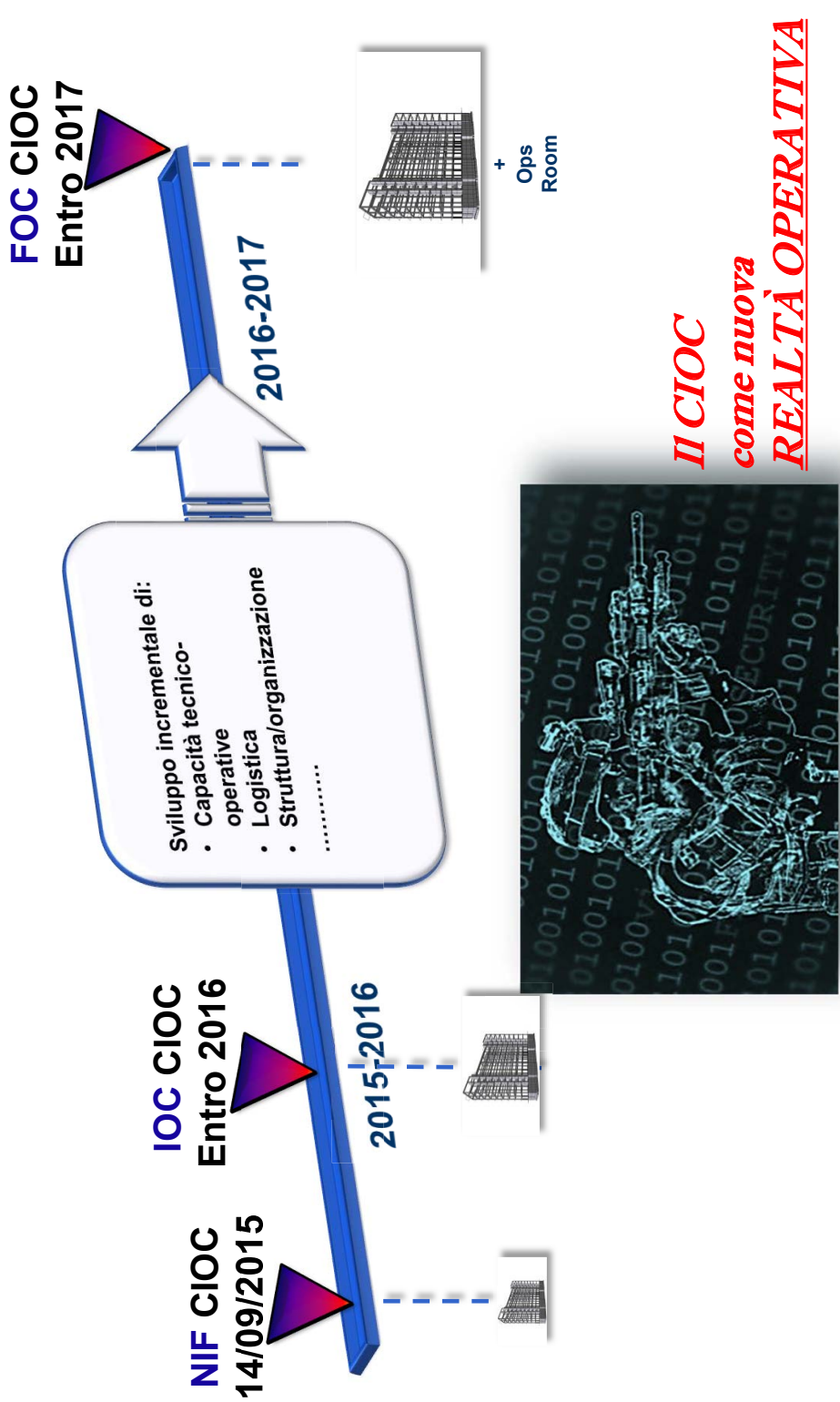


A.	C4D - CERT TC
B.	MAECI
C.	CERT CC
D.	PCM
E.	MIN. GIUSTIZIA
F.	CG G.d.F.
G.	MISE
H.	MIN. DIFESA
I.	MEF
J.	MININTERNO
K.	CERT-PA
L.	MISE CERT-Naz
M.	CNAIPIC



COMANDO INTERFORZE OP. CIBERNETICHE Costituzione del Comando - Sviluppo temporale

Stato Maggiore Difesa



STATO MAGGIORE DIFESA



DOMINIO CIBERNETICO PROSPETTIVE PER LO STRUMENTO MILITARE

9 marzo 2016

Sommario

STATO MAGGIORE DIFESA

- Premessa
- Attività militari nel cyberspace
- Aspetti organizzativi
- Punto di situazione
- Conclusioni

9 marzo 2016

STATO MAGGIORE DIFESA

DOMINIO CIBERNETICO

-

PREMESSA

9 marzo 2016

Premessa - Spettro di capacità Cyber

STATO MAGGIORE DIFESA

Computer Network Operations

- Computer Network Defense
- Computer Network Exploitation
- Computer Network Attack

Information Assurance (IA)

Cyber Defense (CD)

CNE

CND

CNA

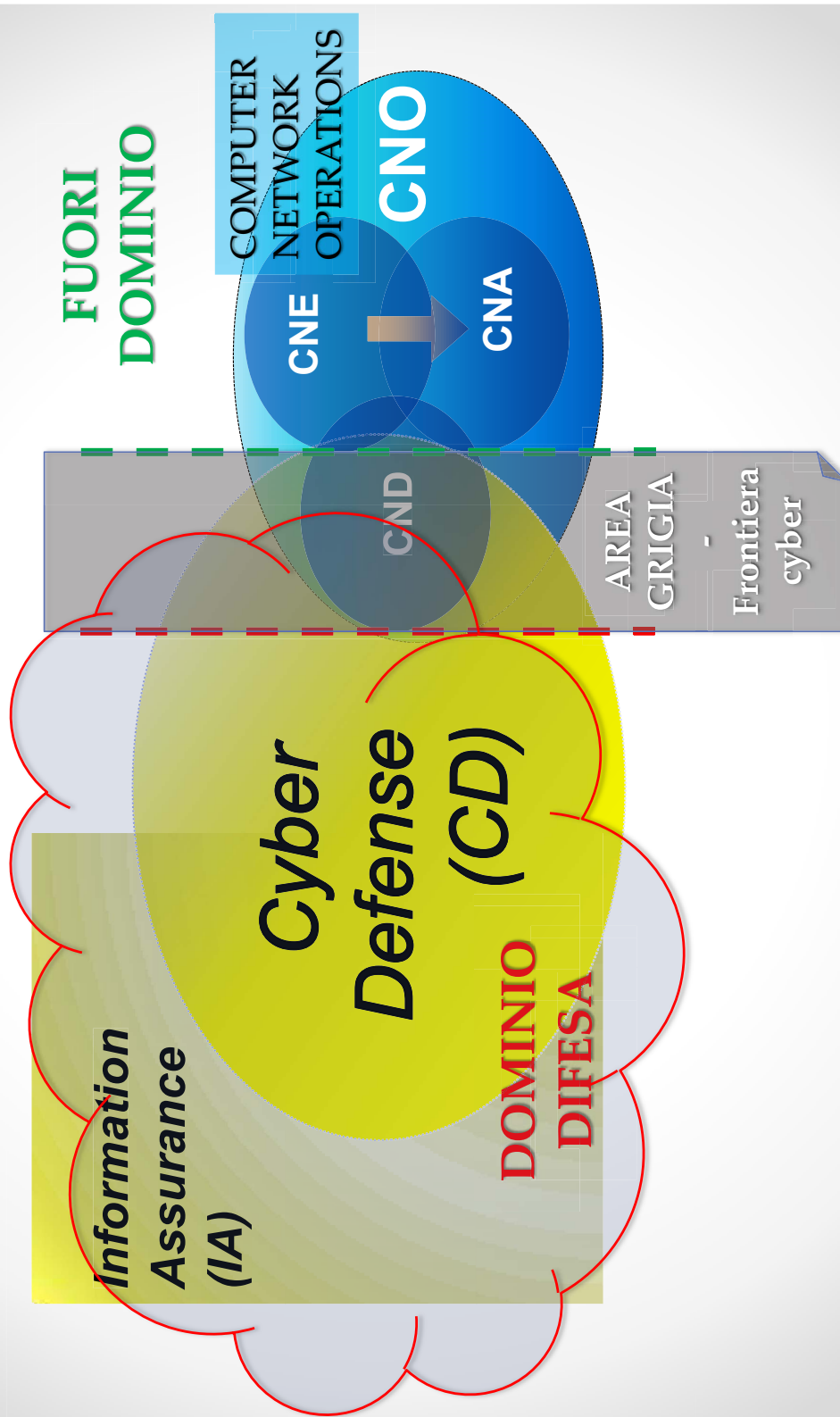
CNO

Policy, misure, prevenzione, protezione, difesa, operazioni

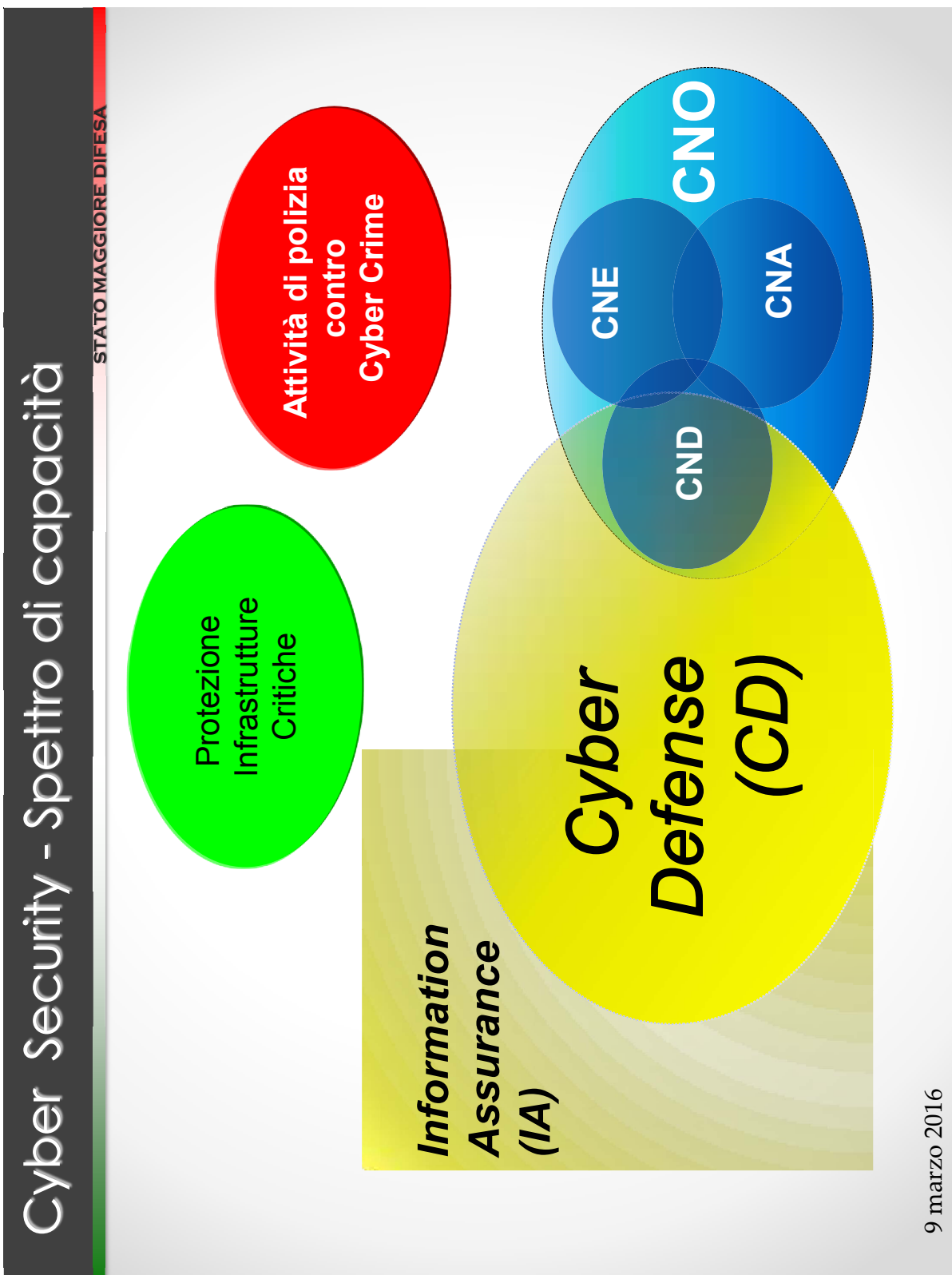
9 marzo 2016

Aree di applicazione - capacità Cyber

STATO MAGGIORE DIFESA



9 marzo 2016



Piano del conflitto cibernetico

STATO MAGGIORE DIFESA

CNO alleate



Cyber
warfare



Cyber Defense

Cyber crime



Hactivism

CNO avversarie



Considerazioni

STATO MAGGIORE DIFESA

- Ambiente cyber cresciuto a "macchia di leopardo",
- In Italia limitata "sensibilità" alle materie di sicurezza informatica e cyberspace non ha agevolato la creazione di capacità concrete ed una relativa *governance*
- Sulla scena internazionale pochi realmente competenti hanno sviluppato in casa delle capacità *effettive* che non vengono condivise (caso Snowden...)
- Limitate risorse nazionali non utilizzate secondo un piano/razionale condiviso/coordinato

9 marzo 2016

STATO MAGGIORE DIFESA

DOMINIO CIBERNETICO
-
**ATTIVITA' MILITARI
NEL CYBERSPACE**

9 marzo 2016

Cyberspace: nuovo dominio operativo

STATO MAGGIORE DIFESA

- Dimensione artificiale creata dall'uomo

- Layer fisico
- Layer logico
- Layer cognitivo



- Caratteristiche

- Dominio a se stante, ma anche trasversale ai domini tradizionali
- Assenza di confini geografici
- Compressione della dimensione temporale
- Problematiche di identificazione e attribuzione
 - "Plausible deniability"



Cyberspace come dominio

STATO MAGGIORE DIFESA

- Semplificando, l'informatica è percepita come evoluzione della macchina da scrivere (office) e della corrispondenza cartacea (email), oltre che passatempo
- In realtà, il processo di digitalizzazione continua, ha stravolto le metodologie di vita e di lavoro.
- Anche lo strumento militare si sta trasformando con l'interconnessione di tutti gli assetti e sistemi d'arma in rete:
 - ha reso più efficiente l'impiego degli stessi assetti consentendone il controllo (anche da remoto) in tempo reale
 - offre opportunità all'avversario di sfruttare la nuova dimensione per incidere o inibire l'impiego degli stessi assetti
- Analogamente il nostro strumento militare può avvalersi del cyberspace contro la capacità di impiego degli assetti dell'avversario (come vera e propria arma)

9 marzo 2016

Computer come Sistema d'Arma

STATO MAGGIORE DIFESA

- **Il mezzo non fa la differenza: è come lo si usa**
 - Una pistola può essere usata per difesa, per costringere qualcuno a rivelare informazioni, o per uccidere
- **Sistema d'arma: nell'ottica che il computer utilizzato per CNO deve essere distinto (in termini di impiego) dal computer che è strumento di lavoro quotidiano**
- **Il vantaggio del cyberspace è che in assenza di confini posso condurre l'operazione "da casa" con accorgimenti speciali (anonimato, ecc.) senza dover rischiare assetti o quant'altro.**
- **Occorre percepire/interpretare la dimensione della problematica cyber:**
 - **tendenza comune: evento malevolo = reato** (..di violazione della **privacy**)
 - lo strumento militare può già **operare nel cyberspace** in analogia agli altri domini (*Transfer of Authority, Rules of Engagement, SPINS*)
 - **L'intelligence** deve saper sfruttare le opportunità offerte dalla nuova dimensione in **analogia** a quanto viene fatto **ambito SIGINT/HUMINT**

9 marzo 2016

Analogie con gli altri domini


STATO MAGGIORE DIFESA

Domini tradizionali	Capacità nel cyberspace
Sicurezza e Protezione delle installazioni	Cyber Defense (CD)
Scorta armata ad un convoglio	Computer Network Defense (CND)
Intelligence, Surveillance, Reconnaissance (ISR) • Assetti COMINT / SIGINT	Cyber Intelligence • Computer Network Exploitation (CNE)
Produzione di effetti tangibili (es. <i>Suppression of Enemy Air Defense</i>)	Computer Network Attack (CNA)

9 marzo 2016

Dimensione cyber della Difesa

STATO MAGGIORE DIFESA

- **Cyber Defense** **CD**
 - Comparto Difesa ≡ ogni organizzazione o istituzione:
 - **Protegge** i propri *Communication and Information Systems (CIS)* per **garantire il funzionamento** dello strumento militare
- **Computer Network Operations (Cyber OPS)** 
 - **Difesa Attiva** -> Contrasto dell'offesa da parte dell'avversario
 - Concorso alla salvaguardia delle libere istituzioni
 - Concorso alla protezione delle infrastrutture critiche
 - Concorso al contrasto del cyber crime
 - **Intelligence** -> Sfruttamento del cyberspace quale:
 - dimensione dalla quale attingere ad intelligence a tutto tondo (Cyberspace come "**banca dati**")
 - dominio operativo dell'avversario sulle cui capacità occorre fare intelligence per supportare le nostre *cyber operations* (**ordine di battaglia cyber**)
 - **Offesa** -> Prevedere l'impiego di **capacità offensive** in modalità **proporzionale e controllata** in supporto delle operazioni militari (solo nell'ambito di una coalizione e/o in risposta ad una situazione di crisi)
 - Soft, Hard, Controllo dei danni collaterali

9 marzo 2016

STATO MAGGIORE DIFESA

DOMINIO CIBERNETICO
-
ASPETTI ORGANIZZATIVI

9 marzo 2016

Riferimenti principali

STATO MAGGIORE DIFESA

STRATEGICI:

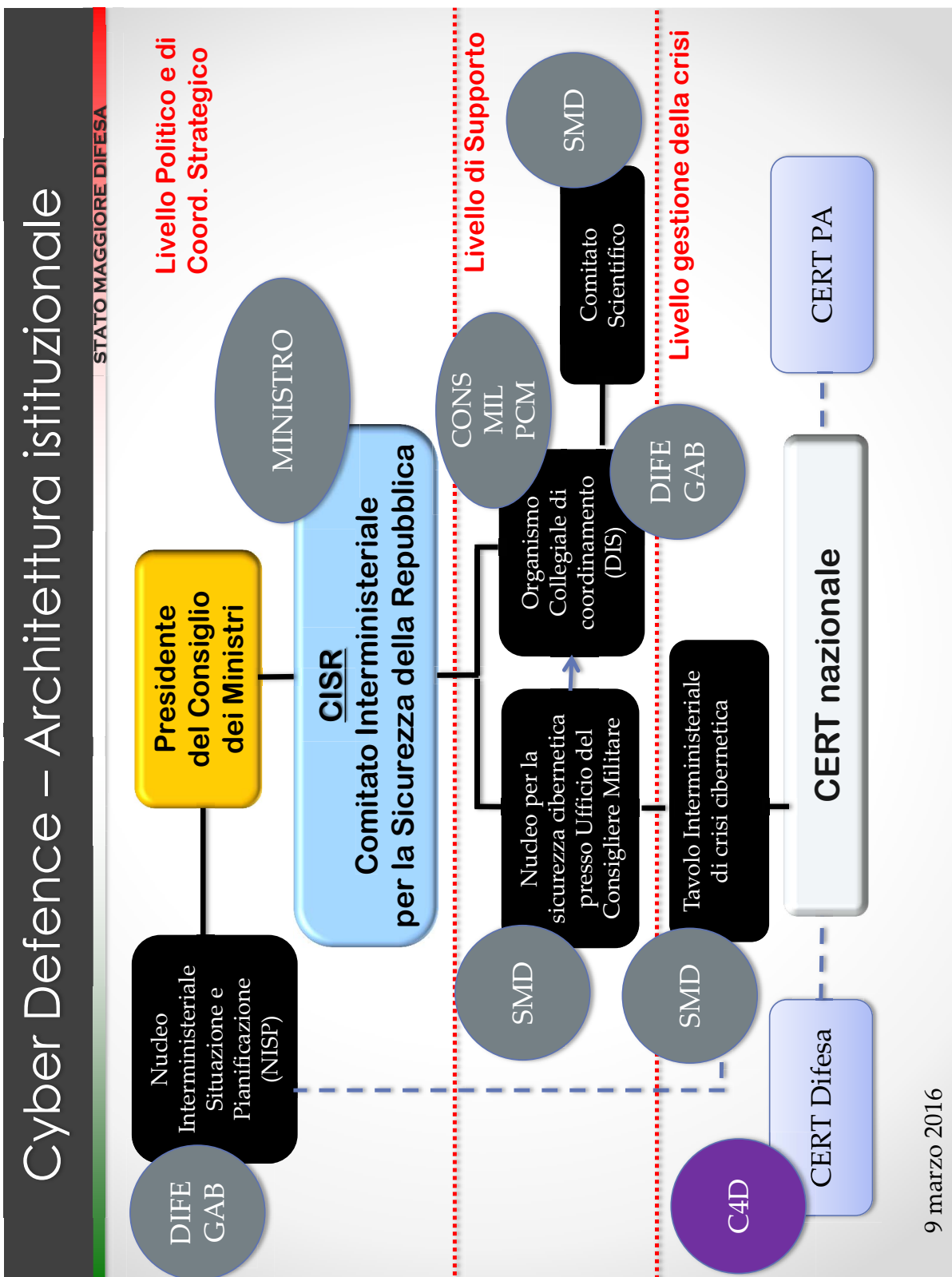
- **DPCM 24 gennaio 2013** "Decreto del Presidente del Consiglio dei Ministri 24 gennaio 2013 - Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale."
- **Piano Nazionale** per la Protezione Cibernetica e la Sicurezza Informatica
- **Quadro Strategico Nazionale Cyber** per la Sicurezza dello Spazio Cibernetico

La NATO **NON** può essere riferimento per CNA e CNE

DIFESA:

- **JIC-011** *Joint Integrating Concept* - Computer Network Operations ed. 2009
- **SMD-G-032** - "Direttiva Interforze di Policy sull'Ambiente Cibernetico" ed.2012
- **JIC-012** *Joint Integrating Concept* "Le attività militari nello spazio cibernetico (la Cyber-Warfare)" ed. 2014

9 marzo 2016

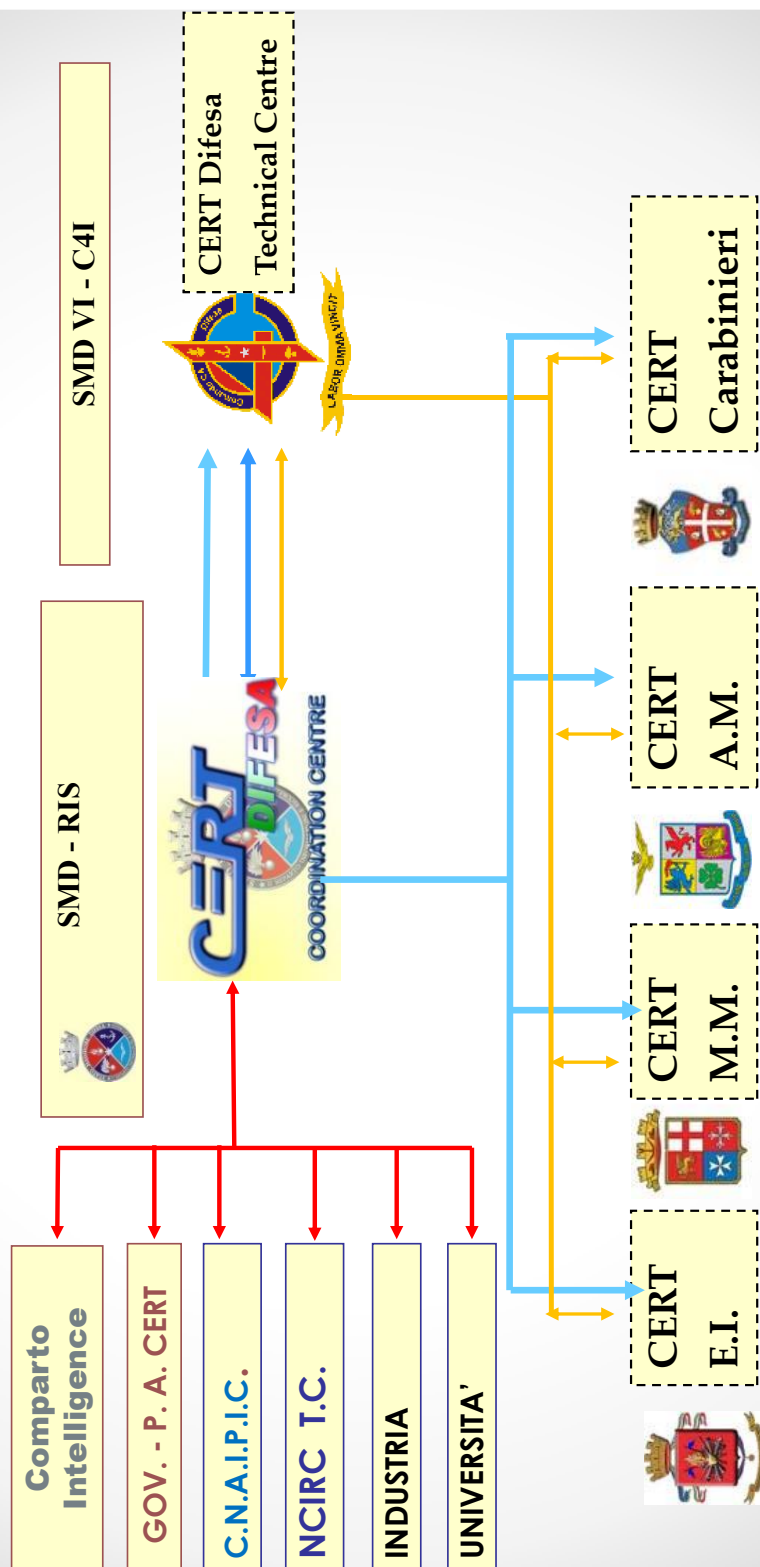


9 marzo 2016

Governance attuale sicurezza

STATO MAGGIORE DIFESA

Computer Emergency Response Team (CERT) – organizzazione deputata a fornire risposta in caso di incidente informatico

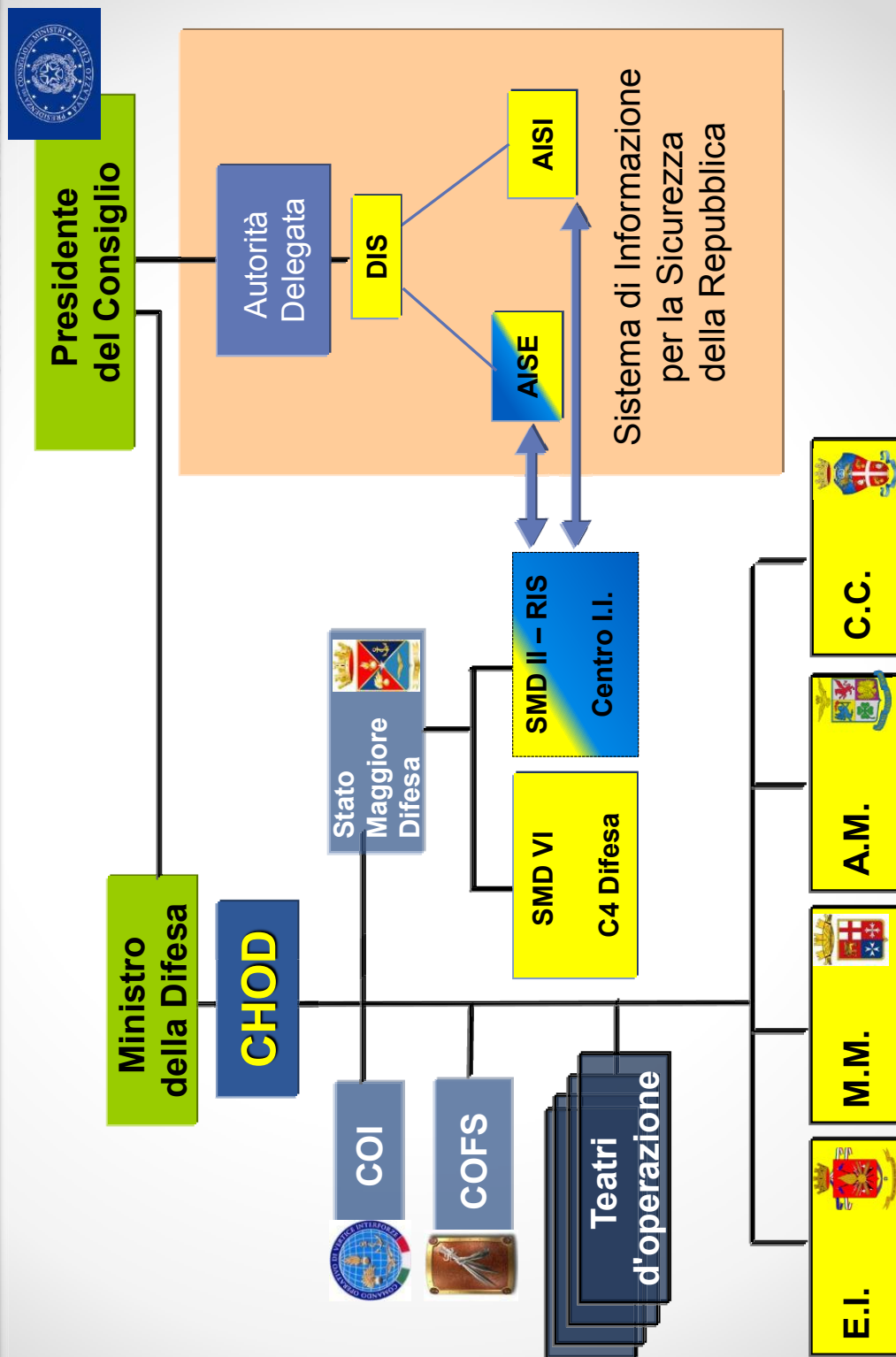


Suddivisione funzionale in analogia a quanto avviene per la NATO

9 marzo 2016

Competenze cyber – situazione attuale

STATO MAGGIORE DIFESA



9 marzo 2016

Organizzazioni nazionali attuali

STATO MAGGIORE DIFESA

Ministero della Difesa



Ministero dell'Interno



CNAIPIC



Polizia postale
delle telecomunicazioni

9 marzo 2016

Considerazioni

STATO MAGGIORE DIFESA

- Questione cyber come una problematica di gestione e sicurezza dei sistemi e delle reti
- Principio fondamentale è che organizzazione gestione dominio Cyber si basa su [2 pilastri](#):
 - **Protezione** sistemi/reti per garantire funzionamento
 - Dimensione **Operazioni** militari per agire/contrastare avversario
- **Computer Network Operations (CNO)** sono **altamente sensibili**: Know-how viene gelosamente custodito e deve essere sviluppato autonomamente
- **Percorsi formativi** devono essere sviluppati in proprio:
 - percorso formativo interno pienamente operativo, ma le **tempistiche** associate alla formazione di personale realmente competente sono lunghe

9 marzo 2016

STATO MAGGIORE DIFESA

DOMINIO CIBERNETICO

-

PUNTO DI SITUAZIONE E CONCLUSIONI

9 marzo 2016

Attività svolte

STATO MAGGIORE DIFESA

- **Sviluppato percorso formativo** altamente specialistico interno (già attivo)
- Implementata capacità iniziale di **cyber lab CNO**
- Condotta **attività esercitativa** specialistica
- **Acquisita capacità pronto intervento, analisi e risposta** in caso di eventi malevoli di rilievo
- Impostati programmi di **acquisizione sistemi** di supporto
- Avviata formazione cyber presso istituti di formazione di base delle Forze Armate (dopo reclutamento), da intensificare progressivamente

9 marzo 2016

Formazione specialistica CNO

STATO MAGGIORE DIFESA

Periodicità	Corso	Capacità
2 / anno	Acquisizione forense Preservazione evidenze digitali	First response agli incidenti informatici
1 / anno	Analisi forense Ricostruzione delle attività perpetrate dall'avversario	Intelligence, risposta agli incidenti informatici, sviluppo tecniche operative
1 / anno	Penetration testing Sviluppo attività offensive contro sistemi e reti in maniera controllata	Active Defense / Incremento sicurezza
1 / anno	Web exploitation Sfruttamento informativo di siti e altre risorse esposte nel web	Capacità di procurare intelligence da server web e basi dati di supporto
1 / anno	Reverse engineering Reingegnerizzazione/ ricostruzione del codice software	Analisi del software malevolo, studio delle modalità operative avversarie, intelligence
2016	Advanced exploitation (pilot) Cyber Intelligence Avanzata	Sviluppo operazioni di cyber intelligence (con malware)

I nomi comuni sono stati lasciati per ragioni di classifica dell'offerta formativa. Alcuni corsi sono dual-use, ma lo sviluppo delle lezioni è orientato alle operazioni.

Sviluppo capacitivo CNO – Attività iniziali

STATO MAGGIORE DIFESA

CNO

- Realizzazione ordine di battaglia cyber
- Sviluppo sistemi di supporto alla pianificazione e condotta delle operazioni cyber
- Implementazione sistema perimetrale per attività di CND
- Formazione e addestramento personale specialistico avanzato
- Definizione delle procedure operative

Considerazioni

STATO MAGGIORE DIFESA

- Sviluppo attività delle *Computer Network Operations (CNO)* è essenziale per assicurare la possibilità di operare alla Difesa in un settore che diventerà sempre più fondamentale nello spettro delle capacità militari
- Quadro normativo assegna competenza principale al Sistema di informazione per la sicurezza della Repubblica (comparto sicurezza) e *non definisce compiti Difesa*
- Da valutare esigenza di adeguamento del quadro normativo per acquisizione operatività ambito CNO
- I principali alleati hanno già definito il quadro organizzativo e le relative attività

9 marzo 2016

Aspetti critici (1)

STATO MAGGIORE DIFESA

- Sostanziale gap tecnologico-manifatturiero accumulato, difficile da colmare:
 - Investimenti con maggiori risorse
 - Forte indirizzo e valutazione delle performance industria nazionale
 - Rafforzamento partnership di livello europeo
- Le limitate risorse del nostro paese non sono adeguatamente valorizzate e messe a sistema:
 - Completa dipendenza dall'import hardware
 - Sviluppo assetti nazionali per core networking
 - Capacità comunicazioni satellitari nazionali
 - Sostanziale dipendenza dall'import del software
 - Sistema operativo di riferimento
 - Riconoscimento sovranità nazionale per ottenere e valutare codice sorgente
 - Import dei sistemi e software di sicurezza (antivirus nazionale?)

9 marzo 2016

Aspetti critici (2)

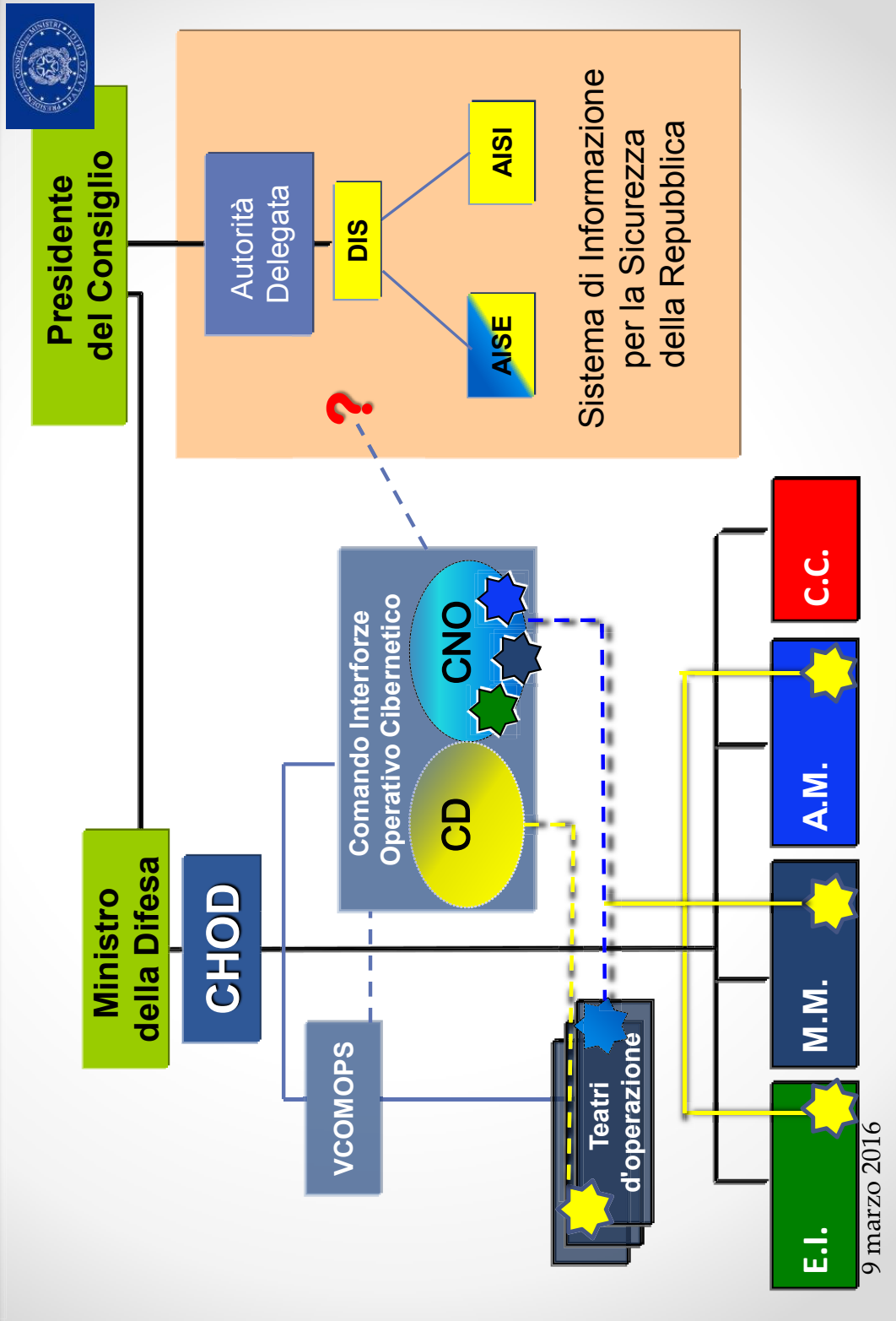
STATO MAGGIORE DIFESA

- Reclutamento personale
 - Percorsi formativi estensivi e differenziati per livelli di impiego
 - Sfruttamento meccanismi della riserva selezionata
 - Reclutamento personale esterno
 - Outsourcing DEVE essere **gestito opportunamente** (*Insider threat*)
 - Maggiore sforzo di promozione della cultura cyber sin dalle scuole dell'obbligo
- Procurement
 - Procedure in vigore non compatibili con compressione dimensione temporale cyberspace
 - Standardizzazione e razionalizzazione della spesa
 - Verifiche di sicurezza

9 marzo 2016

Competenze cyber – Ipotesi

STATO MAGGIORE DIFESA



Fine presentazione

STATO MAGGIORE DIFESA

DOMANDE ?

9 marzo 2016

PAGINA BIANCA



17STC0016810