COMMISSIONE IV
DIFESA

RESOCONTO STENOGRAFICO

INDAGINE CONOSCITIVA

1.

SEDUTA DI MARTEDÌ 9 FEBBRAIO 2016

PRESIDENZA DEL PRESIDENTE **FRANCESCO SAVERIO GAROFANI**

INDICE

N. B. Sigle dei gruppi parlamentari: Partito Democratico: PD; MoVimento 5 Stelle: M5S; Forza Italia - Il Popolo della Libertà - Berlusconi Presidente: (FI-PdL); Area Popolare (NCD-UDC): (AP); Sinistra Italiana-Sinistra Ecologia Libertà: SI-SEL; Scelta Civica per l'Italia: (SCpI); 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 11.05.

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, la trasmissione televisiva sul canale satellitare della Camera dei deputati e la trasmissione diretta sulla *web*-tv della Camera dei deputati.

Audizione del Direttore del Centro di Ricerca Sapienza in *Cyber Intelligence e Information Security* (CIS), professore Roberto Baldoni.

PRESIDENTE. L'ordine del giorno reca, nell'ambito dell'indagine conoscitiva sulla sicurezza e la difesa nello spazio cibernetico, l'audizione del professore Roberto Baldoni, direttore del Centro di Ricerca Sapienza in *Cyber Intelligence e Information Security* (CIS).

Saluto e do il benvenuto al professore Baldoni, che ringrazio per la sua presenza qui oggi. Il professore è accompagnato dall'ingegnere Montanari e dalla dottoressa Caramagno.

Ricordo che l'indagine avviata dalla Commissione si incentra sugli specifici profili di interesse della Commissione difesa, e quindi sulla minaccia cibernetica di livello paragonabile all'attacco armato. Peraltro, proprio per far emergere il ruolo che le Forze armate svolgono oggi e quello che dovranno svolgere in futuro in questo campo, l'indagine intende tenere conto anche del ruolo svolto dagli altri soggetti che operano nel complessivo sistema di protezione dello spazio cibernetico nazionale.

A questo fine, la Commissione è interessata ad acquisire anche il contributo di conoscenza che può venire dall'apporto di inquadramento concettuale, di informazione e di esperienza di soggetti che, pure esterni al sistema della difesa in senso stretto, operino comunque in campi di attività riconducibili al tema di cui si parla.

Il professore Baldoni è il direttore del Centro di Ricerca CIS, costituito nell'ambito dell'Università degli studi di Roma « La Sapienza ». Il Centro ha curato, tra l'altro – insieme con il Laboratorio nazionali di *cyber security* del Consorzio Interuniversitario Nazionale Informatica (CINI) e in collaborazione con diverse organizzazioni pubbliche e private – il rapporto 2015, nel quale viene presentato un *framework* nazionale per la *cyber security*. Il professore Baldoni ha portato delle copie che sono a disposizione.

Dopo l'intervento del professore darò la parola ai colleghi che intenderanno porre questioni o svolgere osservazioni, poi il professore sarà così cortese da rispondere alle domande.

Senza altri indugi do la parola al professore per la sua relazione.

ROBERTO BALDONI, *Direttore del Centro di Ricerca Sapienza in Cyber Intelligence e Information Security (CIS).* Innanzitutto, grazie mille per l'invito, signor presidente. Ringrazio anche i membri della Commissione. La presentazione che svolgerò sarà variegata. In alcuni punti, riguarderà una parte un po' più tecnica, in altri sarà molto più di alto

livello. Non esitate, dunque, a interrompermi se volete ulteriori spiegazioni su qualche punto anche durante la presentazione stessa, altrimenti potrete porre le domande al termine.

Oltre a essere direttore del Centro di Ricerca di *Cyber Intelligence e Information Security* della « Sapienza » (CIS), dirigo anche il Laboratorio nazionale di *cyber security* (CINI), del quale poi parlerò un attimo per farvi capire come si è costituito e come è stato strutturato in questi ultimi anni.

Innanzitutto parliamo di settori economici che ormai vanno dalla parte finanziaria alle infrastrutture critiche, alla pubblica amministrazione, alle industrie, che sono sensibili alle minacce del *cyber space*. Che cos'è il *cyber space* ? Viene definito come il complesso ecosistema risultante dall'interazione di persone, *software* e servizi su *Internet* per mezzo di tecnologie, dispositivi e reti a esso connesse. Dunque il *cyber space*, fondamentalmente, è una struttura su cui si poggia il nostro Paese, e ormai tutta la nostra economia. Non credo che esista un settore in questo momento – anche molto lontano, come l'agricoltura o altri – che non si poggi pesantemente sul *cyber space*.

È importante notare perché nella *slide* che apre la presentazione ho messo l'icona dell'Italia: infatti, nel momento stesso in cui si inizia a integrare economia e cyberspazio, diventa strategico ragionare e difendere il nostro cyberspazio, esattamente come facciamo con il nostro spazio aereo, col nostro spazio marittimo, proprio perché difendiamo di fatto i nostri interessi economici, politici e militari.

Perché c'è stata questa interazione e questo poggiarsi sul *cyber space* da parte di tutti i settori economici, chi prima, chi dopo ? Il discorso è legato all'efficienza e alla produttività: all'efficienza, nel senso di utilizzare dei servizi, il *Web*, le *e-mail* e così via; alla produttività, perché anche le catene di montaggio, i sistemi industriali hanno beneficiato di tutto quello che va sotto il nome di tecnologia IP, basata su *Internet* che ha portato a una riduzione di costi formidabile.

Se pensiamo alle infrastrutture critiche, come una centrale nucleare o una centrale elettrica, è chiaro che hanno sempre vissuto, a partire dagli anni Sessanta, di informazione e dati; tuttavia, in quel momento, informazione, dati e *software* erano proprietari, e quindi c'era un insieme molto ridotto di persone che conosceva i segreti di quella particolare tecnologia, e magari le sue vulnerabilità.

Nel momento stesso in cui ci si è messi a lavorare al di sopra di *Internet*, si sono abbracciati non solo i vantaggi, ossia l'efficienza e la produttività, ma anche tutte le vulnerabilità che *Internet* ha al suo interno. Queste vulnerabilità, che vanno – ad esempio – da errori *software* a misconfigurazioni del sistema, sono quelle porte che vengono usate per entrare all'interno dei nostri sistemi. Da una parte, quindi, ci sono efficienza e produttività e, dall'altra, abbracciamo vulnerabilità.

Quando si parla di *cyber space*, non esiste divisione tra pubblico e privato, tra militare e civile. È un ambiente in cui pressoché tutto è duale e dove tutto può essere preso dalla parte civile e portato verso la parte militare: sistemi operativi, *off the shelf*, *storage*, una serie di *software* che comandano sistemi anche di comando e controllo di tipo militare.

È importante capire un altro concetto: le vulnerabilità non sono numerabili. Non sappiamo quante vulnerabilità ci sono nel *cyber space*. Possiamo soltanto stimarlo, come si stimano i pesci che sono all'interno di un lago o nel mare. Nessuno sa quanti sono i pesci nel mare, ma esistono delle stime con le quali si cerca di fare un conto. La stessa cosa accade per le vulnerabilità. Questo è legato ai processi di gestione *software*. Quando, cioè, si crea il *software* si pensa normalmente all'usabilità, all'utente finale, qualche volta si pensa anche al *beauty*, al bello, giacché l'interfaccia deve essere bella, l'APP accattivante. Non si pensa a problematiche di sicurezza, quindi si lasciano dei buchi all'interno del *software*, che a mano a mano vengono scoperti da parte di persone che guardano il *software* con altri

occhi. Non lo guardano come l'utente che usa l'APP, ma per trovare le debolezze di quel *software*.

È chiaro che in un sistema in cui di fatto non c'è più una divisione tra pubblico e privato, tra militare e civile, nessuno può pensare di gestire questa complessità in isolamento. Per primi lo hanno capito gli Stati Uniti con una serie di passi importanti che hanno compiuto. Le reti di comunicazione, per esempio, o quelle elettriche non sono nazionali. Sono gestite da aziende, ma il Governo ha responsabilità sui dati dei cittadini o anche nel mettere in relazione le diverse infrastrutture critiche. Ha anche, chiaramente, il dovere di mantenere la qualità dei servizi base che eroga ai cittadini. Tutto questo porta a unire pubblico e privato all'interno di questa battaglia.

Che cos'è, quindi, la *cyber security* ? È quella pratica che consenta a un'entità, ad esempio un'organizzazione, il cittadino, la Nazione la protezione dei propri *asset* fisici, la confidenzialità, l'integrità e la disponibilità delle proprie informazioni dalle minacce che arrivano dal *cyberspace*.

Qual è una minaccia di un *asset* fisico per un cittadino ? Io ho un televisore *smart* con un indirizzo IP, e può essere tranquillamente attaccato. Abbiamo una serie di esperimenti che mostrano come si possa entrare all'interno della vostra casa attraverso i vostri *Wi-Fi Gateway*, e iniziare a prendere il controllo di tutte le cose che sono connesse. Sicuramente, da cinque anni a questa parte, avrete almeno una trentina di dispositivi connessi all'interno dei vostri *Wi-Fi Gateway*. Questo è l'esempio per i cittadini. Per la Nazione, ovviamente, parlo di infrastrutture critiche, di tutto quanto porta i servizi primari ai cittadini, acqua, gas, luce elettrica, petrolio e così via.

Questa interazione tra economia e *cyber space* va capita – e poi estesa anche alla difesa – perché non finirà. Anzi, continuerà nel futuro e sarà sempre più forte. Che cosa c'è stato negli anni Duemila ? La rivoluzione del *cloud*, dei *data center,* degli *smartphone*. Noi stiamo vivendo gli effetti di queste rivoluzioni. Avete sicuramente sentito parlare un po' di questi nomi: Industry 4.0, *Smart cities*, *digital currencies*, *big data* eccetera. Queste sono rivoluzioni in atto, ma quando ne vivremo gli effetti, a quel punto, l'economia e il *cyber space* saranno una cosa unica e sarà difficile capire che cos'è economia e che cosa *cyber space*.

Vi mostro ora una *slide* che ho presentato di recente a una manifestazione che c'è stata alla « Sapienza »: la trasformazione economica sarà sempre più veloce, inarrestabile, implacabile, cambierà il lavoro uccidendo vecchi posti e creandone nuovi, ma a una velocità inimmaginabile. Pensiamo al vecchio casellante: tutto cambierà a una velocità ancora più forte, e cambierà pesantemente gli equilibri tra Stati, tra aziende e tra aziende e Stati.

Qualcuno potrebbe pormi la domanda sulle problematiche nella gestione e nella segretezza delle informazioni che tra dieci anni potranno esserci tra Stati, magari Cina e Stati Uniti: io credo che tra dieci anni probabilmente potrebbero esserci anche problemi tra Stati Uniti e qualche multinazionale digitale (le aziende cosiddette *over-the-top)*, o tra multinazionali. Il futuro che abbiamo davanti è veramente molto complesso da decifrare. Già si vedono alcune avvisaglie se si pensa al fatto, ad esempio, che quando è stato lanciato il *framework* nazionale *cyber security* americano, *Google* non era presente allo *speech* che Obama tenne alla « Stanford University », quando chiamò tutte le aziende digitali a cercare di dare una mano. Lui è stato il primo a metterci la faccia, e *Google* non era presente. Iniziano, infine, a vedersi delle acquisizioni di *media* da parte di questi soggetti. Secondo me, si iniziano a piazzare delle pedine per un mondo che va cambiando molto velocemente.

Un altro punto importante è che chi non saprà intercettare questa rivoluzione diventerà terzo mondo del terzo millennio. È bene capirlo. È un concetto che ho affermato in modo molto chiaro già altre volte. O sapremo intercettare questa rivo-

luzione digitale, e quindi anche difenderla, difendere il nostro *cyber space*, o a mano a mano avremo un Paese che si deindustrializza, i cui cervelli andranno all'estero. O meglio, non saranno solo i cervelli ad andare all'estero, ma vi sarà una vera fuga di persone, che è una cosa diversa. Anch'io ero un cervello in fuga, poi nel 1996 sono rientrato, ma si poteva, mentre adesso è molto complesso. Il problema che in questo momento abbiamo non è la fuga dei cervelli, ma la fuga di persone qualificate che non riescono a trovare in questi settori in Italia un livello accettabile di occupazione. Ecco perché la questione è particolarmente importante e va affrontata con estrema velocità.

Non dobbiamo neanche dimenticare che, se il mondo dell'economia correrà, la minaccia *cyber* correrà a una velocità ancora più alta di qualsiasi altra trasformazione. Il nemico è sempre avanti. Questo è un altro importante punto da tenere presente. La protezione del *cyber space* diventa condizione necessaria per la prosperità economica e l'indipendenza di un Paese. Su questo non possiamo immaginare che arriverà qualcuno che ci aiuterà in questo processo. Questa è una *misconception*, un'idea sbagliata. Non bisogna pensare che arriverà qualcuno che ci metterà in sicurezza, perché difesa ed economia sono indistinguibili nel *cyber space*.

Voglio dire che nel momento stesso in cui qualcuno metterà in sicurezza i nostri sistemi, quel qualcuno avrà accesso a tutte le informazioni economiche del nostro Paese. Non so se sarà un bel momento. Ecco perché tutti i Paesi stanno portando avanti, come sapete, una strategia nazionale, un processo di implementazione nel piano strategico nazionale.

Sono stato chiamato dal Lussemburgo per aiutarli a mettere su un sistema di ricerca, che permettesse loro di fare che cosa ? Immaginate come si regge il Lussemburgo: con gli *headquarter* delle grandi aziende, che portano lì molta ricchezza, sulla quale loro guadagnano e prosperano. Se non sono in grado di dare sicurezza, e quindi di porre le basi, di cui poi parleremo, al controllo del *cyber space*, il giorno dopo le aziende se ne andranno tutte.

Lo ha capito molto bene l'Inghilterra, che ha lanciato un piano di sicurezza del proprio *cyber space* quinquennale, mettendo dentro un bilione di euro, creando in otto Università altrettanti centri di ricerca – parlo più della ricerca, perché è quella che ho più vicina – finanziandoli dall'uno ai tre milioni di *pound* ciascuna, ognuno con la sua specificità. Vogliono diventare, come è scritto nello *statement* del primo documento uscito, il Paese più sicuro in cui fare *business* dal punto di vista del *cyber space*. È importante, quindi, pensare a questi incroci, che nessuno verrà a farci i compiti a casa. Se quel giorno accadrà, non sarà un buon giorno per noi.

Vengo al *cyber attack*. Non ho portato numeri, anche se questo è un po' lo sport nazionale. Immagino che abbiate letto rapporti, quindi sapete che il numero e il livello di sofisticazione degli attacchi stanno nettamente aumentando. Abbiamo sulle nostre infrastrutture picchi di migliaia di attacchi all'ora, in cui si vede che c'è un'intelligenza dietro. Gli attacchi avvengono, infatti, prevalentemente la sera e durante i *weekend*, proprio per sfruttare eventuali debolezze del difensore. Ovviamente, è un campo completamente asimmetrico, in cui sul mio *sofa* posso attaccare mille organizzazioni distinte contemporaneamente. Esistono dei *tool* di attacco sempre più semplici, potenti e alla portata di tutti. Questa è chiaramente una manna, soprattutto per la parte criminale della medaglia.

Le difficoltà di attribuzione sono il grosso problema. Non è difficile, una volta che si hanno degli *skill* medi in informatica, nascondersi all'interno del *cyber space*. Esistono tecniche abbastanza semplici con cui far perdere le proprie tracce, per poi da Roma spuntare in Russia e da lì iniziare un attacco verso altre organizzazioni. È importante, quindi, avere questi punti di riferimento.

Un'altra cosa importante da capire è che fino ad alcuni anni fa gli attacchi erano prevalentemente tecnologici, ovvero

si basavano sull'attacco al perimetro aziendale, inteso come perimetro all'interno del *cyber space*, quindi tutta la parte di *firewalling*. Questo accade ancora e ci sono delle inerenti difficoltà in questo momento a contrastarli, soprattutto legati alla *supply chain*, quindi alla catena di approvvigionamento. Ormai, un'azienda che si pone su *Internet* non è un fortino in cui posso mettere le mie difese.

Chi si mette su *Internet* in qualche modo inizia ad avere degli utenti, *customer*, gente che compra da quest'azienda, *partner*, o fornitori. A quel punto, questi *partner*, fornitori, parlano direttamente, *machine to machine*, e il perimetro diventa assolutamente impalpabile. Basta attaccare una società piccola che fa da fornitore, e si ha accesso diretto alla casa madre. Questo è uno dei motivi fondamentali per cui, se non proteggiamo il nostro *cyber space*, nessuno verrà a investire in Italia.

Posso assicurarvelo. Sono già stato a un paio di *workshop* e la gente, e cioè gli investitori, vuole sapere che cosa sta facendo l'Italia in questo settore. Io non vado a mettere un *branch* di una mia azienda su un Paese che non ha quegli strumenti base per la difesa, altrimenti quello diventerà il mio punto debole e da lì entreranno direttamente nell'*headquarter*, attraverso la connessione *machine to machine*.

Il punto, però, non è soltanto tecnologico. Ormai, l'attacco avviene usando il fattore umano e sfruttando le debolezze del fattore umano stesso, quindi la vulnerabilità non è più tecnologica in quanto tale. Ovviamente, le difese si sono sviluppate, soprattutto le infrastrutture critiche hanno portato avanti grossa capacità difensiva. Che cosa si fa? Si attaccano direttamente le persone. Avrete sentito parlare di *phishing*. Quello è uno dei modi con cui si attaccano le persone dentro le organizzazioni. Vi mostrerò degli esempi di *phishing*, e nemmeno io sarei in grado di riconoscere un'*e-mail* con un allegato mandata dal presidente della vostra Commissione a voi o la mia che mi fingo lui e vi faccio aprire un PDF che scaricate nei vostri computer, mentre magari è un *software* di spionaggio. Sempre più abbiamo questi attacchi direttamente alle persone, che a volte sono consapevoli, quindi abbiamo gli *insider*, mentre a volte sono inconsapevoli, appunto attraverso attacchi mirati.

Vi mostro adesso una *slide* in cui vi sono alcuni esempi di attacchi tra i più importanti che abbiamo visto negli ultimi due anni, come *ramsonware*. Proprio ieri, un collega mi diceva che dal suo commercialista aveva visto la segretaria piangere perché avevano subìto un attacco di *ramsonware* e tutti i loro dati erano stati cifrati, per cui stavano vedendo la modalità di pagamento del riscatto, di 500 euro. Non so se sapete come funziona, ma hanno anche una sorta di *customer care*: una volta che vi hanno rimesso i *file* a posto, si raccomandano, se avete un problema, di ricontattarli. Questo è per darvi un'idea anche del livello di sofisticazione. C'è un vero e proprio mercato, con tutti i vari attori, che si sta muovendo nel lato *cyber crime*.

Ci sono stati casi molto importanti di *denial of service*, specialmente in Sud America, negli ultimi due anni. C'è lo spionaggio, il *wiping*, quella tecnica per cui entrano nei vostri sistemi, vi copiano tutte le informazioni, ma non contenti ve le cancellano anche. Di *cyber-physical* adesso parleremo, perché è particolarmente importante in ambiente difesa.

Il *doxing* è un'altra tecnica sulla quale bisogna riflettere un attimo. In questo momento è praticato soprattutto verso le celebrità. In sostanza, questa tecnica consiste nel recuperare informazioni sulle persone. Si può farlo anche direttamente su *Internet*. Se si è una celebrità, si recuperano informazioni e si creano dei *dossier* sulla persona. Ovviamente, nessuno di noi, soprattutto se siamo persone celebri, sa quante informazioni ci sono su di noi su *Internet*. Sfruttandole, si può arrivare a conoscere cose molto importanti sulla persona.

A questo punto, pensate se si iniziasse a fare questo su scala nazionale, ovvero iniziando a « dossierare » tutti i cittadini di

un Paese. Non è un problema, noi siamo 56 milioni, non ci vuole grande capacità computazionale. Sotto questo profilo, avere un *dossier* per ciascuno di noi non è così complesso, né impone uno *storage* particolare. Se si ha accesso all'anagrafe, si inizia a cercare tutti e a vedere le informazioni che ci sono, a fare una tassonomia, a catalogarci uno per uno.

I *cyber-physical* sono i più pericolosi. Tutti voi conoscete *stuxnet*, il primo attacco cyber-fisico. Naturalmente, per arrivarci significava che avevamo davanti a noi un'azione *State-sponsored*, perché tale è il livello di risorse per arrivare a penetrare una centrale altamente protetta e iniziare a distruggerle tutte le centrifughe una per una, nascondendosi e non facendosi trovare fino a che, credo dopo 100-200 centrifughe rotte, riuscirono a capire che cosa non andasse. Anche nel caso del discorso cyber-fisico avremo un abbassamento delle *expertise* che ci sarà bisogno di avere per attacchi di questo tipo. Secondo me, tra dieci anni forse sarà molto più alla portata di tutti. Chiaramente, dall'altra parte spero che le difese saranno molto aumentate.

Abbiamo avuto il secondo attacco cyber-fisico certificato a un altoforno della ThyssenKrupp, che a un certo punto si è spento. Non si capiva perché questo altoforno si fosse spento, e poi ci si è accorti che dentro il sistema SCADA che controllava l'altoforno c'era una variazione di *stuxnet* che ha portato a questa chiusura. Questo è accaduto nel centro dell'Europa. Infine, avrete tutti sentito anche dell'attacco (di *matrice cyber*, ma i dettagli al momento non sono ancora pubblici) alla società elettrica ucraina che ha lasciato al buio 700.000 persone in Ucraina.

Ovviamente, abbiamo avuto casi di spionaggio molto rilevanti. Il più importante è stato il *data breach* che si è verificato in Lockheed Martin e in altri *contractor* americani e che ha portato – se non erro – a 50 terabyte di informazioni su progetti legati all'*F-35* trasferite presumibilmente verso la Cina, Paese che poi ha costruito il velivolo *J-20*, molto molto simile nelle caratteristiche all'*F-35*. Si è trattato di una perdita incredibile. Si è anche dimostrato che in questo modo c'è una scorciatoia, usando il *cyber space*, rispetto all'investire in ricerca e sviluppo. Questa è stata un'altra « botta » molto forte che è arrivata da questo caso.

Non ci si ferma alla parte militare, ma si arriva anche a quella economica. Abbiamo avuto il caso, qualche mese fa, di una compagnia australiana che commerciava in *metal detector* e a un certo punto ha visto diminuire il suo fatturato. Non capivano bene perché, e dopo un po' sono arrivati dei *metal detector* in assistenza che non erano stati costruiti da loro. Si sono visti recapitare questi apparecchi, pensavano che fossero loro, ma in realtà non lo erano. Erano stati costruiti in Cina, utilizzando lo stesso progetto e le stesse tecnologie.

Arrivo a un altro passaggio importante per noi. Che cos'è Hacking Team ? È una piccola media società italiana che realizza un buon prodotto, altrimenti la gente non lo comprerebbe. È una tecnologia particolare, per cui andrebbe protetta. In realtà, vengono rubati 400 gigabyte di informazione, inclusi i codici sorgenti del loro prodotto di punta, che era appunto questo sistema di spionaggio chiamato RCS.

La prima osservazione è che riguarda una piccola media impresa, e questo significa che può capitare a chiunque. Ne abbiamo discusso anche l'altro giorno alla presentazione del Framework Nazionale per la Cyber Security: Barilla ha i suoi dati sensibili, che se vanno in mano di suoi *competitor* diventano armi che vengono usate contro di lei. Per Luxottica vale lo stesso discorso. Ebbene, cerchiamo di contestualizzare questo discorso nell'ottica di un attacco al sistema Paese.

Quando ci fu l'attacco alla Sony, dopo qualche ora, non l'esponente dell'FBI ma il Presidente Obama ha preso il microfono dichiarando che quelle cose negli Stati Uniti non si fanno. Ha poi firmato due *executive order*: il primo per l'aumento dello *sharing* informativo, una delle caratteristiche fondamentali con cui combattere, e lo vedremo successivamente, questo

tipo di attacchi; il secondo, per precisare che, se avessero conosciuto il mandante, avrebbero bloccato tutti i suoi beni all'interno degli Stati Uniti. Era, infatti, un attacco diretto al sistema Paese. È estremamente importante raggiungere questa consapevolezza.

Non possiamo essere un libro aperto per altri che vengono, guardano e decidono se mettere su rete informazioni riservate. Se così fosse, non solo non avremmo più quella tecnologia come Paese, ma la stessa si ritorcerà contro di noi. Come è accaduto per Zeus, virus che attacca infrastrutture bancarie, una volta che fu preso il codice sorgente, sono state poi generate venti mutazioni di quel virus. Che cosa significa mutazioni? Che io azienda straniera prendo il codice sorgente, lo cambio e creo un'altra arma cibernetica. Questo è successo per Zeus. Succederà anche per RCS. È molto più pericoloso. Se rubano un carrarmato, che cosa possono fare? Lo smontano, lo rifanno? Sempre un carrarmato è. Qui creano nuove armi.

Chi è l'avversario? Le *slide* che ora vi mostrerò saranno un po' più tecniche, ma ripeto che cercherò di farvele ad alto livello proprio per capire l'essenza di questo tema. C'è stata una mutazione. Prima del 2004, anno che ha rappresentato un po' la svolta, chi era l'*hacker*? Era un *nerd* particolarmente bravo a smanettare, che per essere *cool*, per essere al passo coi tempi, cercava di infettare altri computer, ma non aveva né l'idea dello spionaggio né quella del controllo dei computer. Aveva soltanto l'idea di fare più notizia possibile.

A un certo punto, si è capito che in realtà queste armi potevano essere usate per ben altri scopi, e allora abbiamo avuto l'esplosione della parte criminale, legata agli Stati, che hanno iniziato a investire su questo tipo di armi cibernetiche. Abbiamo così avuto i *malware* e poi le APT *(advanced persistent threat*) un'evoluzione ancora superiore rispetto ai *malware*.

Come si riconosce l'avversario? L'avversario si riconosce per il livello di *expertise* con cui crea questi virus e con le risorse disponibili. Sappiamo che *stuxnet* – con altissima probabilità e grazie anche a delle fughe di notizie – è stato fatto in una *joint-venture* tra Stati Uniti e Israele. Oltretutto, per fare quel virus in quei tempi c'è bisogno proprio di risorse economiche molto rilevanti, che soltanto uno Stato sovrano poteva mettere a disposizione. L'avversario si riconosce anche da come i vettori di attacco inoculano il virus all'interno dei nostri computer e dal tipo di comportamento, ossia da come si comporta il virus all'interno dei nostri computer.

Giusto per darvi un'idea di un'APT, c'è bisogno di un livello di *expertise* elevato. Infatti, i punti che secondo me in modo essenziale la differenziano dai *malware* classici sono i seguenti: minare o impedire aspetti critici di una missione o di un programma o di un'organizzazione, esattamente quello che come primo esempio di APT abbiamo avuto a Natanz, in Iraq, con l'attacco alla centrale nucleare; posizionarsi e nascondersi per portare avanti questi obiettivi nel futuro; perseguire i suoi obiettivi in modo ripetuto all'interno di un lungo periodo di tempo. Abbiamo, quindi, il nascondersi, il posizionarsi nel mettere un piede all'interno dell'infrastruttura IT per trafugare informazioni, ma anche per prenderne il controllo successivamente.

Mi dicono che ci sono stati casi – sono *rumor*, non confermati – di armi, sistemi missilistici che a un certo punto non hanno funzionato a causa di un virus che aveva attaccato il sistema SCADA del comando e controllo. Le problematiche, come vedete, sono abbastanza rilevanti.

Passo adesso alla *slide* che descrive *equation group*. Voglio darvi l'idea della sofisticatezza che raggiungono questi gruppi. Perché riusciamo a classificarli? Un gruppo non fa un solo *malware*. È una sorta di industria, ne fa un certo numero, ognuno con le sue specificità, dopodiché è chiaro che alcune parti di *software* utilizzate in queste armi cibernetiche vengono riusate, e quindi da lì si capisce la matrice, che è lo stesso gruppo. È come riusare lo

stesso *software*: significa capire che esso è in mano a quel gruppo, e quindi identificare il gruppo stesso.

Equation group è specializzato in spionaggio su PC. È interessante, perché normalmente il virus si può inoculare attraverso l'accesso a un sito *Web* particolare, che può essere fatto perché magari vi mandano un *link* o perché voi andate a visitare quel sito *Web*. Inizialmente vi viene caricato un piccolo virus che sfrutta le vulnerabilità dei vostri *browser*. A quel punto, questo piccolo virus inizia a studiare il vostro computer, cerca di capire se siete un « pesce interessante » da controllare. Se lo siete, fa come quel vecchio cartone animato, Jeeg Robot, che chiedeva i componenti, e li chiede. *Double fantasy* e *equation drug* sono componenti che vengono richiesti mano a mano, in funzione appunto del proprietario della macchina in cui in quel momento il virus è entrato. Se vede che la persona non è rilevante, si uccide, e automaticamente perdiamo ogni traccia della sua esistenza e del suo passaggio, altrimenti vengono installati nuovi componenti.

Inoltre, *equation group* è in grado di lavorare su *air-gapped network* e, quindi, non c'è bisogno che la vostra rete sia connessa a *Internet*, basta che usi tecnologia IP. Molte installazioni non sono connesse direttamente a *Internet*. Il problema è l'impiegato che prende una USB, la usa a casa e, successivamente, la usa dentro l'installazione. Loro sono specializzati proprio in questo tipo di attacchi.

Detto questo, però, la caratteristica fondamentale di *equation group* è il loro modo di infettare il *firmware* dell'*hard disk*. Voi sapete che un *hard disk* esce dalla fabbrica con un *software* che sta dentro un microprocessore. Questo si chiama *firmware*. A quel punto, l'*hard disk* viene messo dentro un PC. *Equation group* è riuscito a nascondere il virus all'interno del *firmware* della vostra macchina. Che cosa significa questo ?

Significa che, anche se vi accorgete che qualcosa non va, e quindi magari resettate e ristallate la macchina, quando la macchina è ristallata e voi riaccendete il sistema, il virus lo avete all'interno, e quindi automaticamente si riposiziona. Capite anche il tipo di attore che può fare una cosa di questo tipo. Vi mostro ora una *slide* dove ci sono circa una dozzina di marche e il *firmware* non è un codice aperto, ma è proprietario della casa costruttrice. Questi dovevano conoscere, per fare questo, tutti i *firmware* di quelle marche, altrimenti non si fa una cosa del genere.

Adesso vi parlo di *rocket kitten*, gruppo famoso per il *phishing*. Loro inoculano il *malware* all'interno attraverso campagne di *phishing* mirate. Per quanto riguarda *rocket kitten*, conosciamo due campagne rilevanti, e le vittime sono state soprattutto organizzazioni israeliane e tedesche. È importante anche notare, come queste armi stiano mano a mano diventando più precise. Il ragazzo che faceva il virus negli anni Novanta voleva raggiungere più computer possibili. Questi vogliono raggiungere l'obiettivo, che è una cosa diversa.

Qui è rappresentato il caso di un CEO, se non vado errato di un'azienda tedesca, (ovviamente, il messaggio è un *fake*) che manda a tutti i dirigenti di primo livello della sua azienda informazioni riguardanti un *meeting*, reale, riguardante le celebrazioni delle relazioni diplomatiche tra Germania e Israele. Ovviamente, c'era anche il *file Excel*, fatto bene, con tutte le informazioni necessarie. Il problema è che, se vedete quelle righe sopra, nel *file Excel* è scritto che però bisogna abilitare le macro. Nel momento stesso in cui si abilitavano le macro per vedere quel *file*, avevate il primo stadio del *malware* che entrava nel vostro computer.

È come se il vostro presidente vi mandasse un'*e-mail* con delle informazioni. Questo è il livello di sofisticatezza.

Vi riporto un altro caso, ma di cui mi sarei accorto. Forse quello di prima mi avrebbe ingannato. C'era l'eseguibile sul PPT e quando lo andavi a vedere, c'era la presentazione. Il problema è che prima della presentazione aveva già caricato con l'*exe* il virus all'interno. Anche qui è un alto ufficiale israeliano che

chiede informazioni a un gruppo di esperti riguardo una delle ultime campagne con gli elicotteri che era stata fatta contro gli *hezbollah*.

MASSIMO ARTINI. Inviarlo è plausibile con qualsiasi sistema SMTP, ma avere l'elenco dei destinatari è la parte che fa più pensare.

ROBERTO BALDONI, *Direttore del Centro di Ricerca Sapienza in Cyber Intelligence e Information Security (CIS)*. Purtroppo, stando in « Sapienza », devo dire che tutti i nostri indirizzi privati sono pubblici in qualche *server*. Certo, è chiaro che devono avere gli indirizzi, ma secondo me sono troppo facili da recuperare. Vedete che era su *OneDrive*, quindi stiamo parlando di una piattaforma *cloud* Microsoft. Anche quello portava un certo *trust* nello scaricare il *file*.

Passo ora a parlare del rapporto tra i Governi e la minaccia *cyber*. Come vi ho detto, tutti i Governi si stanno muovendo in modalità nazionale, poi ci sono i movimenti europei, i movimenti G7, i movimenti NATO, ma ogni Governo si sta muovendo singolarmente. Basta che cerchiate « strategia nazionale *cyber security* » e troverete almeno cento Stati che si stanno muovendo in questa direzione. Ripeto che trattasi di materia molto delicata. Anche l'armonizzazione a livello europeo – chi ha seguìto la direttiva NIS *(Network Information Security*) lo sa – è stata molto complessa e ha portato a un minimo comune denominatore: quegli elementi che ogni Nazione dovrà avere. Sicuramente, le Nazioni più avanzate, come Germania e Inghilterra, non si fermeranno a quello, ma andranno molto oltre, e lo faranno seguendo le proprie regole.

Relativamente alla capacità necessaria a livello di sistema Paese, ho cercato di condensare un po' di cose anche per darvi diversi livelli di astrazione. Che cosa tocca il problema *cyber* ? Tocca *in primis* la parte della difesa militare, la parte della *intelligence*, quella della *law enforcement* (ossia dell'interno), della ricerca domestica, dell'industria domestica e tocca il discorso delle relazioni internazionali. Probabilmente, se ci pensiamo un attimo, ci viene anche qualche altra cosa in mente, ma se dovessi pensare a delle componenti che devono occuparsi di questo, penserei a queste in prima battuta.

Quali sono le linee strategiche ? Abbiamo identificato i componenti, adesso cerchiamo di capire come dipanare una serie di linee. L'*information sharing* è fondamentale. Il vostro attaccante sarà sempre più avanti di voi. Noi cercheremo di stargli dietro, ma lui sarà più avanti. La condivisione delle informazioni è fondamentale, e farla in modo veloce ed efficiente è uno dei meccanismi chiave. Il Presidente Obama ha firmato tre *executive order* sull'*information sharing*, due dei quali sono stati tradotti anche in legge. Sapete che negli Stati Uniti c'è questo problema per cui l'*executive order* è importante, ma se cambia l'Amministrazione, possono cambiare le cose. Diverso è se questo è stato anche approvato dal Senato, o comunque supportato con qualcosa di simile dal Senato. Lì abbiamo questa situazione.

Quanto alle *partnership* pubblico-private, come ho detto, non si risponde in isolamento, ma tutti insieme, cercando di evitare i punti deboli. C'è sicuramente bisogno di *partnership* pubblico-private, ma poi toccherò questo tema.

C'è l'*education and hygiene*. *Cyber hygiene* è una delle espressioni chiave. Dobbiamo educare le persone a capire il mezzo e a capirne i rischi. C'è la *forensic capability*: dobbiamo sicuramente avere capacità forensi che ci permettano di capire quello che sta accadendo o che è accaduto nei nostri sistemi. C'è la preparazione, c'è il *cyber* nel DNA dell'organizzazione, sia essa militare, civile, industriale, pubblica o privata. Bisogna migliorare la ricerca e l'innovazione. Serve una *active defence*. Noi siamo un grande Paese. Se viene fuori l'attacco massiccio di una *botnet* da altre Nazioni, che cosa facciamo ? È un problema che molti si sono posti. Chi può fare qualcosa ?

Credo che, tra il gruppo che ho elencato sopra, in alcuni casi sicuramente

l'*intelligence* può fare qualcosa, ma chi può andare fuori dal dominio italiano e fare qualcosa per queste problematiche forse è soltanto la difesa, dal punto di vista costituzionale. Sicuramente, non può farlo l'interno, o un'altra istituzione di *law enforcement*, e gli attacchi non verranno dall'interno dell'Italia.

Bisogna sviluppare relazioni multilaterali e creare un'infrastruttura di *cyber intelligence*. Dobbiamo capire quello che ci accade intorno, molto legato all'*information sharing*, all'*active defence*. Forse qualcuno di voi saprà che l'NSA *(National Security Agency*), elemento cardine della famiglia di *intelligence* americana sul *cyber*, è talmente legata all'*active defence* che questo legame è definito dal fatto che c'è lo stesso capo. Hanno deciso di mettere anche la stessa persona fisica a comandare le due strutture.

Passo ora alle linee operative, tra cui il *framework* nazionale e il *cyber range*, dove avanzare gli *skill* delle nostre parti militari e civili. Sul *framework* nazionale siamo partiti, sul *cyber range* credo che da Chiavari stiano arrivando notizie positive. È partito il CERT nazionale *(Computer Emergency Response Team*), c'è il controllo della *supply chian*, c'è *Internet governance*, un tavolo che dobbiamo assolutamente presidiare. Non so nemmeno se qualche italiano vada all'*Internet governance*, ma rientra anche nello sviluppo delle relazioni multilaterali e bilaterali. Anche se realizzassimo il miglior sistema di *information sharing* in Italia, è chiaro che non andiamo da nessuna parte senza ramificazioni internazionali. Quello è una linea strategica, e l'*Internet governance* è la linea operativa che va seguìta. Magari su qualcuno di questi punti, per esempio la Nazione imprenditore, mi piacerebbe tornare verso la fine.

Passo ad un pezzo del percorso americano che porta due *executive order* sull'*information sharing*. Il primo ha dato luogo al *framework* del NIST *(National Institute of Standards and Technology*). Il secondo è quello che farà transitare i sistemi di *information sharing*, i cosiddetti ISAC americani *(Information Sharing and Analysis Centers*), agli ISAO *(Information Sharing and Analysis Organizations*).

I primi erano fondamentalmente lasciati al privato, un'organizzazione privata di aziende dello stesso settore, che condividevano informazioni. Negli ISAO c'è anche la parte pubblica, quindi non soltanto le aziende private dello stesso settore – se c'è un attacco verso l'azienda di un certo settore, con altissima probabilità anche altre aziende di quel settore verranno attaccate nello stesso modo – per dare forza a questo anche la parte della famiglia di Intelligence degli Stati Uniti entrerà dentro i cosiddetti ISAO.

L'implementazione è, però, complessa. Lo è negli Stati Uniti, lo sarà in Italia. C'è poco da fare. Ci sono problematiche economiche dietro, ma dobbiamo avere chiara la direzione dove andare, non a 360 gradi, e per questo è importante il *framework* nazionale per la *cyber security*, come uno dei paletti che dice che si va in una certa direzione. L'implementazione è complessa perché la consapevolezza è bassa.

Vi mostro ora un rapporto sullo stato della consapevolezza degli impiegati pubblici americani. Credo ci sia scritto che la *password* più utilizzata nei sistemi da parte degli impiegati pubblici è « password ». Mi sembra che dica questo. È chiaro che stiamo parlando di un Paese che comunque, da un punto di vista tecnologico, su questa materia è molto avanti e molto attenzionato, anche per questo.

Ho anche cercato di fare un esercizio per darvi un'idea di come negli Stati Uniti si gestisce questo problema. Abbiamo la parte difesa, con Darpa, Cyber Command, NSA, CIA, FBI, DHS *(Department of Homeland Security)*, NIST, che lavora con le industrie e gestisce tra l'altro il *framework* per la *cyber security* omologo americano, mentre il DHS gestisce tutta la parte ISAO. Tutti questi sono legati alle linee strategiche che vi dicevo. Questa è un po' la figura: tutto si raccorda nella White House, dove c'è una sorta di comitato, dove c'è un *representative* di ognuno,

tranne forse che dell'NSF *(National Science Foundation)*, che è proprio ricerca pura. Gli altri stanno sicuramente all'interno di questo gruppo.

Per l'Italia, come sapete meglio di me, quindi andrò molto veloce, c'è il decreto del Presidente del Consiglio Monti, il piano strategico, e il 13 maggio 2014 nasce il Laboratorio nazionale di *cyber security*, e poi vi farò vedere alcune cose su questo. Nasce poi il CERT nazionale e abbiamo avuto il *cyber security*, il *framework* italiano per la sicurezza cibernetica.

È chiaro che stiamo facendo cose, le stiamo facendo in un panorama istituzionale, che è il seguente, che esce fuori dal decreto Monti. Credo che non ci sia bisogno di spiegare questa struttura, che sicuramente da un punto di vista costituzionale è assolutamente corretta. Bisognerà vedere se raggiunge la velocità necessaria. Il problema non è nel nostro spazio. Certamente, è fare qualcosa che sia costituzionalmente ben fatto. D'altra parte, il problema è stare dietro a questa velocità.

Abbiamo, per esempio, il NSC (Nucleo pianificazione Sicurezza Cibernetica), l'organismo che viene chiamato nel momento stesso in cui l'attacco di tipo cibernetico diventa sistemico verso l'Italia. Immagino che il NSC sia un'incarnazione del CISR (Comitato interministeriale per la sicurezza della Repubblica), per cui vi parteciperanno tanti quanti sono i membri di questo Comitato, e magari sarà giunta AgID o qualcun altro.

Il problema è quali sono i tempi di reazione che ha tutta questa struttura. Questo è il punto fondamentale. Noi andiamo avanti con attacchi che si dispiegano in un certo tempo: magari per la preparazione ci vogliono settimane, ma quando partono sono molto veloci. Dobbiamo avere una struttura che abbia quella velocità o riesca ad avere velocità, poi riprendiamo più avanti il concetto di velocità. Non voglio dire se va bene o meno. Cartesianamente, dobbiamo misurare la velocità di questa struttura (definita dal citato decreto Monti): se raggiunge la buona velocità, siamo tutti felici, altrimenti bisognerà ripensare la cosa.

Ecco alcune *slide* sul Laboratorio nazionale di *cyber security*. Parte dal CINI, un Consorzio interuniversitario nazionale per l'informatica. Di fatto, riunisce tutta l'informatica italiana. Tutti i professori di informatica italiana sono all'interno del CINI. La relazione tra accademia e architettura *cyber* governativa, in particolare la Presidenza del Consiglio dei ministri, parte nel 2010, quando in « Sapienza » si definisce un tavolo di lavoro misto su queste problematiche. Il tavolo ha dato luogo a una serie di operazioni soprattutto inizialmente educative, come *master* e simili. Il punto fondamentale è che nasce CIS Sapienza, un organismo che racchiude circa sessanta ricercatori su tre aree distinte: economia, giurisprudenza e tutta l'area tecnologica. Il problema è, infatti, multidisciplinare.

Noi siamo, però, un po' diversi rispetto al Regno Unito, non è facile in Italia creare otto centri di ricerca che coprano il territorio nazionale, Polimi, Polito, Federico II, cercando di strutturare l'iniziativa in modo che, se « Sapienza » avrà una responsabilità sulla parte *cyber*, un'altra università l'avrà sulle biotecnologie, tentando una razionalizzazione. Discorsi di questo tipo in Italia sono molto complessi.

Che cosa abbiamo fatto ? Ricevevamo come CIS Sapienza telefonate in cui si chiedeva aiuto per organizzazioni su tutto il territorio nazionale, ma siamo professori universitari, non possiamo rispondere a queste richieste. Abbiamo deciso di lavorare su scala nazionale. Abbiamo iniziato un percorso, che devo dire i miei colleghi hanno condiviso forse proprio perché noi informatici vediamo già quello che potrà accadere, come vedevamo il discorso *cloud*, i *data center*. Vediamo il futuro e capiamo la minaccia.

Rispetto ad altre operazioni è stata una presa d'atto e un unirsi, come si è confermato alla manifestazione dell'altro giorno in « Sapienza », dove era praticamente presente tutta la comunità accade-

mica di *cyber security* italiana, a parte quella governativa e quella industriale. Da lì è nato il Laboratorio nazionale.

A quel punto abbiamo stretto accordi con la Presidenza del Consiglio dei ministri, che ha visto positivamente e ha seguìto questa nascita, col CERT nazionale, e abbiamo iniziato a fare iniziative e progetti. Noi viaggiamo a un'altra velocità, devo dirvelo molto onestamente. Sentirete molte storie sull'ambiente universitario. Io devo dirvi, che per quanto riguarda almeno l'informatica, noi veniamo valutati e ci mettiamo in gioco ogni giorno di fronte al contesto internazionale. Punto. Io sono quello che rifletto in ambito internazionale, e i miei colleghi sono la stessa cosa. Viaggiamo, quindi, a un'altra velocità.

Con questa velocità abbiamo realizzato il libro bianco, abbiamo portato a casa il *framework* nazionale, che può essere perfettibile, ma c'è adesso, per cui ora il problema è spingerlo. Lavoriamo su una serie di progetti molto rilevanti. Il problema era fare massa critica. Se io sono un professore bravissimo su un certo tipo d'attacco, ma sono io col mio dottorando, non riusciamo a fare massa critica. Se, però, unisco questo professore che sta a Trento, quest'altro che sta a Modena, quest'altro che sta a Perugia e faccio un *team*, allora le cose cambiano. Questo è stato il punto fondamentale.

Chiaramente, siamo universitari, quindi ci piace la parte metodologica, con la definizione di *framework* e metodologie, implementazione di programmi di formazione a livello nazionale. Quello che portiamo di più importante sono le nostre reti di relazioni internazionali. Questo è uno dei punti fondamentali, che secondo me possono tornare molto utili al sistema Paese.

Il Laboratorio nazionale adesso è su 36 siti, almeno credo. Ci sono i nostri gioielli di famiglia là dentro, e sicuramente CIS Sapienza è un gioiello di famiglia. Ce ne sono altri. Ci sono anche altri meno ingaggiati, ma è importante avere un presidio sul territorio, perché per esempio può essere una spinta per il *framework* nazionale. Le associazioni di categoria non verranno tutte da me. Sarebbe assurdo, torneremmo al problema precedente, invece dobbiamo cercare di distribuire questa conoscenza, portarla sul territorio. Abbiamo dentro ENEA, FBK, stiamo chiudendo l'accordo col CNR. Questo porterà ad avere « l'interfaccia per la ricerca » per il sistema governativo.

Oltre all'accordo col CNR, stiamo portando avanti anche un accordo con LUISS, Scuola Superiore Sant'Anna e IAI (Istituto affari internazionali). Qui la maggioranza è tecnologica. Questo è, ricordate, il CINI (Consorzio interuniversitario nazionale per l'informatica). Abbiamo bisogno all'interno come il pane di organizzazioni che portino le altre competenze: la geopolitica la parte normativa, la parte economica. È per questo che ci stiamo muovendo in questa direzione.

Vengo a che cos'è la ricerca in Italia in sicurezza e che tipo di *asset* è. Abbiamo messo anche il numero di progetti che è stato acquisito dall'Italia in FP7, quindi prima di Horizon 2020. Notate che siamo secondi solo alla Germania. La parte blu, che è quella accademica, è di gran lunga la seconda dopo la Germania. Lì competiamo su *call* dove passa un progetto su dodici, e un progetto significa tre mesi non del lavoro di un ragazzo, ma di mio lavoro o del lavoro di un mio collega. È per darvi un'idea della qualità che c'è in questo momento in Italia in questo settore. È una finestra. La qualità c'è adesso, tra qualche anno non ci sarà più, e potete immaginare perché: l'Università non fa *hiring* da tempo.

Con il *Cyber security national Lab* stiamo cercando di realizzare un'interfaccia verso l'architettura attuale di *cyber security* o verso quella che sarà un giorno. In ogni caso, c'è sempre un *cloud* governativo. Anche da questa parte si sta cercando di razionalizzare così come nella parte impresa. Vi sono alcuni dei progetti che stiamo portando avanti in questo momento con diversi attori, tenendo anche il coordinamento tra tutte queste iniziative.

Per quanto riguarda il piano strategico, lavoriamo su sei indirizzi operativi all'interno di quei progetti.

MASSIMO ARTINI. Presidente, avrei alcune domande che riguardano tutta la parte che è stata trattata finora.

ROBERTO BALDONI, *Direttore del Centro di Ricerca Sapienza in Cyber Intelligence e Information Security (CIS)*. Posso anche rispondere adesso, se lo ritenete.

PRESIDENTE. Facciamo delle domande su questa parte, e poi passiamo alla seconda con le conclusioni. Do la parola all'onorevole Artini.

MASSIMO ARTINI. Anzitutto, professore, grazie per l'ampiezza della sua relazione. L'obiettivo di quest'indagine è prima di tutto renderci consapevoli di cosa sia questo mondo. Effettivamente, le *slide* e la trattazione che ne ha fatto hanno estremamente chiarito tutti i punti. Lei ha avviato il ragionamento indicando le minacce, per poi passare a come queste sono state risolte.

ROBERTO BALDONI, *Direttore del Centro di Ricerca Sapienza in Cyber Intelligence e Information Security (CIS)*. Non si sono risolte. Sono passato a come si stanno affrontando.

MASSIMO ARTINI. Sì, e da vari sistemi, non solo quello nazionale, ma anche all'estero.

La prima domanda è quella relativa a quale genere di sovranità dobbiamo aspettarci su questo tipo di ambiente. In questo mondo, la sovranità dipende anche dalla capacità di controllo che si ha sui sistemi *software*, *hardware* e *firmware* che si sviluppano o si hanno nella vita normale. In questo c'è una divisione ampia tra privati, enti, infrastrutture critiche e Stato.

Per garantirsi questa sovranità, può bastarci solamente un livello di certificazione rispetto ai materiali introdotti in Italia oppure è opportuno, anche per dar seguito a quello che ha detto lei, rimanere agganciati a questo settore industriale che sarà il futuro per i prossimi cento anni o anche di più ? Che genere di sovranità e capacità lo Stato dovrebbe essere in grado di sviluppare insieme a tutti gli attori, l'università nella parte di progetto, industrie certificate per questo tipo di lavoro e via dicendo ?

Detto questo, anche lei si è posto la stessa questione: la struttura del decreto Monti è una mera fotografia dell'esistente o è qualcosa che ha permesso di fare qualche passo in avanti ? Anche dalla sua valutazione, senz'altro qualche passo è stato fatto, altrimenti dal 2013 al 2014 non sarebbe nato il Laboratorio né ci sarebbe stata tutta una serie di passaggi che, senz'altro per il tramite della Presidenza del Consiglio, hanno avuto un seguito. Nel caso di un'effettiva necessità di risposta a una minaccia, il fatto che il Nucleo di sicurezza cibernetica sia un insieme di attori abbastanza ampio, con più soggetti da coinvolgere affinché sia presa una decisione, è un punto che può essere sanato rispetto alla situazione attuale anche di parcellizzazione dei vari CERT ? La situazione del CERT nazionale, del CERT-PA, del CERT difesa, dei vari CERT – e penso a quello dei Carabinieri e così via – ha un senso o, in prospettiva, come legislatori è più opportuno ragionare su un'agenzia o un dipartimento sotto la Presidenza del Consiglio ?

Sulla parte difesa ha fatto un appunto che mi trova perfettamente d'accordo. Non può essere altro che il mondo delle Forze armate a fare questo tipo di lavoro. Mi chiedo se ci sia stata da parte vostra, anche in maniera molto astratta, una valutazione non solo sulle approvazioni politiche che devono essere nell'alveo di quel rispetto costituzionale. È guerra o non è guerra un attacco o un contrattacco rispetto a quello che può essere l'attacco di un altro Stato ? Che tipo di minaccia dobbiamo aspettarci ? Di questo problema il Paese deve essere reso consapevole.

Faccio poi una domanda sulla consapevolezza. La consapevolezza deve essere a tutti i livelli, aziendale, privato, ma

anche di Stato. Non vorrei che succedesse che in delle situazioni, per una noia ad aggiornare delle *password*, alti dirigenti impongano la rimozione di determinati livelli di sicurezza perché manca questo tipo di consapevolezza.

Su questo – chi meglio dell'università, o comunque della parte di scuola può rispondere – che tipo di formazione anche a lungo termine può essere introdotta per rendere consapevoli su questo tipo di problema ?

Infine, lei ha detto che non avrebbe voluto valutare il discorso numeri, ma un dato mi interessa, e se ci fosse una valutazione anche da parte dell'università rispetto a quello che dovrebbe essere il corretto stanziamento finanziario sulla parte di *cyber* sicurezza. Al momento, tutti i CERT, CERT-PA, CERT nazionale, che io sappia, non hanno fondi o capitoli di bilancio stanziati, ma lavorano rispetto alle spese generali, e quindi hanno una difficoltà di programmazione che in questo mondo è drammatica.

Vero è che nell'ambito della legge finanziaria c'è stato uno stanziamento di almeno 150 milioni di euro, se non ricordo male, che però copre tutto l'ambito cibernetico, sia la parte di *law enforcement*, sia quella di difesa prettamente militare e così via.

A chiosa di tutto questo, mi domando se non sarebbe opportuno concentrare le forze dei vari CERT e che da quelli nasca un sistema di *information sharing* unico e un sistema di linee guida che venga anche dipanato in maniera gerarchica presso gli enti che ne hanno necessità ? Lei ha citato giustamente l'esempio della piccola azienda che magari collabora col Ministero della giustizia e che non ha sistemi di difesa, però ha un contatto sempre diretto, una chiavetta normale, e vengono introdotti sistemi di hackeraggio, di virus, che vanno a ledere i diritti di un determinato cittadino.

L'altro giorno ero all'incontro che si è tenuto alla « Sapienza ». Anche lei ha riportato la mia preoccupazione. Gli americani si stanno spostando dalla struttura esclusivamente volontaria da parte delle aziende verso qualcosa di diverso. Per esperienza, in maniera volontaria le aziende fanno ben poco. I sistemi di imposizione nelle aziende sono quelli che funzionano meglio. La parte pubblica come può essere un attore fondamentale ? Non deve imporre determinati standard, ma dovrebbe svolgere un ruolo che aiuti a sviluppare questo sistema.

L'imposizione di standard o di regole impatta su quanto questo è costato. Il dottor Caroti, di Terna, l'altro giorno parlava delle disposizioni minime del decreto legislativo n. 196 del 30 giugno 2003, teoricamente perfette, ma che nella reale applicabilità è difficile imporre ai clienti. Mi chiedo se nell'ammontare finanziario dovrebbe esserci come obiettivo dello Stato quello di rendere questo sistema qualcosa di facilitato da fondi a cui le aziende possono accedere.

Vale il sistema delle alleanze: siamo un po' all'inizio di questa storia, perché le alleanze tra Stati crollano, si pensa al *Datagate* e all'acquisizione direttamente da parte degli Stati. Tutto crolla anche rispetto ad alleanze strutturate da decenni. Vale lo stesso nel ragionamento tra aziende, e il fatto che io debba poter fare in modo che questi sistemi siano implementabili. Diversamente, relativamente a tutte quelle che rimangono decisioni che possono essere prese sulla carta, mi domando, se ho una polizia che protegge in maniera « gratuita », perché pagata con la fiscalità generale, perché lo Stato non debba iniziare a pensare di dotarsi di sistemi che sulla parte di difesa cibernetica possano essere non dico gratuiti, ma non totalmente a carico di chi subisce danni.

LUIGI LACQUANITI. Ringrazio il professor Baldoni. Vorrei tranquillizzarla, la mia domanda sarà una sola.

Faccio riferimento all'evoluzione storica dal secondo dopoguerra a oggi. Sia per motivi di ordine politico, sia per risorse materiali ed economiche, si sono sviluppati dei grandi blocchi e delle grandi superpotenze. Questo schema si è riprodotto nel tempo con l'evoluzione dei

sistemi di difesa. Ancora oggi possiamo dire che ci sono dei grandi blocchi e delle grandi superpotenze. Per quanto riguarda il nostro sistema di difesa, siamo un po' piccolini, abbiamo il nostro sistema di difesa, non abbiamo mai avuto grandi risorse materiali ed economiche. Il tipo di sistema che oggi ci ha esposto è un universo in esplorazione per quanto ci riguarda, e la ringrazio per questo motivo. Mi ricollego anche a una delle ultime *slide*, dove è esposto l'apporto del mondo accademico, molto interessante anche nel confronto con il mondo accademico degli altri Paesi.

Per questo tipo di sistemi di difesa dobbiamo pensare che anche nel futuro si riprodurrà lo stesso schema, per cui ci saranno delle grandi superpotenze, si richiederanno grandi risorse economiche ? O possiamo pensare che per il tipo di sistema di difesa di cui stiamo parlando si potrà per una volta pensare che anche il nostro Paese può avere un ruolo di primo piano nel panorama internazionale ?

ANGELO TOFALO. Sarò veramente brevissimo, anche perché cercherò di soffermarmi solo su una parte, poi magari mi riserverò delle altre conclusioni.

Su scala internazionale, relativamente alla problematica dell'*attribution* dell'attacco, quali sono gli ultimissimi aggiornamenti ?

Ha poi citato l'esempio di Hacking Team, che abbiamo seguìto tutti. Vorrei porre una questione perché vorrei che restasse a verbale. Quando un qualunque tipo di virus – anche quelli che sono stati più pubblicizzati attraverso le notizie di stampa – porta un attacco del genere, e prende possesso anche di uno *smartphone* o di un PC, oltre a prendere i dati, è possibile anche modificarli o inserirne di nuovi ?

Ci ha mostrato la struttura, che conosciamo tutti, che va dalla Presidenza del Consiglio fino al NISP, al CISR tecnico. So che non vi compete, e ho apprezzato molto il lavoro che state facendo, ma volevo chiedervi se state ragionando anche su chi, come, quando, sui i termini dell'attacco e i tempi per intervenire quando il NISP rileva qualcosa. Vedo che c'è moltissima confusione proprio in questa parte, da parte del legislatore, tra ministeri, agenzie, eccetera. Vedo che qui nessuno riesce a metterci mani: avete una vostra idea dopo tutto questo studio fatto ?

Mi riservo comunque di intervenire dopo per ulteriori considerazioni.

PRESIDENTE. Cedo adesso la parola al nostro ospite per questa prima tornata di risposte.

ROBERTO BALDONI, *Direttore del Centro di Ricerca Sapienza in Cyber Intelligence e Information Security (CIS)*. Queste prime risposte mi permettono anche magari di saltare alcune *slide* successive.

Quanto al discorso della sfida per quanto riguarda la certificazione *hardware*, *software* e componenti, se legge il libro bianco, è una delle sfide fondamentali. Dobbiamo trovare un'*Italian way* per farlo. Mi spiego meglio, partendo dalla cosa più difficile per noi, ossia la componentistica *hardware*.

Noi non siamo più un Paese, ahimè, che produce *hardware*. La Francia ha avuto il coraggio di mantenere *bull* anche quando la situazione economica era molto drammatica. A questo punto, si trovano comunque una serie di competenze che noi abbiamo perso.

Da questo punto di vista, sarà estremamente importante – diverso è il discorso per il *software*, su cui siamo dei buoni *player* – che troviamo un modo italiano per approcciarci al problema degli approvvigionamenti *hardware* per le Forze armate, per l'*intelligence e per l'interno*. Bisognerebbe pensare in modo molto meticoloso e trovare qualcuno che rifletta su questo punto.

Si possono tirar fuori delle metodologie. È vero che non produco più *hardware* all'interno del mio Paese, ma posso pensare di produrlo all'interno di due o tre Stati, prendo un progetto, lo divido in pezzi, faccio fare un pezzo alla Cina, un altro agli Stati Uniti, e poi mi doto di una

capacità di assemblaggio in Italia. Va studiato. È un problema molto rilevante. Possiamo pensare a tutti i *framework* o ai *cyber range* che vogliamo, ma se poi non abbiamo la certezza che l'*hardware* che imbarchiamo nei nostri sistemi è « pulito », tutto cade miseramente. C'è bisogno di una forte riflessione. È una delle sfide che elenchiamo là dentro: come arrivare a quest'approvvigionamento di componenti *hardware* in modo « sicuro ».

Sul discorso NSC e su altre domande che riguardano l'architettura nazionale, avevo una *slide* nelle conclusioni, che voglio anticipare: riguarda la necessità di sviluppare la capacità di difesa attiva. Tornando al discorso dei costi, lo sviluppo di queste cose non è particolarmente oneroso. Dico spesso che bisognerebbe dare alla ricerca una ruota di un *F-35*. Abbiamo fatto tutte le cose che avete visto senza risorse, a costo zero come previsto dal decreto Monti. Abbiamo i nostri canali, fortunatamente siamo abbastanza ricchi, perché abbiamo progetti in Europa, quindi riusciamo a fare anche queste operazioni.

Non c'è bisogno, però, di grandi cifre, non stiamo parlando di grandi investimenti per essere una potenza degna di una Nazione che è all'interno del G7. Magari tra cinquant'anni i discorsi saranno un po' diversi, ma sicuramente l'investimento di cui c'è bisogno non è paragonabile – all'interno della *cyber security*, sia per scopi di difesa ma anche per scopi civili – a quelli che si possono trovare nelle armi classiche (navi, aerei, eccetera). Qui stiamo parlando di ordini di grandezza inferiori rispetto a questi piani.

Questo ci permetterebbe comunque di avere le nostre capacità deterrenti e un innalzamento delle difese dei vari attori pubblici e privati. Che cos'è poi la resilienza di un Paese ? È Terna, Barilla e la difesa che mettono un pezzettino e diventano più resilienti. È l'unione di tanti mattoni che mettiamo noi. Mio nipote capirà, la prossima volta che compererà un PC, che dovrà metterci un antivirus. Parlo di mio nipote, che sa quello che faccio. Ha preso un computer, si è collegato a *Internet*, ha iniziato a scaricare i giochi più in voga tra gli adolescenti: dopo una settimana il computer non funzionava più. Aveva preso tanti di quei virus che avevano bloccato addirittura il computer.

Questi discorsi sono importanti. Per questo è un discorso di sistema Paese, è un discorso culturale. Purtroppo il futuro è complesso. Sembra più semplice, ma è più complesso. Sembra più semplice perché abbiamo i nostri *smartphone* con accesso a informazioni. Per carità, è tutto vero e tutto giusto, ma è più complesso.

Un'altra cosa importante è che, per affrontare questo futuro, dobbiamo muoverci come sistema Paese. Dimentichiamoci dell'idea dell'italiano che mette su l'azienda soltanto dotato di estro. Sicuramente l'estro ce l'abbiamo, le capacità e così via, ma queste sono cose che dobbiamo affrontare a livello sistemico, altrimenti non ne usciremo e torneremo quel Paese in continua deindustrializzazione e fuga di persone di alto profilo da un punto di vista tecnologico, con l'immissione di una serie di persone, magari immigrati, che invece hanno un livello tecnologico basso. Da qui a cinquant'anni avremo cambiato completamente, e non in meglio, il profilo di questo Paese.

Inoltre, l'architettura nazionale *cyber* deve acquisire velocità. Dobbiamo veramente guardare questa struttura e capire se possa raggiungere questa velocità di reazione. Va considerata un'altra cosa fondamentale: ci vogliono le competenze in questo settore. Abbiamo uno *shortage* di competenza a livello mondiale, poi in Italia abbiamo il nostro, ma se gli esperti superano le Alpi guadagnano dieci volte quello che guadagnano da noi; se superano la Manica, guadagnano venti volte e se vanno dall'altra parte dell'oceano, ancora di più, perché vengono presi da grandi assicurazioni.

Ogni grande banca ha il *cyber command*, non solo per scopi difensivi, ma anche per fare *intelligence* sulle mosse degli avversari. Capiamo come si sta muovendo il mondo. Dobbiamo assolutamente avere competenze. Su questo ci metto

anche l'università, che deve migliorare i propri programmi in *cyber security*. La cosa migliore sarebbe, come hanno fatto in Inghilterra, un approccio che coinvolga i famosi ministeri del CISR, dando a ognuno di questi la sua fetta sia di risorse sia di operatività, e una di queste riguarda appunto la crescita delle competenze *cyber* in Inghilterra. Andrebbe preso il MIUR e andrebbe spiegato che forse andrebbe un attimo indirizzato anche il Paese secondo il futuro.

Quindi, serve certamente una semplificazione dell'architettura, se si riesce. Più si semplifica e meglio è, con le competenze all'interno. Come ho detto diverse volte negli ultimi anni, l'altra cosa fondamentale è un chiaro *cyber commitment,* ossia un impegno sulla *cyber security* nella missione dell'organizzazione di almeno una struttura (Agenzia, Dipartimento, eccetera). È chiaro che le competenze *cyber* devono essere distribuite su più strutture, ma se penso al MISE, per esempio, questo ha i suoi obiettivi, le sue strategie: la *cyber* è al centro delle strategie del MISE ? Non lo so, forse qui mi aiutate voi, io non credo.

Si può decidere la strategia e imporre la competenza. A quel punto, queste cose si traducono in *budget*. Quando si va a litigare per la torta di un ente, al *cyber* vengono date le briciole. Secondo me, servono semplificazione e un chiaro *cyber commitment* di almeno una struttura, che si individui una struttura *cyber*. Come si chiamerà non lo so, non sono esperto da poter capire da un punto di vista istituzionale le possibili strade, ma deve esserci qualcosa che abbia l'etichetta « c*yber* » per indicare che è quello che fa le metodologie per la componentistica *hardware*, noi gestiamo il *framework*, noi faremmo il *cyber range*, noi daremo le direzioni alle varie organizzazioni di quello che dovranno fare per difendersi. Secondo me, questo va centralizzato.

Quanto alle approvazioni politiche rispetto a operazioni di *cyber command,* se mi metto a studiare, esco fuori magari con un mio commento, ma non so rispondere a questa domanda adesso.

La consapevolezza rispetto al *cyber risk* dobbiamo costruirla. È un percorso complesso. Come lo è negli Stati Uniti, lo sarà in Italia, ma è una strada secondo me obbligata.

Su tipo e quantità di spesa vi cito un esempio: il consolidamento dei *data center* in Italia. Lo scorso anno abbiamo redatto il *Cyber security report* – in quello di quest'anno c'era il *framework* – dedicato alla pubblica amministrazione, e l'abbiamo fatto in collaborazione con AgID, mostrando le debolezze della pubblica amministrazione italiana. Se non l'avete letto, fatelo, perché veramente troverete informazioni interessanti.

Una delle cose che mi ha sconvolto durante la preparazione è che in Italia abbiamo ordine di decine di migliaia di centri di spesa in grado di acquistare *hardware* e *software*: un certo comune, quell'ospedale, quella determinata scuola. Dove troviamo decine di migliaia di esperti in sicurezza che vanno lì e difendono queste strutture ? C'è un passaggio logico, grazie al *cloud* o ad altro, che deve portare alla realizzazione di un *asset* nazionale, che deve essere un'infrastruttura che permette agli utenti più piccoli di connettersi a queste strutture e ricevere i servizi da lì. Parliamo di consolidamento di *data center* italiani, che rappresenterebbero una struttura portante per l'economia del Paese.

Pensate a una piccola e media impresa, che se in questo momento vuole andare su *cloud*, deve andare su un *provider* straniero, e sotto quali regole di *privacy* ? Nessuno lo sa. Non abbiamo nemmeno il *Safe Harbor* adesso. I loro dati li portano dall'altra parte dell'oceano, e che ne sappiamo di che cosa ne fanno ? In questo mondo basta vedere LinkedIn per capire la dimensione dell'azienda. Io vedo le persone che lavorano dentro quest'azienda. Se sono una grande *corporation*, quell'azienda me la compro, comprando tutti i suoi impiegati.

È fondamentale, quindi, avere un *asset*, altrimenti si rientra nella spesa corrente. Quando abbiamo 40.000 centri di spesa, è chiaro che la spesa in informa-

tica diventa spesa corrente, che sta sotto la scure di una *spending review*, che giustamente deve fare il suo dovere, mentre questo è un *asset* nazionale, per cui va consolidato. A quel punto, se avremo cinquanta *data center* in Italia tra pubblica amministrazione centrale, includendo anche la difesa, e l'amministrazione pubblica periferica, allora abbiamo un numero di esperti in sicurezza ragionevole, che possiamo acquisire e che possono fare il loro lavoro. Come facciamo, però, su 40.000 centri di spesa ?

Una delle cose che ho detto è di mettere l'agenda digitale al centro del Paese, ma realmente, mettendo da parte questi 40.000 centri di spesa. Di che cosa stiamo parlando ? Di fare già domani una legge per incentivi e disincentivi, e o ci si attacca a quella struttura nel giro di due anni o non si avranno più soldi propri per l'informatica. È con le grandi infrastrutture che si muove il Paese.

Abbiamo fatto una rivoluzione economica in Italia quando c'è stato il *boom* sulle infrastrutture: autostrade e ferrovie. Un *boom* economico nel futuro su che cosa sarà ? Su che cosa può essere ? Su autostrade e infrastrutture ? Non credo. Lo stesso discorso vale per una guerra nel futuro: sarà come l'abbiamo conosciuta finora ? Non credo. Sicuramente, quantità e tipologia della spesa sono fondamentali.

Sulla quantità vi ho detto del Regno Unito e del miliardo di *pound* in cinque anni. Stessa cifra è stata stanziata dalla Francia.

MASSIMO ARTINI. In Israele, se non sbaglio, si parla di 3 o 4 miliardi di dollari l'anno come investimento.

ROBERTO BALDONI, *Direttore del Centro di Ricerca Sapienza in Cyber Intelligence e Information Security (CIS)*. Israele mi porta a un altro punto: quello delle *start up*.

Ho parlato di Stato imprenditore. Mettiamoci adesso nell'ottica in cui il Parlamento riesca a trovare anche la migliore architettura nazionale possibile. Non ci dobbiamo dimenticare, tuttavia, che siamo nell'alveo del pubblico che, come in America, anche qui è lento. Questa struttura, invece, ha bisogno di velocità, quindi è fondamentale l'interazione col mondo esterno, perché la ricerca e il privato danno velocità e perché il problema è comune.

Per quanto possiamo, sicuramente ci sarà la possibilità di migliorare l'architettura, ma il problema è proprio legato al pubblico. Oltre una certa velocità non si potrà andare, e quindi bisogna sfruttare una serie di altre situazioni, tra cui l'interazione con la ricerca, ma non solo. Abbiamo degli acceleratori naturali: G7, NATO, Unione europea. Dobbiamo sfruttare le onde che creeranno. Sono certo che in quei contesti arriveranno accelerazioni, su cui forse voi come Commissione difesa, soprattutto sulla parte NATO, potrete avere a breve delle notizie in merito.

Quello che non dobbiamo fare è rimanere immobili o a bassa velocità. A quel punto, o verremo lasciati alla deriva o verremo messi in sicurezza da altri: in entrambi i casi, non è una bella prospettiva per i nostri figli e per il nostro Paese. Rispetto alla guerra fredda, ai due blocchi, se qualcuno ci mette in sicurezza, avrà il controllo di tutti i nostri dati, di tutto quello che facciamo. Può essere una prospettiva, va bene. Io spero di no. Se sarà questa la prospettiva, pian piano vedremo sempre più persone che andranno via.

Quanto alle facilitazioni fiscali, sarebbe molto interessante un discorso del genere. Sarebbe bello concepire delle agevolazioni fiscali per quelle aziende che cercano di adottare il *framework*, e quindi iniziano un percorso importante. Stavo dicendo, tornando a Israele, che la cosiddetta « *Start up Nation* », per chi la frequenta come me da diversi anni, per tanti colleghi che ho nelle varie università, ha visto proprio cambiare Israele da così a così. In tale Paese è lo Stato che ha investito molto in quest'interazione tra università e difesa, ma anche tra università e settore pubblico.

In questo momento, i miei colleghi vengono valutati in Israele per il numero di *start up* che aprono. In base a questo

danno loro le sedie dentro i dipartimenti, i posti dove poter sviluppare le cose.

Credo che Israele sia l'esempio di come, senza troppe risorse economiche, si possa riuscire a creare un certo sistema. Quello che colpisce di più in Israele è che non si capisce più in questo momento quando parli con l'università o quando con qualcosa di privato, con una *start up*, è un tutt'uno. Questo segue molto *Internet*, è veramente un amalgama. Lo Stato aveva bisogno di una serie di cose e – comportandosi come un imprenditore – ha favorito la crescita di aziende in alcuni settori. Anche in altri Paesi fanno così. Bisogna vedere la sicurezza non soltanto come un problema. La sicurezza del nostro Paese è certamente importante, ma bisogna vederla anche come opportunità economica, creazione di *start up*, che possono essere stimolate anche dal pubblico.

L'attribuzione è un bel problema. Ci stiamo lavorando. È un problema reale. Gli israeliani credono che non sia un vero problema. Secondo me, siamo lontani da un'attribuzione. Loro sono un po' più grossolani forse nell'attribuire cose, mentre secondo me l'attribuzione è ancora un problema tecnicamente non indirizzabile, sempre se il livello dell'attaccante è tale per cui sa fare il suo lavoro. Non è banale.

Il *framework* ve l'ho illustrato, in pezzettini. Sicuramente troverete tutte le informazioni anche sul documento che vi ho lasciato. C'è anche una serie di articoli usciti che cercano di spiegare il *framework* nazionale.

ANGELO TOFALO. Forse mi sono perso un passaggio: una volta che ha preso possesso di una macchina il *malware* o il virus, è possibile, oltre che prendere i dati, inserirli e modificarli ?

Ho avuto il piacere di ascoltarla anche alla « Sapienza ». È mia opinione convinta che questi 150 milioni di euro servano a malapena a mettere mano sui ministeri, sull'Agenzia, e a cercare nemmeno una struttura, ma un'idea di struttura, che poi operi come cabina di regia. Da quello so, da un'analisi un po' internazionale, se non spendiamo almeno 2 miliardi di euro, ragionando sul sistema Paese, su strutture critiche – quel discorso israeliano mi piace di interazione tra tutti – non ne veniamo fuori.

Dico da politico che, ahimè, la politica è ancora molto distante da queste problematiche, anche se per fortuna adesso si inizia a parlare: come facciamo a sopravvivere ? Qual è lo scenario ? Ha detto più volte che tra qualche anno ci saranno i cervelli in fuga e le persone fuggiranno: il mio timore è lo stesso.

ROBERTO BALDONI, *Direttore del Centro di Ricerca Sapienza in Cyber Intelligence e Information Security (CIS)*. Ripeto che credo molto negli acceleratori naturali.

ANGELO TOFALO. Oltre a diffondere una cultura della sicurezza cibernetica, a costo zero che cosa possiamo fare ? Concludo invitandola a continuare a correre su questa strada. Una voce almeno in Parlamento c'è. Ho visto che molti colleghi anche dell'altra parte, al di là del colore politico, sono sensibili. La voce qui ci sarà. Il mio invito è a continuare a correre, ma, attualmente, a costo zero che cosa possiamo fare noi ?

ROBERTO BALDONI, *Direttore del Centro di Ricerca Sapienza in Cyber Intelligence e Information Security (CIS)*. A costo zero, secondo me dobbiamo aumentare la consapevolezza. Ho un'idea in mente, una sorta di pubblicità progresso, per cercare di far capire alle persone le problematiche che questo mondo porta.

Immagino uno *spot* in cui si vede un'azienda florida, medio piccola, che a un certo punto per qualche motivo nel giro di un paio d'anni perde tutte le quote di mercato e non capiscono perché. Questo è uno *spot* che secondo me potrebbe iniziare a far ragionare soprattutto le piccole e medie imprese. Abbiamo scritto il *framework* con in mente le piccole e medie imprese, ma il loro problema è raggiungerle, perché sono fatte in genere da poche persone, focalizzate 24 ore su 24 sul loro

business, ed è difficile distoglierle. Questi messaggi dovrebbero arrivare e dovrebbero fargli dire che forse si sono persi qualche puntata. Devono cercare di approfondire queste cose. Questa potrebbe essere una buona iniziativa.

Tutto ciò che si può fare a livello di disseminazione di consapevolezza, tutto ciò che un servizio pubblico, come la RAI, potrebbe fare in questa direzione potrebbe essere assolutamente ben recepito. Peraltro, mi dicono che trasmissioni come quella andata in onda l'altra sera, uno speciale TG1 andato in onda domenica sera tardissimo fanno degli ascolti notevoli, quindi c'è l'interesse. Dobbiamo cercare di spingerlo un po' oltre, e spiegare alle persone che il futuro è complesso. È bene che si inizino ad attrezzare per questa complessità.

In « Sapienza » ho parlato del *weekly address* alla Nazione del Presidente degli Stati Uniti: in tale occasione Obama ha detto che per creare posti di lavoro e navigare in quest'economia che cambierà questa velocità così forte, la prima risposta per le giovani generazioni è l'educazione. Hanno messo su un piano di 4 bilioni di dollari in cinque anni per portare l'informatica, non solo la parte *cyber*, all'interno delle scuole e delle *high school*, fino a livello universitario, dove chi è interessato può proseguire approfondendo. Questi sono punti secondo me rilevanti. Guardatevelo: 4 bilioni di dollari, detto in modo molto chiaro, come lui sa fare. Spiegava anche le problematiche di *cyber security* alle aziende. Questa è la risposta se vogliamo sopravvivere in questo mondo.

MASSIMO ARTINI. Questa materia mi appassiona molto. Spero che il Parlamento possa dare un contributo con questa indagine conoscitiva, che sta destando l'interesse di tutti, attraverso successivi eventuali provvedimenti.

Detto questo, lei ha fatto un appunto, riprendendo le mie parole, sulla competenza. Penso sempre all'ambito dello Stato, sia della competenza di chi lavora a livello operativo, sia per la competenza del decisore. Ritengo che, ad esempio, nel decreto Monti il fatto che il consigliere militare sia a capo del Nucleo di sicurezza cibernetico possa essere un rischio. Non è detto che sia competente, senza nulla voler togliere a chi ricopre quel ruolo, che però è nato per un altro motivo, ha una funzione di consulenza nei confronti del Presidente del Consiglio. Già un primo passo nell'accelerazione potrebbe essere, anche senza grandi provvedimenti, definire questo tipo di figura, una sorta di direttore del Nucleo, che già sarebbe una persona con titolarità e forse competenza.

Dall'altro lato, mi interessa comprendere nella pubblica amministrazione in quale modo faccio *recruiting*? Formo il personale che fa quel tipo di operazione e, contemporaneamente, formo in maniera univoca tutti gli operatori più coinvolti nella parte di cibernetica. Per questo le chiedo: istituire una sorta di scuola che faccia da capofila, che magari prenda delle esperienze – prima si riferiva a Chiavari, dove c'è la scuola della difesa – come anche quella universitaria, o in osmosi tra università e mondo...

ROBERTO BALDONI, *Direttore del Centro di Ricerca Sapienza in Cyber Intelligence e Information Security (CIS)*. Come Laboratorio nazionale già lavoriamo su questo.

MASSIMO ARTINI. Ne sono perfettamente consapevole. Il punto è che non posso lasciare in mano alla buona capacità amministrativa di chi è dedicato per mansione a quel tipo di lavoro che tutto funzioni regolarmente. Se ci fosse un percorso normativo che lo definisse, spero che sia d'accordo con me che sarebbe la cosa più opportuna, anche per un discorso di fondi.

Una formazione univoca per chi opera permette di avere un'interscambiabilità anche tra gli operatori. È una considerazione che mi interessa fare, perché la parte di formazione, consapevolezza e competenza in questo mondo è qualcosa che non può essere altro che di sistema. Un piccolo operatore rimane piccolo e verrà tagliato fuori perché il sistema è

corrotto da un punto di vista informatico, non mi fraintenda. Io posso avere il migliore sistema informatico e la mia linea, presa a 2 euro, non funziona, altro spunto su cui non si torna mai.

La pubblicità di una rete che sia solo pubblica, almeno una parte, non dico tutta, avere la proprietà statale di un'infrastruttura, a parte quelle dell'università, ma che sia anche utilizzabile dal privato, potrebbe essere un altro incremento di sovranità ?

ROBERTO BALDONI, *Direttore del Centro di Ricerca Sapienza in Cyber Intelligence e Information Security (CIS).* Da quello che mi risulta, siamo in questo momento credo uno dei pochissimi Paesi a non essere proprietario della propria infrastruttura di rete. Se lei e io dovessimo scambiarci dei messaggi, su che mezzo lo faremmo ? Questo è un problema serio, come quello dell'approvvigionamento *hardware*.

Ecco perché c'è bisogno di un luogo in cui si discutano queste problematiche per trovare soluzioni. Non può che essere un luogo dove le competenze ci sono. Qui entro, però, nel problema del pubblico. Si può immaginare questo luogo all'interno dell'architettura nazionale governativa di *cyber security*, certamente per una serie di ragioni. Per altre, vi invito anche a riflettere su qualcosa che può stare in un alveo un po' privato. C'è sempre il tema della velocità che si riuscirà a raggiungere con questa architettura, e quello dei rischi.

Chi saranno le persone di riferimento di questa iniziativa ? Si realizza una bellissima struttura anche con le migliori intenzioni, dopodiché che cosa succede ? Secondo me, va trovato il giusto equilibrio pensando anche al privato. Penso alle nostre grandi aziende, alle *big four*: loro hanno problemi serissimi. Allora forse avere qualcosa dove discutere di queste cose tra le grandi aziende nazionali e difesa, *intelligence*, *law enforcement*, quelle che sono per necessità in prima linea su questo settore, forse potrebbe essere un'idea da non scartare. Dico di pensare anche all'altra parte, a quella dello spettro privato.

Concordo praticamente con quasi tutto quello che ha detto l'onorevole Artini.

PRESIDENTE. La *cyber*-sussidiarietà.

ROBERTO BALDONI, *Direttore del Centro di Ricerca Sapienza in Cyber Intelligence e Information Security (CIS).* È normale, perché dobbiamo avere proprio dei luoghi in cui, soprattutto con alcune aziende, iniziare a condividere informazioni. Dirò di più: dobbiamo cercare di riportare in Italia – ho letto molto bene la notizia su Cisco – dei centri di ricerca. Quando io uscii dall'università, nel 1990, Roma era piena di centri di ricerca di grandi aziende. Avevamo Telecom, 500 persone occupate nella ricerca; avevamo IBM; avevamo Italtel. Tutto ciò negli anni Novanta e nei primi anni Duemila è stato completamente raso al suolo.

Abbiamo visto una serie di scenari, pensiamo ai *big data*, alle *smart cities*: chi li realizza ? Puoi andare da *Google*, da IBM, ma loro che cosa ti vendono per le *smart cities* o i *big data* ? Le infrastrutture, dopodiché sopra l'infrastruttura hai bisogno di una serie di algoritmi, di strumenti specifici per quella città per esempio. La *smart city* di Roma non è *smart city* Milano. C'è una prateria per costruire nuove aziende, che poi potrebbero usare questo come mercato.

Il problema è, se non abbiamo le competenze di alto profilo, come fare queste aziende. Queste competenze si trovano soltanto o partono da centri di ricerca, da gruppi dove ci sono 100-200 persone che discutono e creano innovazione. Noi abbiamo raso al suolo tutto quello che c'era quindici anni fa, e quindi va ricostituito questo tessuto.

PRESIDENTE. Ringrazio molto il professor Baldoni per la completezza della sua relazione, per la competenza che ha proposto anche con le sue osservazioni e con le sue risposte, e per la sua disponibilità. Lo ringrazio, altresì, per la docu-

mentazione informatica che ci ha lasciato – di cui autorizzo la pubblicazione in allegato al resoconto stenografico dell'audizione odierna *(vedi allegato)* – e lo consideriamo ancora a disposizione della Commissione, perché il nostro viaggio è appena cominciato. Oggi abbiamo cominciato questa indagine conoscitiva. Se sarà utile, se servirà, ci riserviamo di poterla avere ancora con noi quando saremo un po' più avanti e anche più consapevoli. Il termine centrale della nostra riflessione di oggi è consapevolezza, e vale anche per chi, come noi, come decisori politici siamo chiamati a esercitare su questo terreno così nuovo e così inedito alla nostra responsabilità.

Dichiaro conclusa l'audizione.

La seduta termina alle 13.15.

IL CONSIGLIERE CAPO DEL SERVIZIO RESOCONTI ESTENSORE DEL PROCESSO VERBALE

DOTT. RENZO DICKMANN

Licenziato per la stampa il 29 aprile 2016.

STABILIMENTI TIPOGRAFICI CARLO COLOMBO

Audizione Commissione Difesa

9/2/2016

Prof. Roberto Baldoni

Cyber Security National Lab Director

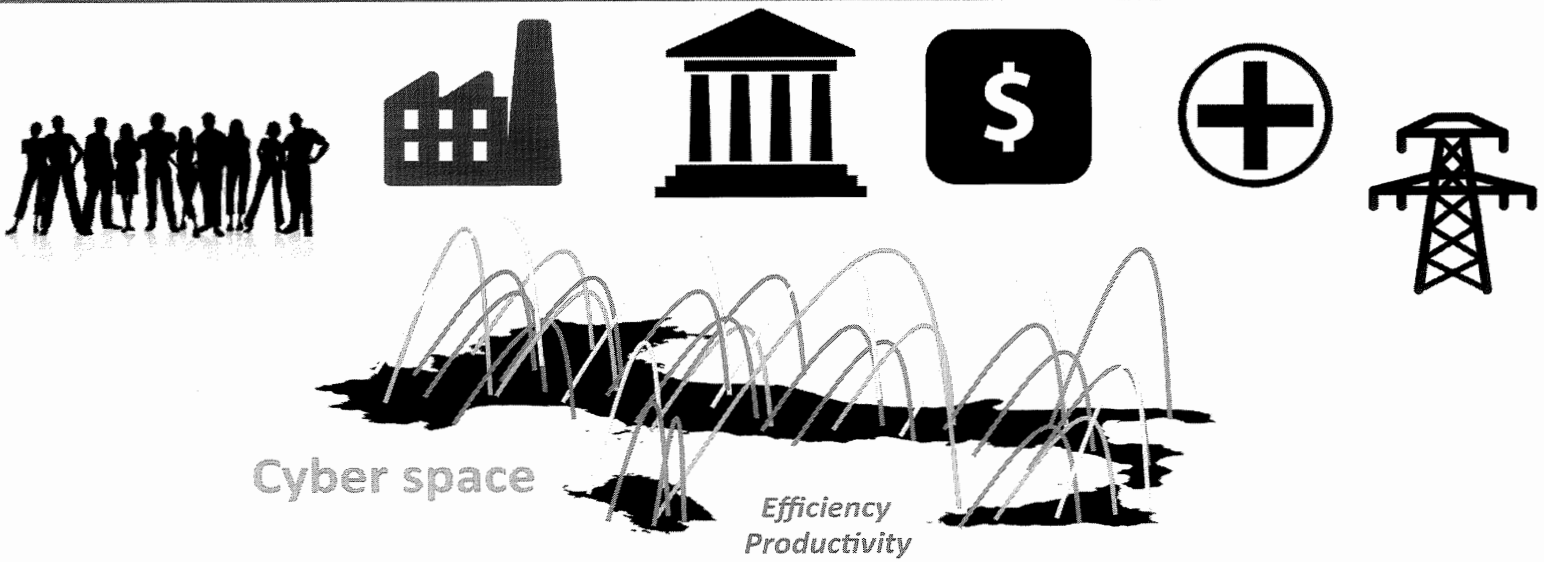
Università degli Studi di Roma «La Sapienza»

baldoni@dis.uniroma1.it

http://www.consorzio-cini.it/lab-cyber-security

cini Cyber Security National Lab

Settori economici sensibili alle minacce cyber



Nel prossimo futuro la prosperità economica e l'indipendenza di un paese sarà misurata in base al grado di sicurezza che sarà in grado di assicurare all proprio cyberspace

cini Cyber Security National Lab

Cyber Security: Definizione

La cyber security è quella pratica che consente a una entità (ad esempio, organizzazione, cittadino, nazione ecc.) la protezione dei propri asset fisici e la confindezialità, integrità e disponibilità delle proprie informazioni dalle minacce che arrivano dal cyber space.
A sua volta, *il cyber space viene definito come il complesso ecosistema risultante dall'interazione di persone, software e servizi su Internet per mezzo di tecnologie, dispositivi e reti ad esso connesse*

cini Cyber Security National Lab

Unicità del Cyberspace

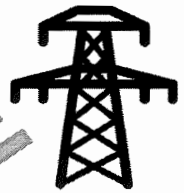
- Non esiste divisione tra pubblico e privato, tra militare e civile. Un ambiente dove tutto è duale!
- Vulnerabilità non numerabili, attacchi in costante aumento per precisione e potenza
- Nessuno può pensare di gestire questa complessità in isolamento

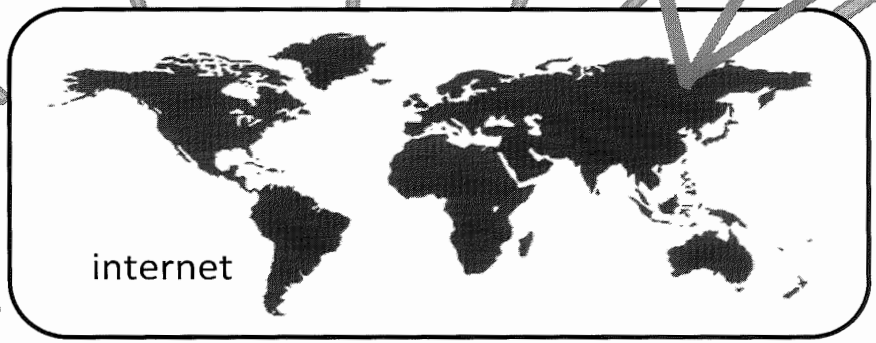
cini Cyber Security National Lab

Economia
Cyberspace
IoT
Big Data
Robotics
Industry 4.0
Smart Cities
Drones
Digital Currency
Agricolture 4.0

Cyber Attacks

Business continuity





Peaks of thousands attacks per hour

Attacks on evenings and weekends

Asymmetry

increasingly powerful, simple and inexpensive tools

difficulty to attribute

In cyber space is always emergency!

cini Cyber Security National Lab

Come avviene un attacco

- Attraverso il cyberspace sfruttando vulnerabilità tecniche sul perimetro (concetto molto debole nell'internet attuale – vedi supply chain)
- Attraverso il cyberspace usando le vulnerabilità (consapevoli o inconsapevoli) legate al fattore umano
- entrambe

1. Actor
   - 1.1 Commercial Competitor
   - 1.2 Hacker
     - 1.2.1 Script Kiddie Hacker
     - 1.2.2 Skilled Hacker
   - 1.3 Insider
     - 1.3.1 Admin Insider
     - 1.3.2 Normal Insider
   - 1.4 Organised Criminal Group
   - 1.5 Protest Group

2. Actor Location
   - 2.1 Foreign Actor Location
   - 2.2 Local Actor Location

   Indeterminate Actor Location

3. Aggressor
   - 3.1 Individual Aggressor
   - 3.2 Commercial Aggressor
   - 3.3 State Aggressor
   - 3.4 Group Aggressor
     - 3.4.1 Ad-hoc Group Aggressor
     - 3.4.2 Organized Group Aggressor

4. Attack Goal
   - 4.1 Change Data
   - 4.2 Destroy Data
   - 4.3 Disrupt Data
   - 4.4 Steal Data

   Springboard for other attack goal

5. Attack Mechanism
   - 5.1 Access
     - 5.1.1 Brute Force
     - 5.1.2 Buffer Overflow
     - 5.1.3 Spear Phishing
     - 5.1.4 Physical
   - 5.2 Data Manipulate
     - 5.2.1 Network-based
       - 5.2.1.1 Denial of Service
     - 5.2.2 Virus-based
       - 5.2.2.1 Trojan
       - 5.2.2.2 Virus
       - 5.2.2.3 Worm
     - 5.2.3 Web-Application-based
       - 5.2.3.1 SQL Injection
       - 5.2.3.2 Cross-site scripting
   - 5.3 Information Gathering
     - 5.3.1 Scanning
     - 5.3.2 Physical

6. Vulnerability
   - 6.1 Configuration
     - 6.1.1 Access Rights
     - 6.1.2 Default Setup
   - 6.2 Design
     - 6.2.1 Open Access
     - 6.2.2 Protocol Error
   - 6.3 Implementation
     - 6.3.1 Buffer Overflow
     - 6.3.2 Race Condition
     - 6.3.3 SQL Injection
     - 6.3.4 Variable Type Checking

7. Effects
   - 7.1 Null
   - 7.2 Minor Damage
   - 7.3 Major Damage
   - 7.4 Catastrophic

8. Motivation
   - 8.1 Financial
   - 8.2 Fun
   - 8.3 Ethical
   - 8.4 Criminal

9. Phase
   - 9.1 Target Identification
   - 9.2 Reconnaissance
   - 9.3 Attack Phase
     - 9.3.1 Ramp-up
     - 9.3.2 Damage
     - 9.3.3 Residue
   - 9.4 Post- Attack Reconnaissance

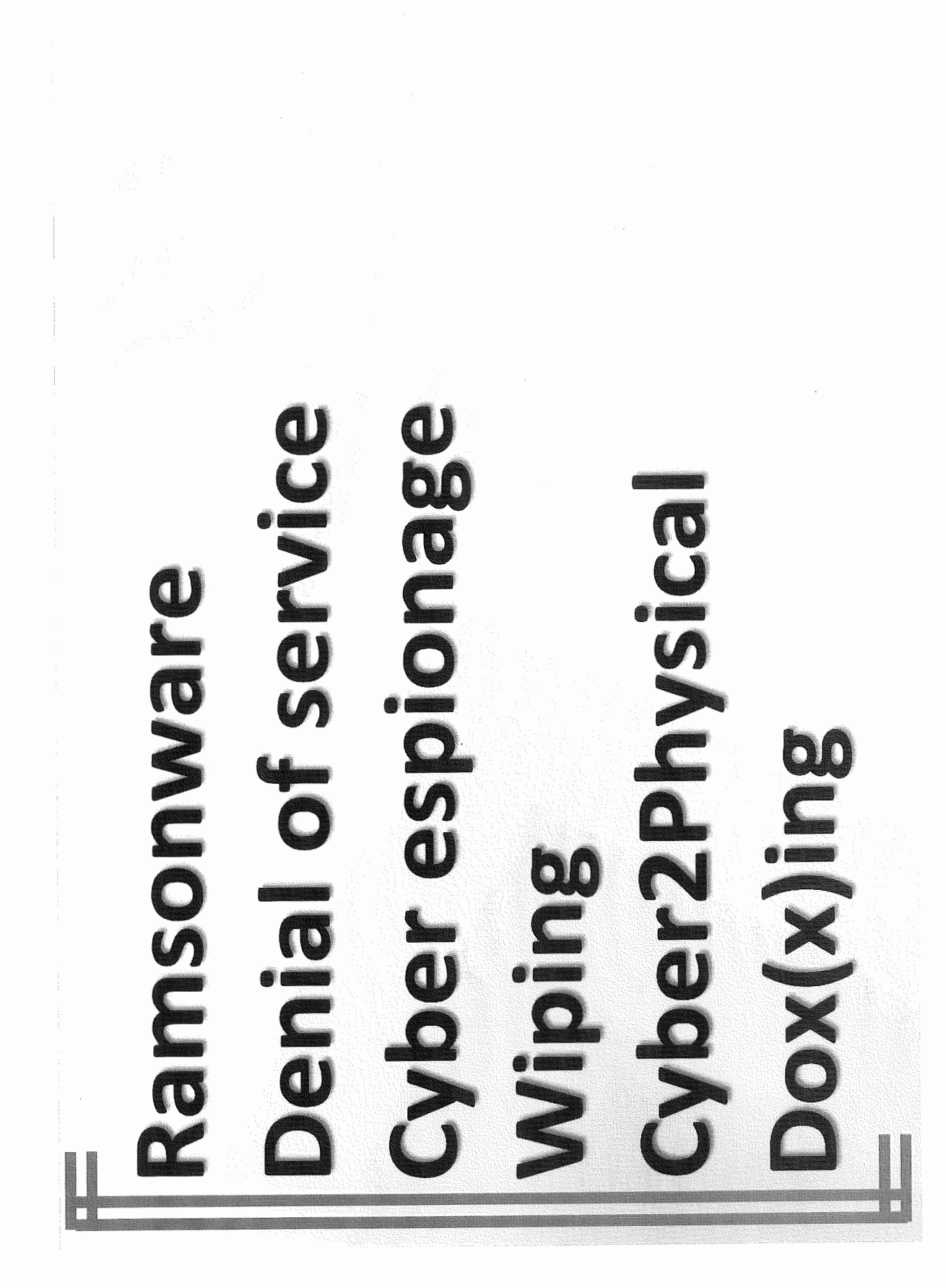
10. Scope
    - 10.1Corporate Network
      - 10.1.1 Large Corporate Network
      - 10.1.2 Small Corporate Network
    - 10.2Government Network
      - 10.2.1 Large Government Network
      - 10.2.2 Small Government Network
    - 10.3Private Network

11. Target
    - 11.1Personal Computer
    - 11.2Network Infrastructure Device
    - 11.3Server

12. Automation Level
    - 12.1Manual
    - 12.2Automatic

      Semi-Automatic

[27] R. P. van Heerden, B. Irwin, I. D. Burke: *Classifying network attack scenarios using an Ontology*, In: Proceedings of the 7th International Conference on Information Warfare and Security. Academic Conferences Limited, pages 331-324, 2012


Ramsonware
Denial of service
Cyber espionage
Wiping
Cyber2Physical
Dox(x)ing

Other Trendy attacks in 2015
Ramsonware
Denial of service
Cyber espionage
Wiping
Cyber2Physical
Dox(x)ing
ThyssenKrupp

Other Tre

Ramsonw

Denial of

Cyber esp

W

C

D

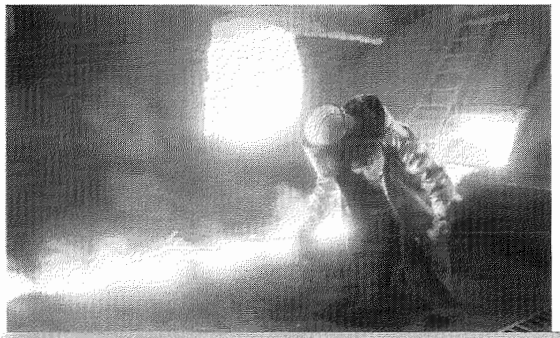
MILITARY

FOR THE SECOND TIME EVER, A CYBERATTACK CAUSES PHYSICAL DAMAGE

IT'S THE DAWN OF A NEW KIND OF WAR

By Kelsey D. Atherton Posted 12 hours ago

35 Shares

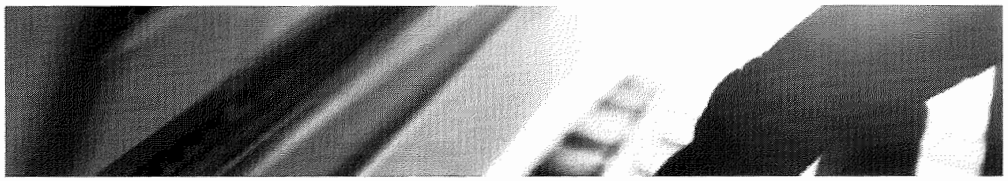


ThyssenKrupp

Cyberattack that crippled Ukrainian power grid was highly coordinated

1st power outage caused by cyberattack suggests similar attacks possible around the globe

Thomson Reuters Posted: Jan 11, 2016 11:52 AM ET | Last Updated: Jan 11, 2016 12:17 PM ET



Cyber Espionage in the past
cini
Cyber Security National Lab
12

Cyber espionage: Today

Australian company devastated by Chinese hacking, IP theft

By Reuters Staff on Jun 25, 2015 11:13 AM
Filed under Security

Page 1 of 2 | Single page

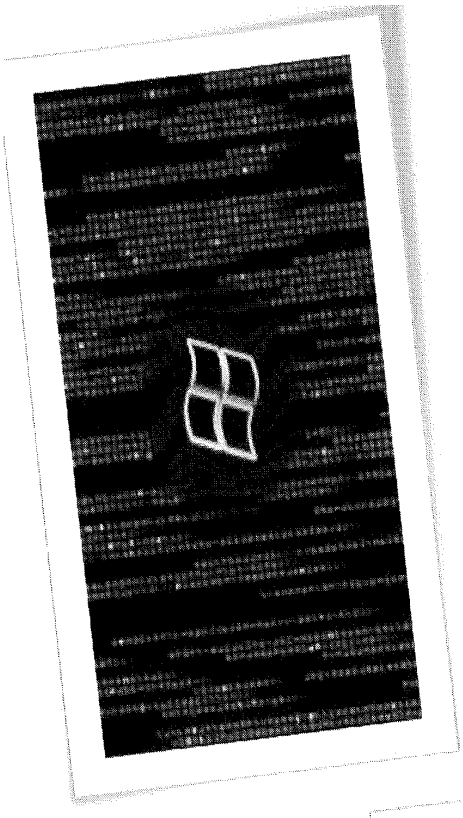
Federal govt said 'You're on your own', claims business owner.

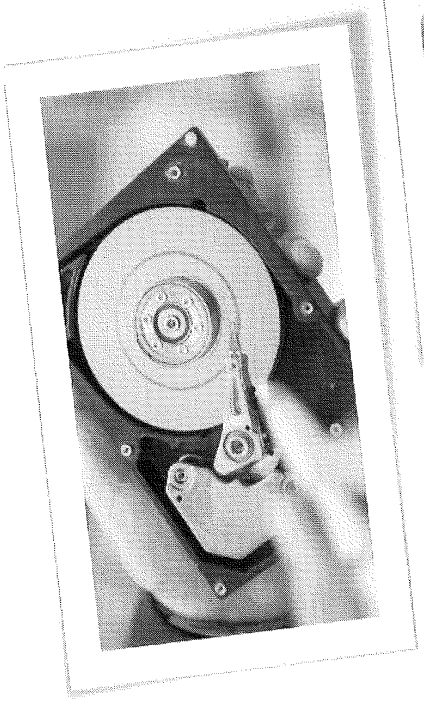
Hackers steal $160 billion worth of intellectual property from western

cini Cyber Security National Lab

2015 Top Attack: The hacking team data breach (thehachernews.com)

- Milan (Italy) based IT firm and surveillance software solutions to Governments and Law Enforcement agencies worldwide.
- exposed over 400 gigabytes of its internal sensitive data on the Internet.
- Hackers leaked:
  - Executive Emails
  - Source codes for Hacking and Spyware Tools
  - Zero-day exploits, including for Flash, Internet Explorer
  - Government client list with date of purchase and amount paid

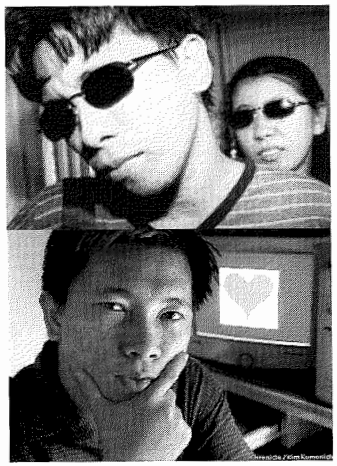




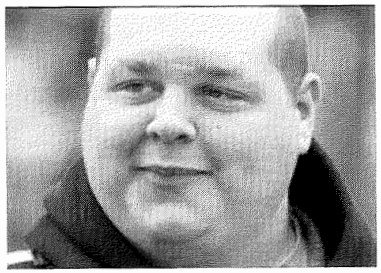
THE ADVERSARY

Who is behind the cyber threat

Till 2004



I LOVE YOU



BLASTER

Virus

today

CONFIKER

DUQU

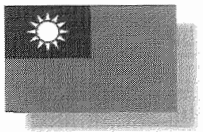
STUXNET

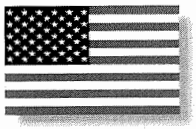
Flame

ZEUS

GAUSS

MIRAGE





APT, Malware

cini Cyber Security National Lab

Adversary

- Expertise
- Risorse Disponibili
- Attack vectors
- Behaviour

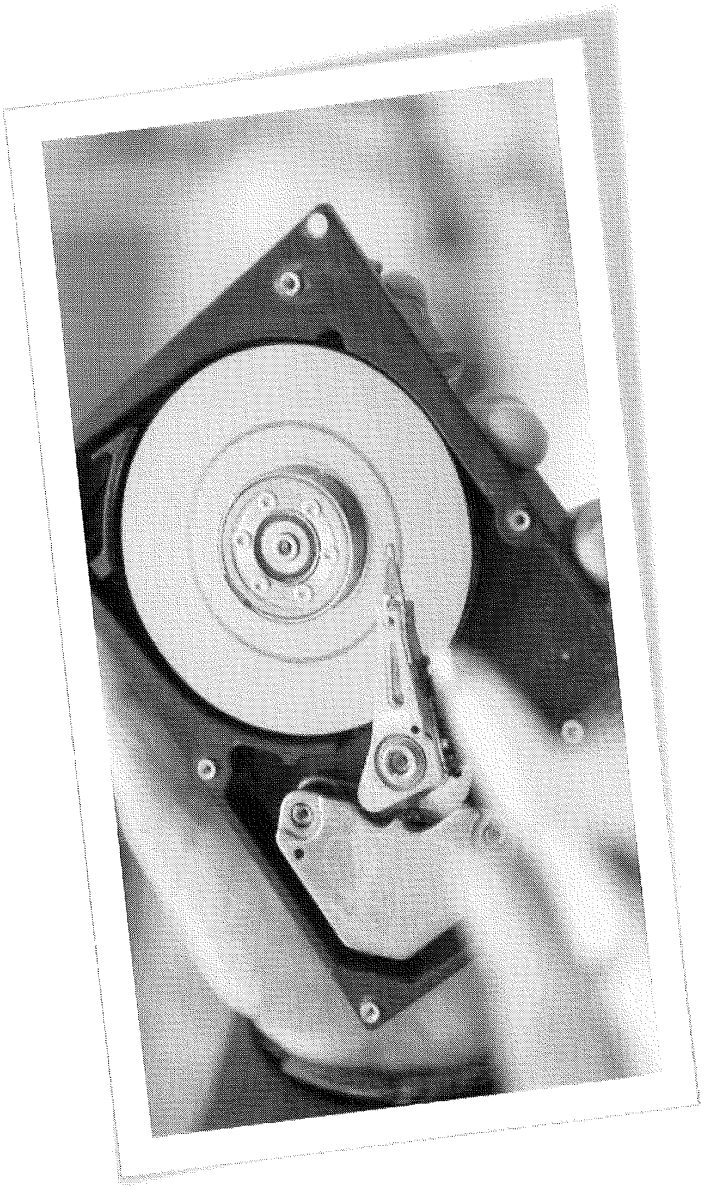
cini Cyber Security National Lab

Advanced Persistent Threats

- sophisticated levels of expertise
- significant resources
- Objectives (footholds within the information technology infrastructure of the targeted organizations)
  - exfiltrating information
  - undermining or impeding critical aspects of a mission, program, or organization
  - positioning itself to carry out these objectives in the future

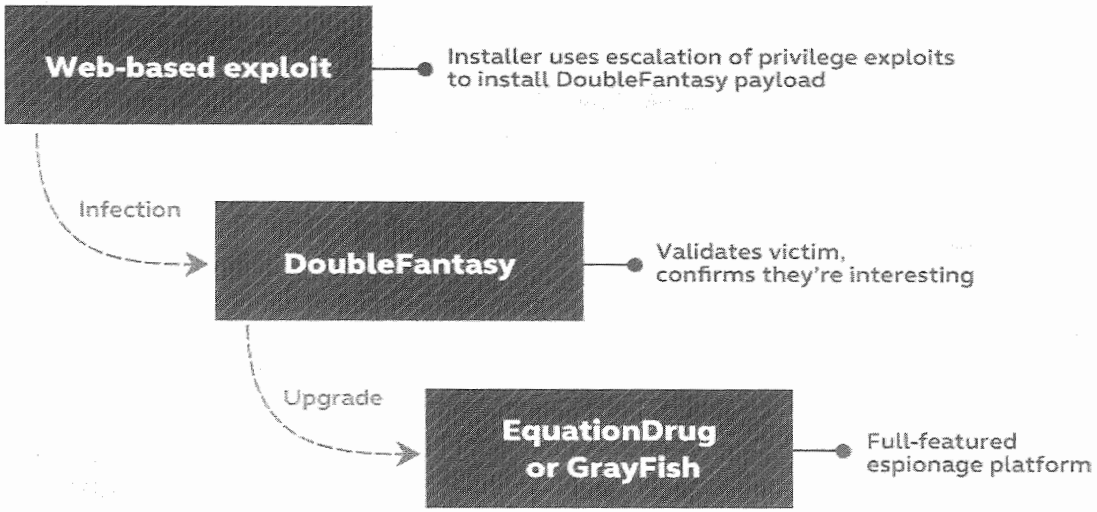
- multiple attack vectors
- behavior
  1. pursue its objectives repeatedly over an extended period of time;
  2. adapt to defenders' efforts to resist it
  3. determined to maintain the level of interaction needed to execute its objectives.

cini Cyber Security National Lab



THE EQUATION GROUP

Infection lifecycle of EquationDrug



GREAT KASPERSKY lab

cini Cyber Security National Lab

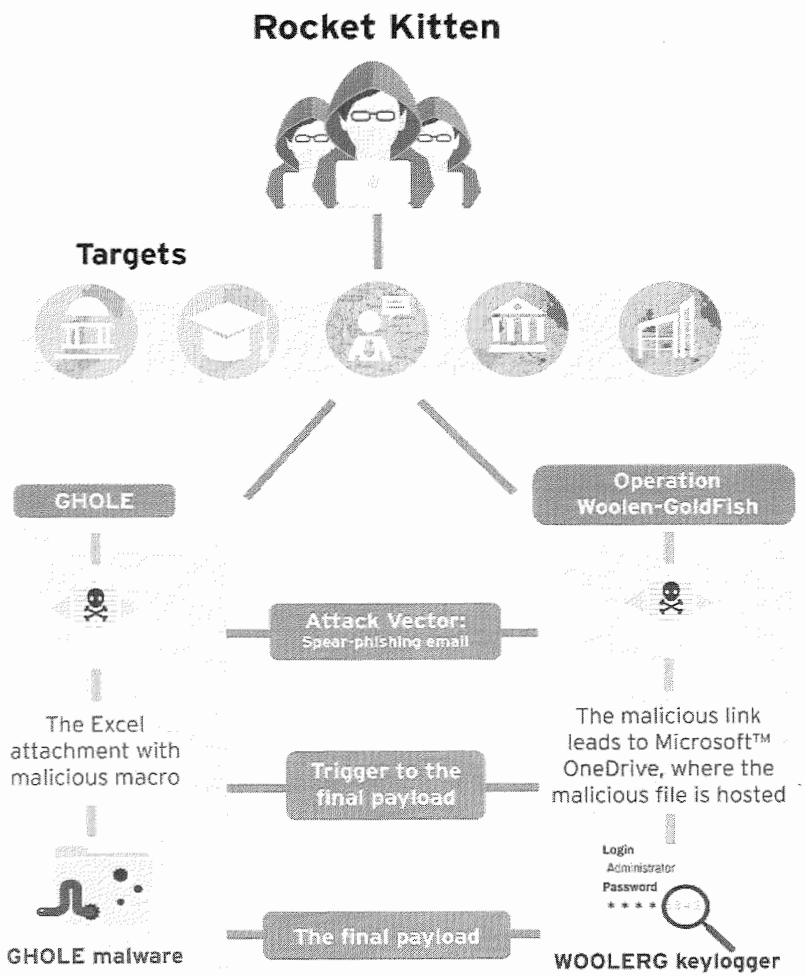
Implant the malware

- The equation group
  - Self-replicating (worm) code – Fanny
  - Physical media, CD-ROMs
  - USB sticks + exploits
  - Web-based exploits

Infecting the hard drive firmware

- Reprogramming and Flashing HDD firmware
- Modules in EQUATIONDRUG and GRAYFISH platforms (from 2010 to 2013)
- 12 Drives categories: “WDC WD”, “ST”, “Maxtor STM”, “SEAGATE ST”, “SAMSUNG”, “WDC WD”, “IC”, “IBM”, “Hitachi”, “HTS”, “HTE”, “HDS”, “HDT”, “ExcelStor” etc.
- reprogrammed by a series of ATA commands. The plugin uses a lot of undocumented, vendor-specific ATA commands
- Identified only a few victims. This indicates that it is probably only kept for the most valuable victims

ROCKET KITTEN



Victims

- Civilian organizations in Israel
- Academic organizations in Israel
- German-speaking government organizations
- European organizations
- European private company

cini Cyber Security National Lab

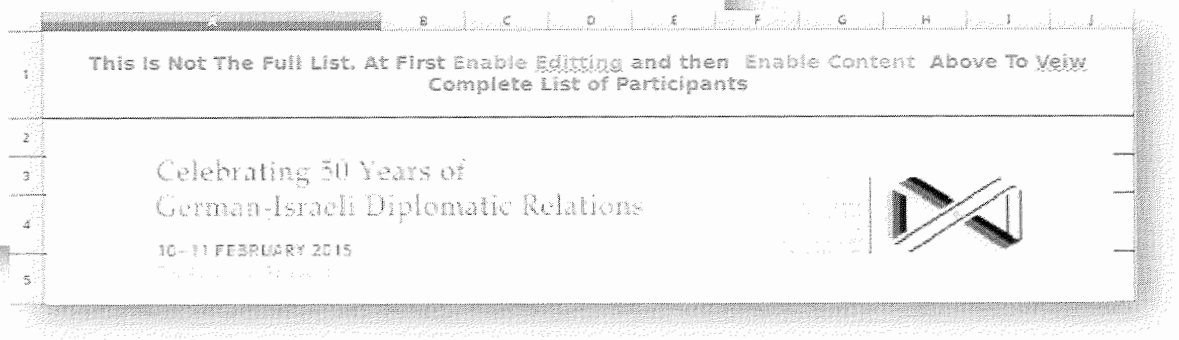
Rocket Kitten spear-phishing emails

From: [redacted]
Date: Apr 23, 2014 10:08 AM
Subject: Message
To: [redacted]

Dear all,
Enclosed is some information that I hope you will find it useful.
Hag Sameah.

[redacted]
CEO, [redacted]

[redacted]



cini Cyber Security National Lab

From: FirstName [mailto: firstnamelastname1@gmail.com]
Subject: Possible Scenarios for Hezbollah's Retaliation? your comments are most welcome.

Dear experts,

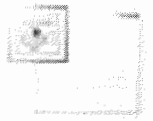
As you know Israeli helicopter had conducted a strike against "terrorists" near Quneitra, on the Syrian side of the Golan Heights
that killed several of Hezbollah's members including one Iranian commander.
I wrote an article about possible scenarios about Hezbollah's reactions and
would like to know your ideas about it?

I answered some questions about possible reactions:

- Is it in the common interest between Hezbollah and Iran to retaliate?
- What can be the worst-case scenario?
- Time and place to hit back?
- Will the retaliation be restrained enough to provoke a war?
- ...

You can download and see the article in my Drive:
https://onedrive.live.com/redir?resid=xxxxxxxxxxxxxxx
Best regards,
FirstName

--
(here followed an official signature)



Iran's Missiles
Program.ppt.exe

cini
Cyber Security National Lab

GOVERNMENTS AND CYBER THREATS

BRIEFING ROOM
ISSUES
THE ADMINISTRATION
PARTICIPATE
Executive Order -- Improving Critical Infrastructure Cybersecurity
Framework for Improving Critical Infrastructure Cybersecurity
Version 1.0
National Institute of Standards and Technology
February 12, 2014
The White House
FACT SHEET: Executive Order Promoting Private Sector Cybersecurity Information Sharing
February 12, 2015
12/2/2013
12/2/2014
15/2/2015
cini
Cyber Security National Lab
28

Complex Implementation

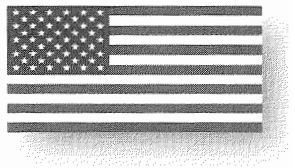
Forbes.com

"Problematic voluntary adoption plan"

14 Feb 2013

"Google, Apple and Microsoft may be exempt from Obama's cybersecurity order"

"Obama's Cybersecurity Order Exempts Software" 5 March 2013



cini Cyber Security National Lab

Complex Implementation

The Federal Government's Track Record
on Cybersecurity and Critical Infrastructure

A report prepared by

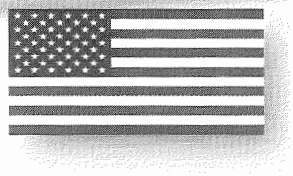
the Minority Staff of the Homeland Security and Governmental Affairs Committee

Sen. Tom Coburn, MD, Ranking Member

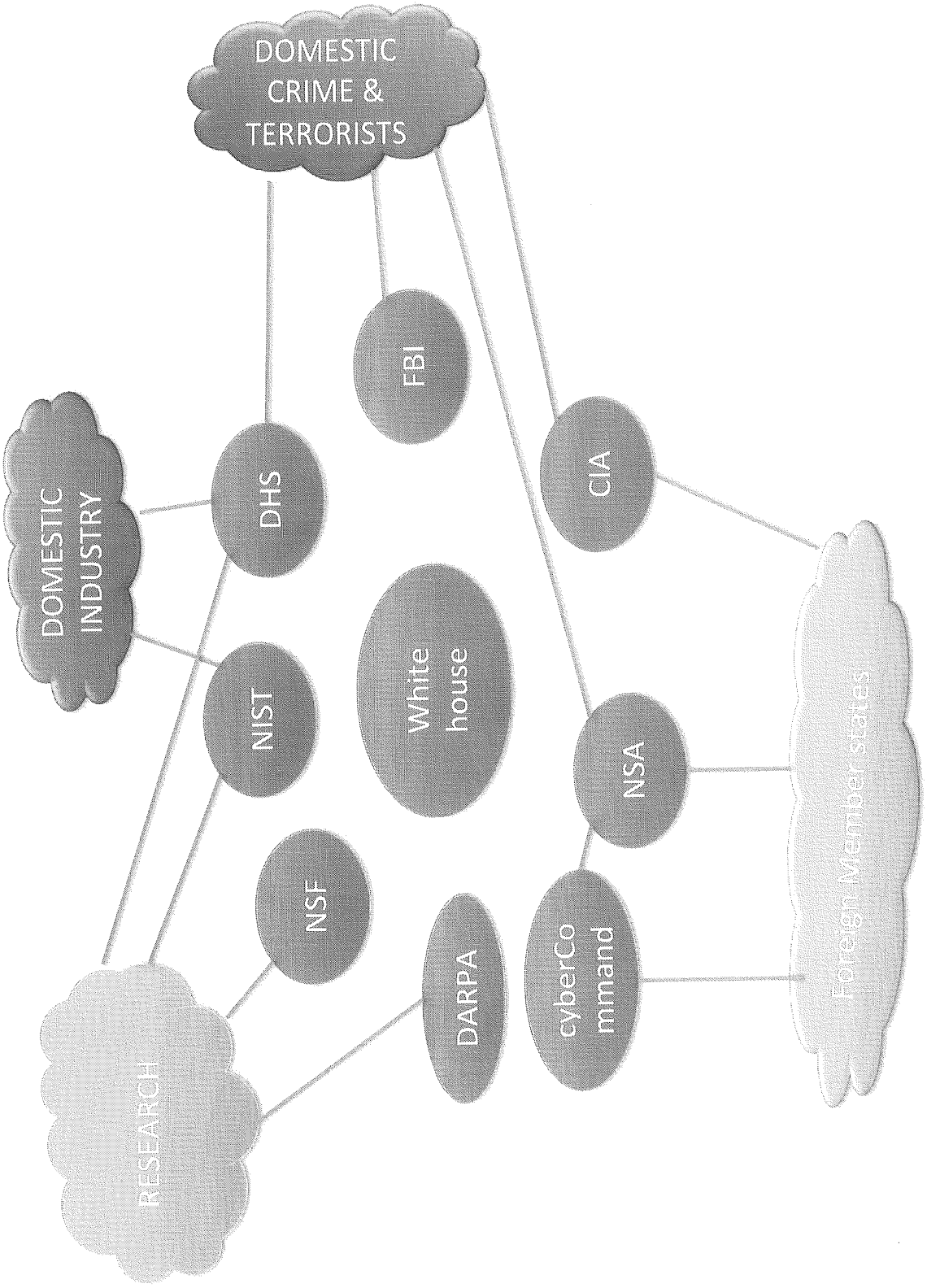
February 4, 2014

The report draws on previous work by agency inspectors general and the Government Accountability Office to paint a broader picture of chronic dysfunction, citing repeated failures by federal officials to perform the unglamorous work of information security. That includes installing security patches, updating anti-virus software, communicating on secure networks and requiring strong passwords. A common password on federal systems, the report found, is "password."

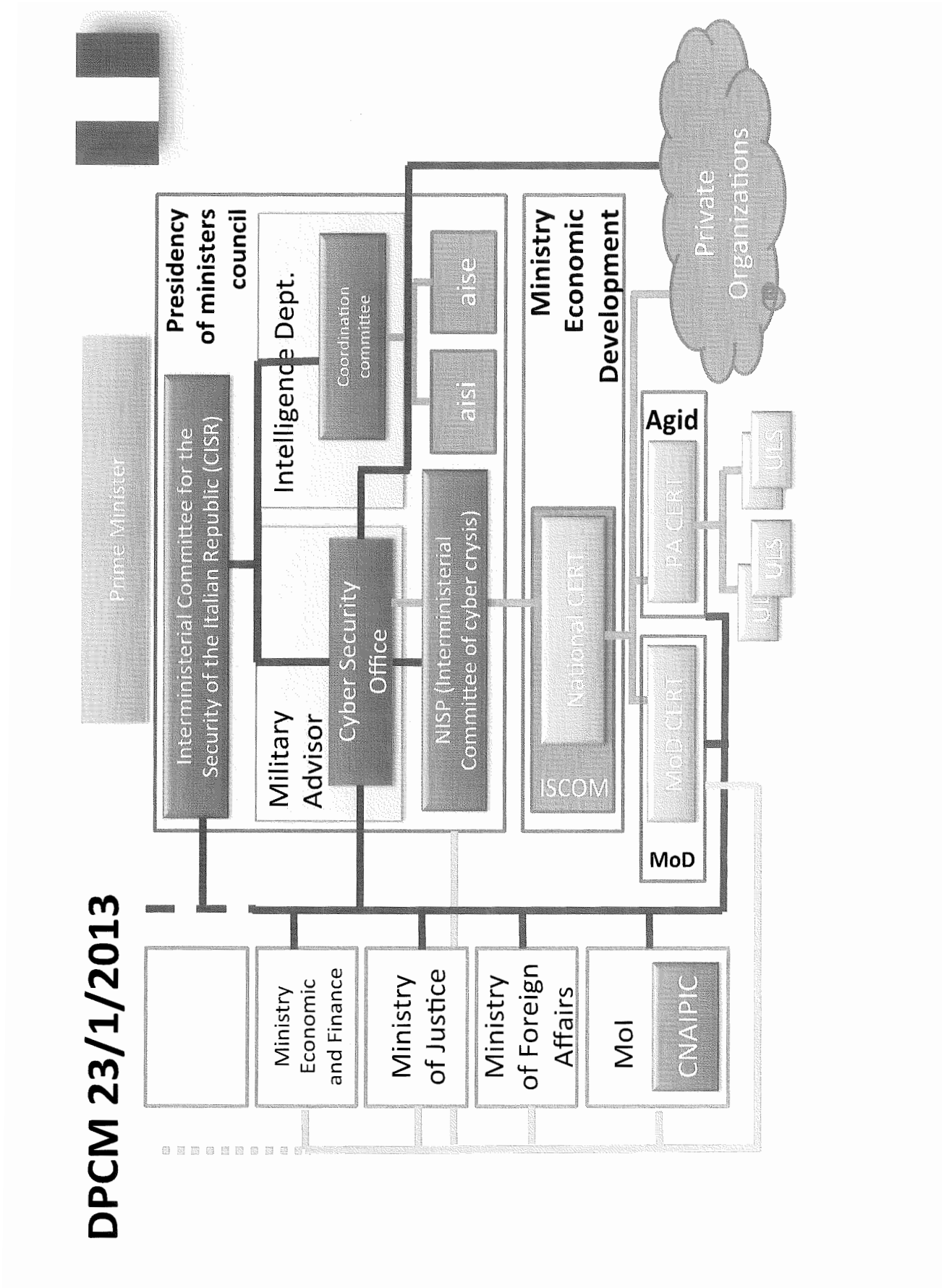
In March 2013, GAO [Government Accountability Office] reported that IRS allowed its employees to use passwords that "could be easily guessed." Examples of easily-guessed passwords are a person's username or real name, the word "password," the agency's name, or simple keyboard patterns (e.g., "qwerty"), according to the National Institute of Standards and Technology.

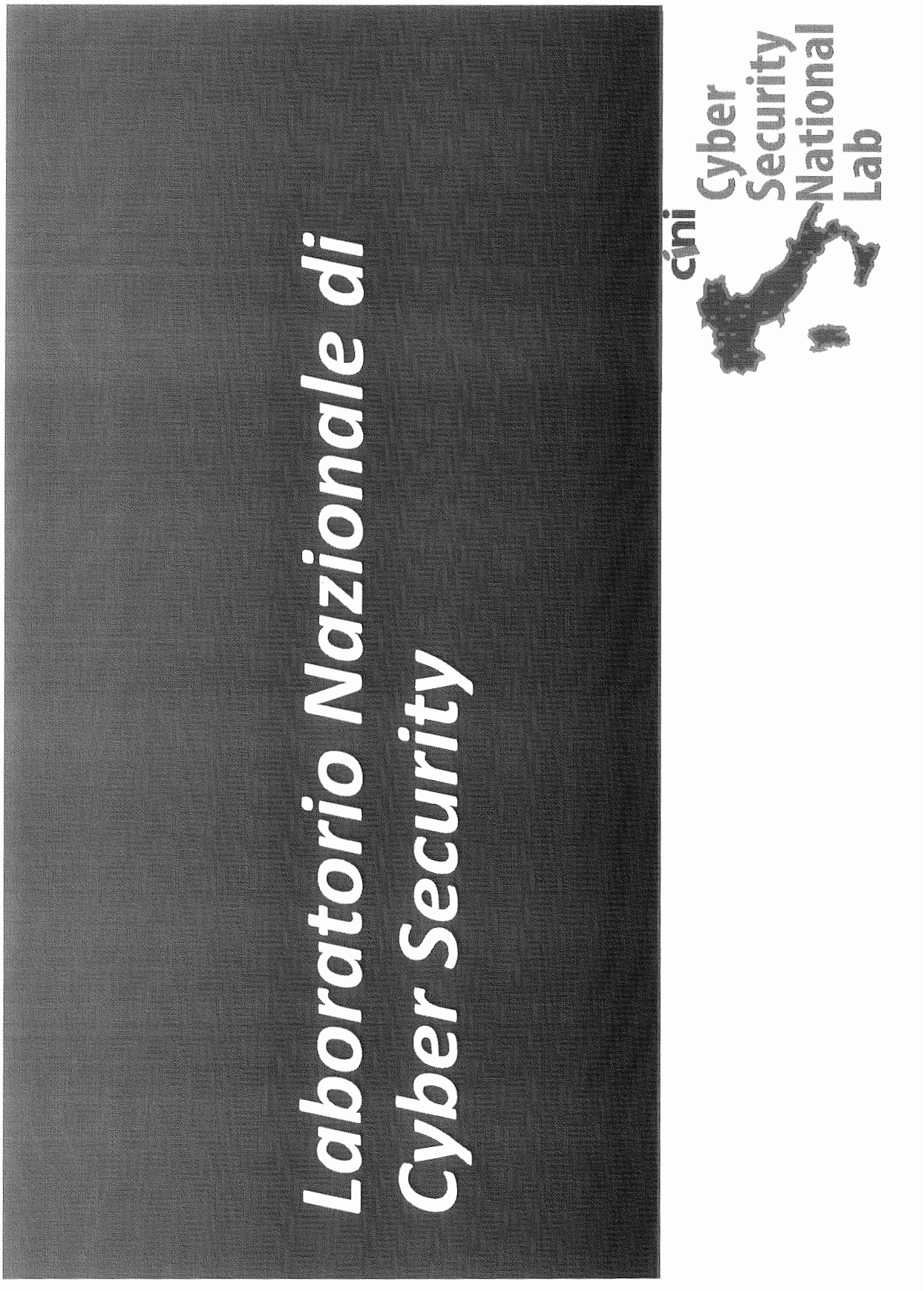


cini
Cyber Security National Lab


DOMESTIC CRIME & TERRORISTS
FBI
DOMESTIC INDUSTRY
DHS
CIA
NIST
White house
NSA
Foreign Member states
NSF
DARPA
cyberCo mmand
RESEARCH

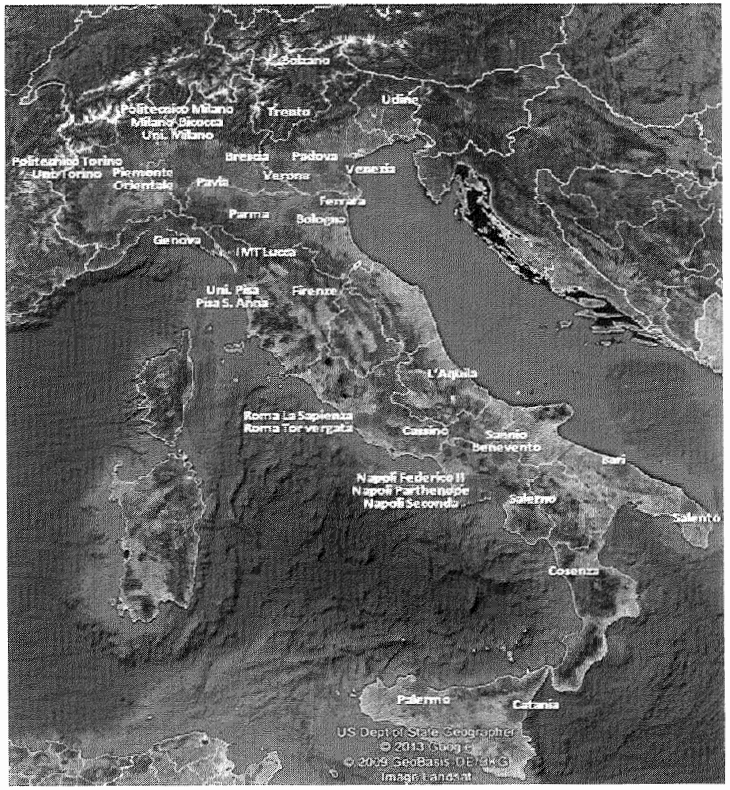
Some milestones
cini
Cyber Security National Lab
Feb 2016
Italian Framework for cyber security
13/11/2014
13/05/2014
27/12/2013
24/1/2013
CERT nazionale Italia
Adobe risolve diciotto vulnerabilità di Flash P
QUADRO STRATEGICO NAZIONALE
PER LA SICUREZZA
DELLO SPAZIO CIBERNETICO
DECRETO DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI 24 gennaio 2013


DPCM 23/1/2013
Prime Minister
Presidency of ministers council
Interministerial Committee for the Security of the Italian Republic (CISR)
Intelligence Dept.
Coordination committee
aise
aisi
Military Advisor
Cyber Security Office
NISP (Interministerial Committee of cyber crysis)
Ministry Economic Development
National CERT
ISCOM
Agid
PA CERT
UTIS
UTIS
UTIS
MoD
MoD CERT
Private Organizations
Ministry Economic and Finance
Ministry of Justice
Ministry of Foreign Affairs
MoI
CNAIPIC


Laboratorio Nazionale di
Cyber Security
cini
Cyber
Security
National
Lab

The CINI Consortium

- CINI (Consorzio Interuniversitario Nazionale per l'Informatica)
- A consortium of 36 Italian public universities that deliver MS degrees in CE and/or CS
- Established in 1990



cini
Cyber Security National Lab

Relazione tra Accademia e Architettura Cyber Nazionale Governativa

Sept 2010 — *Joint working group Sapienza-Presidency of Ministry Councils*

March 2012 — CIS SAPIENZA (Cyber Intelligence and Information Security)

May 2014 — cini Cyber Security National Lab

Sept 2014 — *Agreement between CINI and - Presidency of Ministry Councils*

June 2015 — *Agreement between CINI and – National CERT*

Nov. 2015 — *White Book on Cyber Security*

31/12/2015 — *Cyber range, National cyber security framework, Italian-Israeli Cyber Lab, Polo Tecnologico*

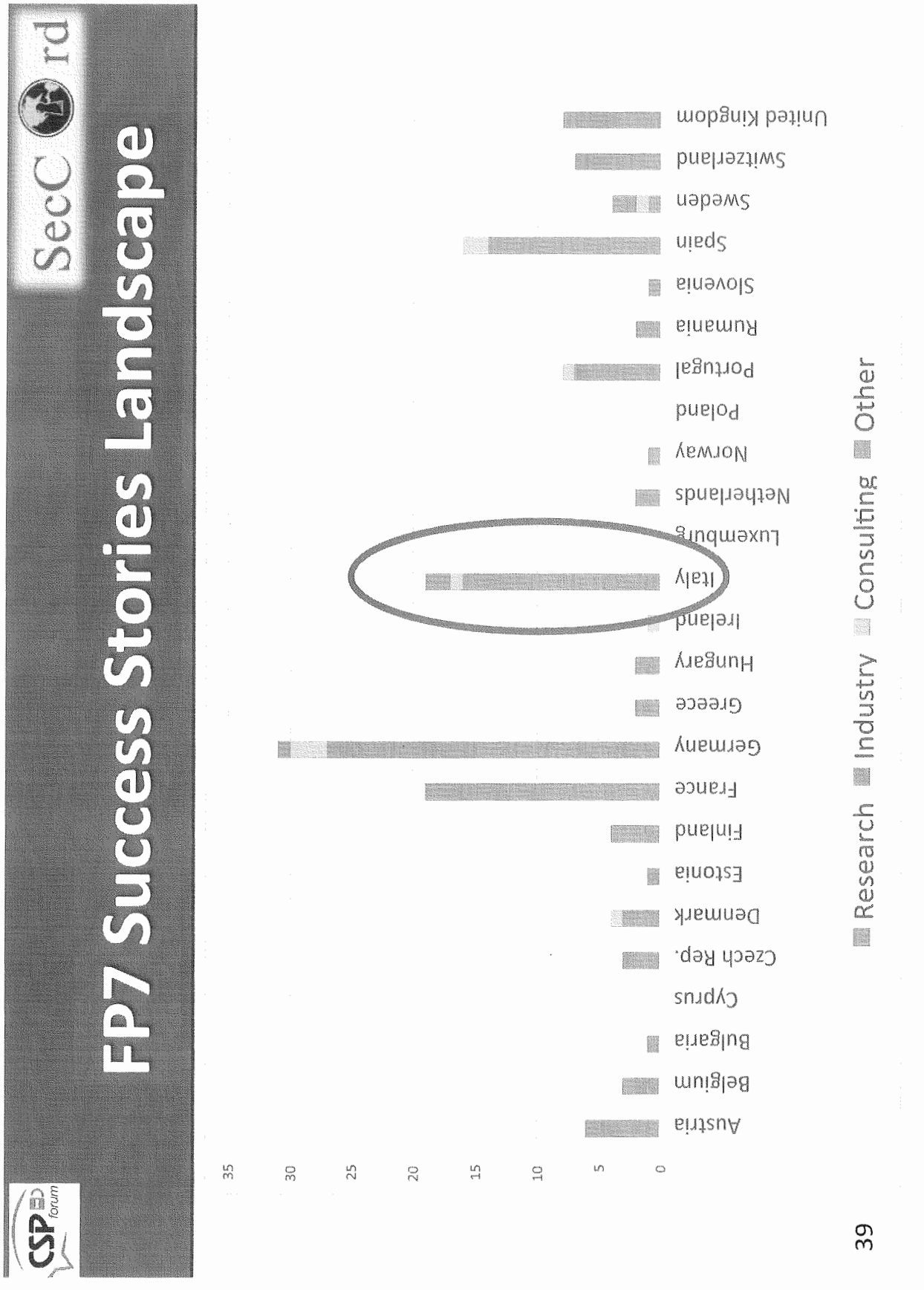
Cyber Security National Lab: *mission*

Critical mass geographical distribution and highest multidisciplinary research quality

- Actor of the process of implementation of the Italian Cyber Security Strategy nationwide
- Implementation of on-the-edge cyber security projects through one or multiple local sites
- Definition of standard and methodologies at the national level
- Implementation of education and awareness nationwide plans
- Large portfolio of relationships worldwide

cini Cyber Security National Lab

Laboratori Locali e Coordinatori
• IMT Lucca Rocco De Nicola
• Politecnico di Milano Stefano Zanero
• Politecnico di Torino Antonio Lioy
• Seconda Univ. di Napoli Bernardino Di Martino
• Univ. di Venezia Riccardo Focardi
• Univ. del Sannio Corrado Visaggio
• Univ. dell'Insubria Elena Ferrari
• Univ. di Bari Donato Malerba
• Univ. di Bologna Gabriele D'Angelo
• Univ. di Cagliari Massimo Bartoletti
• Univ. di Catania Dario Catalano
• Univ. di Firenze Andrea Bondavalli
• Univ. di Genova Alessandro Armando
• Univ. di Milano Pierangela Samarati
• Univ. di Milano-Bicocca Claudio Ferretti
• Univ. di Modena e Reggio Emilia Michele Colajanni
• Univ. di Napoli "Federico II" Antonino Mazzeo
• Univ. di Napoli "Parthenope" Luigi Romano
• Univ. di Padova Mauro Conti
• Univ. di Palermo Giuseppe Lo Re
• Univ. di Parma Michele Tomaiuolo
• Univ. di Pavia Antonio Barili
• Univ. di Perugia Stefano Bistarelli
• Univ. di Pisa Gianluca Dini
• Univ. Politecnica delle Marche Marco Baldi
• Univ. di Roma "La Sapienza" Luigi Mancini
• Univ. di Roma "Tor Vergata" Maurizio Talamo
• Univ. di Salerno Carlo Blundo
• Univ. di Torino Francesco Bergadano
• Univ. di Trento Fabio Massacci
• Univ. di Udine Marino Miculan
• Univ. della Calabria Domenico Sacca'
• Univ. di Reggio Calabria Francesco Buccafurri
34 Local units
240 Faculties
— 68 Full Prof
— 57 Ass. Prof
— 100 Researchers
178 PhD students
76 postdocs
51 Experts
FONDAZIONE BRUNO KESSLER
ENEA


FP7 Success Stories Landscape
SecC rd
CSP forum
Austria
Belgium
Bulgaria
Cyprus
Czech Rep.
Denmark
Estonia
Finland
France
Germany
Greece
Hungary
Ireland
Italy
Luxembourg
Netherlands
Norway
Poland
Portugal
Rumania
Slovenia
Spain
Sweden
Switzerland
United Kingdom
0
5
10
15
20
25
30
35
Research
Industry
Consulting
Other
39

Cyber Security National Lab: Actions

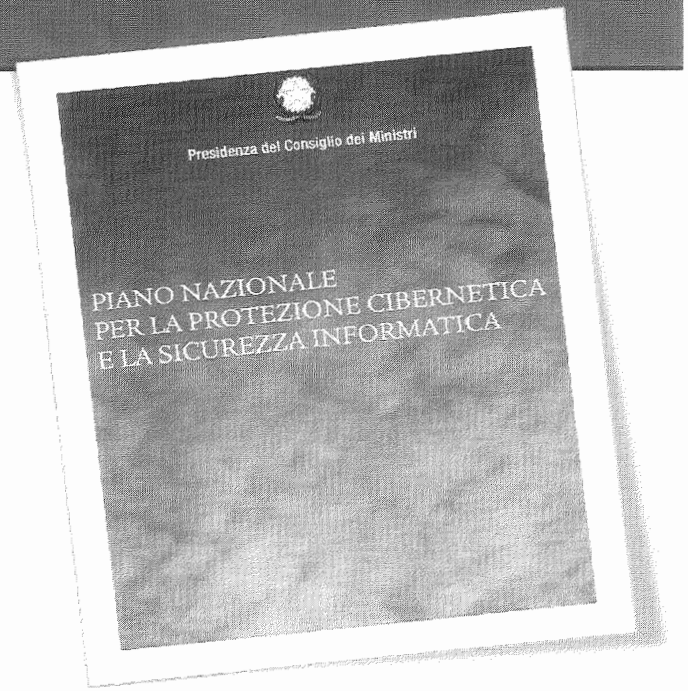
- Raising Awareness in the society
- continuous education - high level skills
- Supporting actions: Government, Industry, Finance
- Innovation &Research Excellence
- Main reference contact for large EU initiatives
- Coordination of excellence research units

Italian Cyber Security Architecture led by the Intelligence Dept. (DPCM Monti)
Tavolo Tecnico Imprese
Strategic Italian Companies
Cyber Security National Lab
Univ or Research agency
DPCM 23/1/2013
Presidency of ministers council
Intelligence dept.
Military Advisor
Cyber Security Office
Ministry Economic Development
AgID
ISCOM
MoD
Ministry Economic and Finance
Ministry of Justice
Ministry of Foreign Affairs
MoI

Current Actions

Action	Partner	Led by
Cyber Security National Framework	Presidency of Ministry Council	Sapienza
Cyber Range	Ministry of defense	Univ. of Genova
Polo Tecnologico	Presidency of Ministry Council and industries	Sapienza and others
Italian CERT	Ministry of Economic Development	Milan Polytechnic and others
Education	Presidency of Ministry Council	Trento Univ
Intelligence on the web	Presidency of Ministry Council	Sapienza
White book on cyber security for Italy	Presidency of Ministry Council	IMT Lucca-Sapienza and others
Italy-Israel action	Italian foreign office	Modena Univ.

Strategic Plan (11 operative objectives)



cini Cyber Security National Lab

The future of Cyber Security in Italy – A White Book

cini Cyber Security National Lab

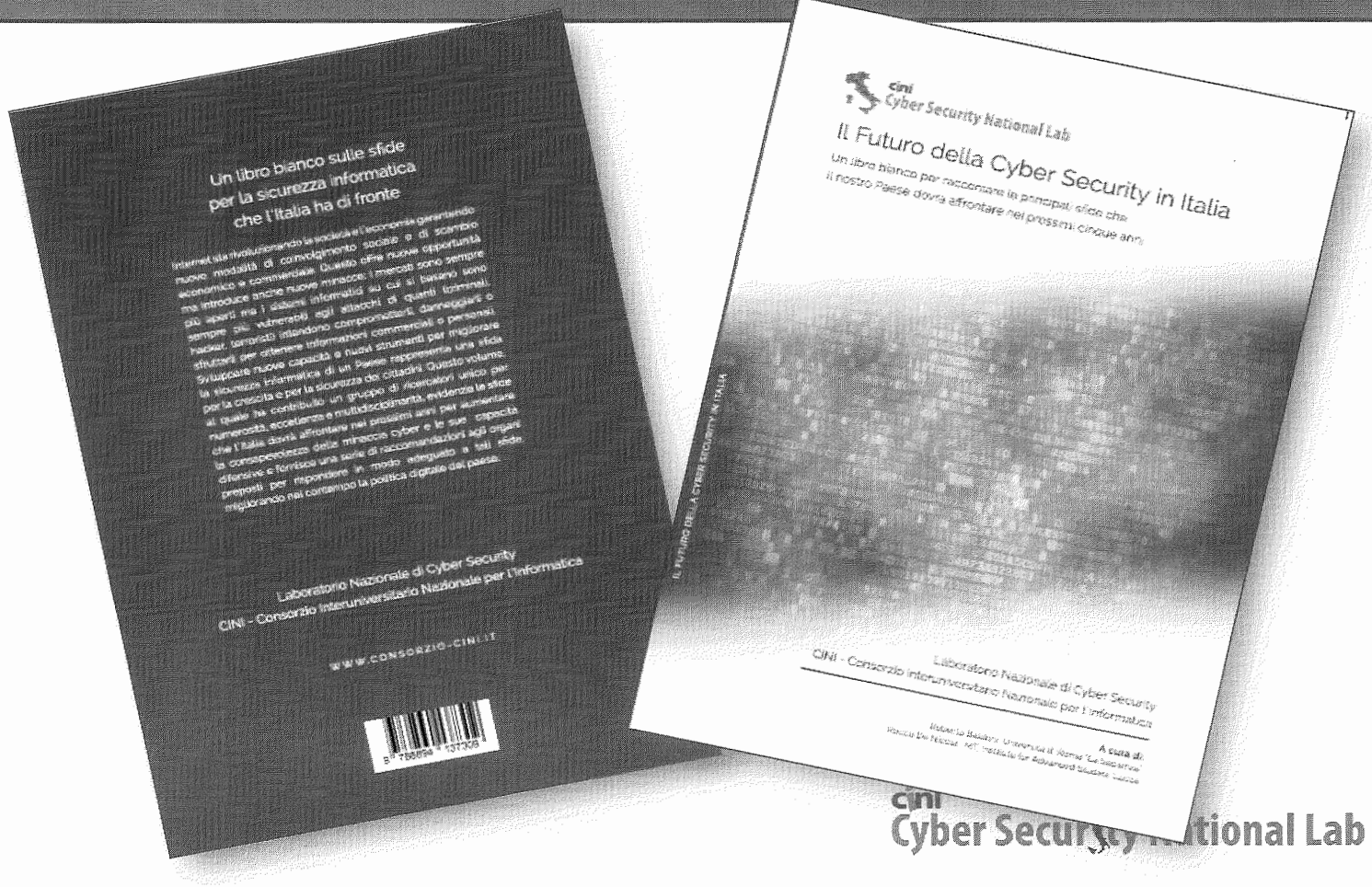
Paolo Prinetto

President of CINI

Politecnico di Torino

Paolo.Prinetto@polito.it

The future of Cyber-Security in Italy
A white book



Goals

- Outlining the *challenges* that the country has to face in the next 5 years to increase at any level:
  - The awareness of the cyber threats
  - Its defensive capabilities
- Proposing *recommendations* aimed at

Goals

- Outlining the *challenges* that the country has to face in the next 5 years to increase at any level:
  - The awareness of the cyber threats
  - Its defensive capabilities
- Proposing *actionable objectives* aimed at
  - Takling the challenges
  - Improving the country's digital policy

Targets

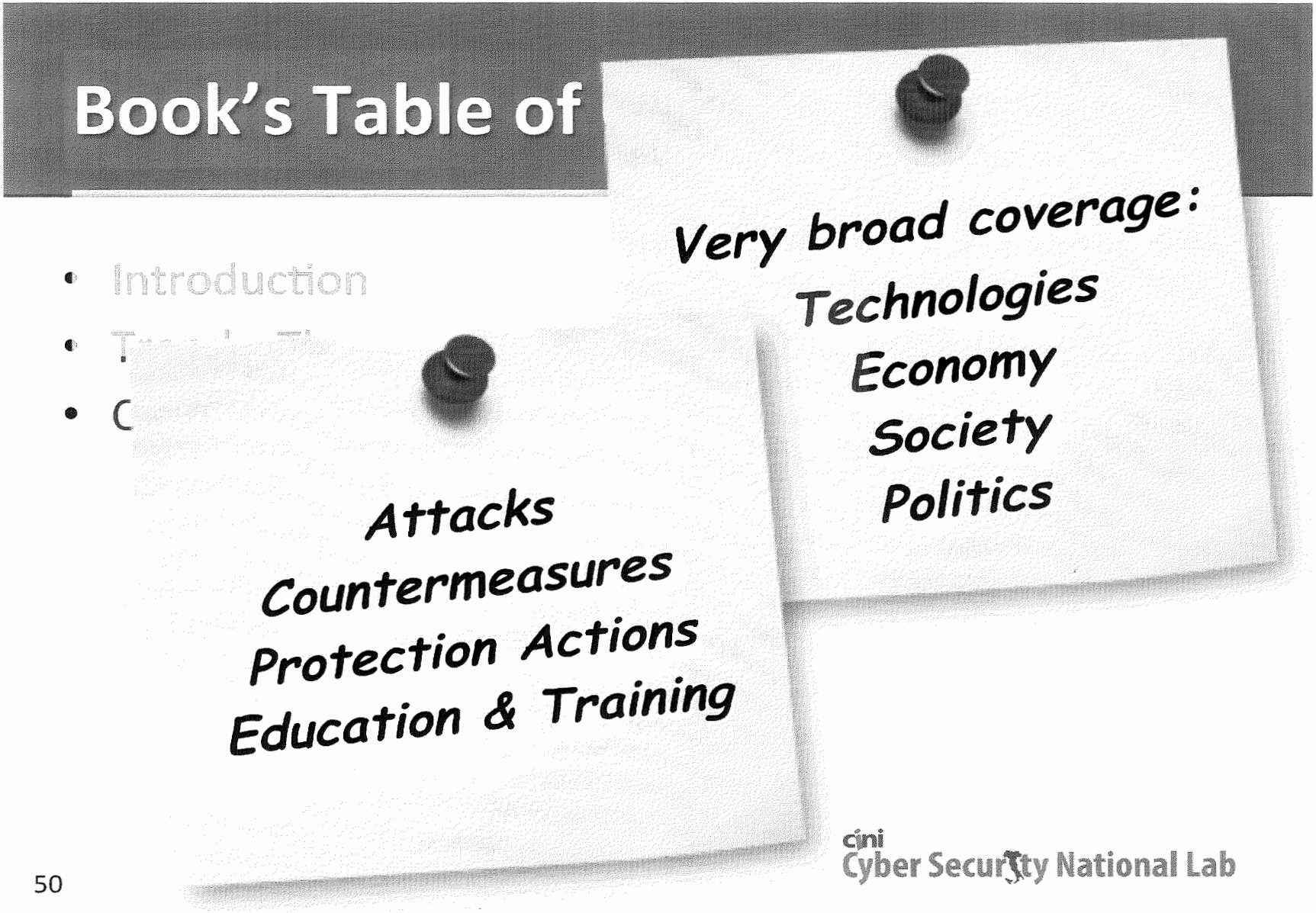
- Who:
  - *Policy & Decision Makers*
  - *Stakeholders*
  - *Managers*
  - *Professionals*
  - *Citizens*
  - *…*

cini Cyber Security National Lab

Targets

- Where:
  - *Industries*
  - *Public Administrations*
  - *Private & Public Sectors*
  - *Universities*
  - *Society*
  - *...*

cini Cyber Security National Lab


Book's Table of
Introduction
Very broad coverage:
Technologies
Economy
Society
Politics
Attacks
Countermeasures
Protection Actions
Education & Training
cini
Cyber Security National Lab
50

The Challenges

- *Internet of Things*
- *Critical Infrastructures & Cyber Physical Systems*
- *Organization, Human Factor & Social Engineering*
- *Secure and Trusted Hardware*
- *Biometry*
- *Advanced Cryptography*
- *Internet Protection*
- *Data & Information Protection*
- *Attack Surface Minimization*
- *Complex Information System Design*
- *Cyber Range*
- *Digital Investigations*
- *Intelligence & Big Data Analytics*
- *Information Sharing*
- *Risk Assessment Metrics*

cini Cyber Security National Lab

Book's Table of Contents

- Introduction
- Trends, Threats, the Italian Legal Framework
- Challenges
- Recommendations

cini Cyber Security National Lab

Book's Table of

- Introduction
- Trends, Threats, the Itali
- Challenges
- Recommendations

cini Cyber Security National Lab

Book's Table of

- Introduction
- Trends Threats the [illegible]

1. Strategy, Planning & Control
2. Security as an Investment
3. Cyber Security Center (I-PPP)
4. Consolidation
5. Education & Training
6. National Security Framework

cini Cyber Security National Lab

Book's Table of Contents

- Introduction
- Trends, Threats, the Italian Legal Framework
- Challenges
- Recommendations
- Appendix: Actions taken in some foreign countries

cini Cyber Security National Lab

National Framework for Cyber Security
www.cybersecurityframework.it
(in alignment with US NIST)
cini Cyber Security National Lab

Il "Framework Nazionale per la Cyber Security" è uno strumento definito in un contesto PPP che serve per aumentare la velocità di implementazione del piano strategico nazionale

cini Cyber Security National Lab

Framework Nazionale per la Cyber Security: obiettivi

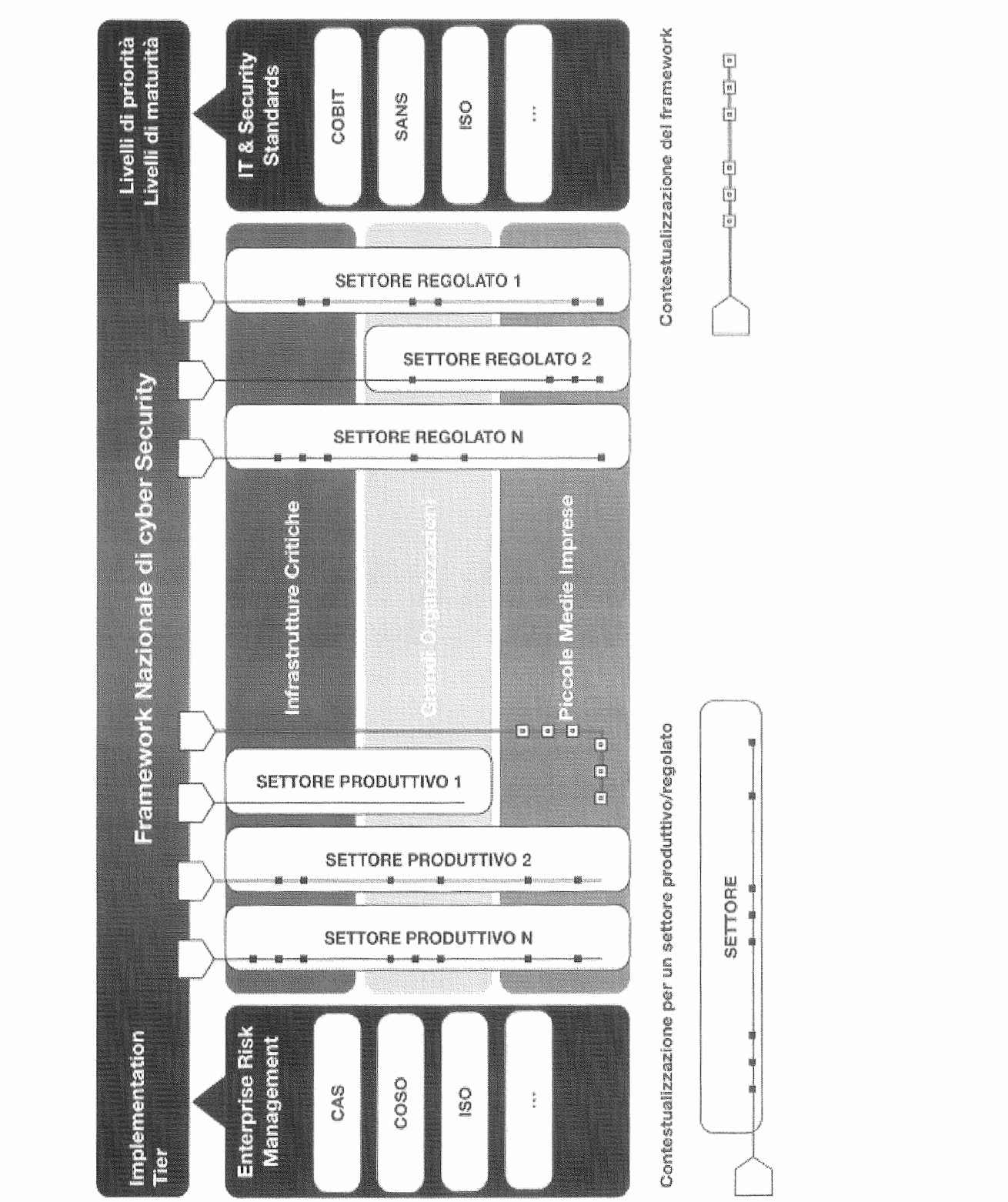
- Rischio cyber come un rischio economico aziendale (parte del risk management e del DNA aziendale)
- Portare il rischio cyber nei CDA (non rimanere confinato nell'ambiente tecnico)
- Considerare lo scenario economico italiano (dominato dalla presenza di PMI) ed i diversi settori produttivi
- Non reinventare la ruota (il framework non è tecnologia è metodologia)

cini Cyber Security National Lab

Il framework nazionale è uno strumento (ad adozione volontaria) di auto-analisi di una organizzazione

cini Cyber Security National Lab

59


Framework Nazionale di cyber Security
Implementation Tier
Livelli di priorità
Livelli di maturità
IT & Security Standards
COBIT
SANS
ISO
...
Enterprise Risk Management
CAS
COSO
ISO
...
SETTORE REGOLATO 1
SETTORE REGOLATO 2
SETTORE REGOLATO N
SETTORE PRODUTTIVO 1
SETTORE PRODUTTIVO 2
SETTORE PRODUTTIVO N
Infrastrutture Critiche
Piccole Medie Imprese
Contestualizzazione del framework
Contestualizzazione per un settore produttivo/regolato
SETTORE

Framework Nazionale per la Cyber Security: Vantaggi grandi imprese

- Top Management Awareness
- Un aiuto a definire piani a risorse sostenibili di gestione del rischio cyber (anche attraverso lo strumento assicurativo)
- Gestione della catena di approvvigionamento
- Un aiuto nell'approntare un processo evoluto di gestione del rischio cyber

cini Cyber Security National Lab

Framework Nazionale per la Cyber Security: Vantaggi per la nazione

- Fornire una quadro comune a diverse autorità che regolamentano il settore in modo da regolamentare in modo coerente e.g.,Garante Privacy, AGID, PCM, ecc.)
- International due diligence

cini Cyber Security National Lab

NOTE CONCLUSIVE

63

Difesa e Cyber

- Sviluppare capacità di difesa attiva (se abbiamo un attacco che proviene da un altro paese verso nostre infrastrutture informatiche militari o civili, chi si occupa di bloccarlo?)

Architettura Cyber Nazionale

- Rispetta architettura Costituzionale italiana
- Deve acquisire velocità
- Se non la raggiunge dovrebbe essere revisionata su alcuni punti cardine
  - Semplificazione architettura
  - Chiaro commit "cyber" di almeno una struttura

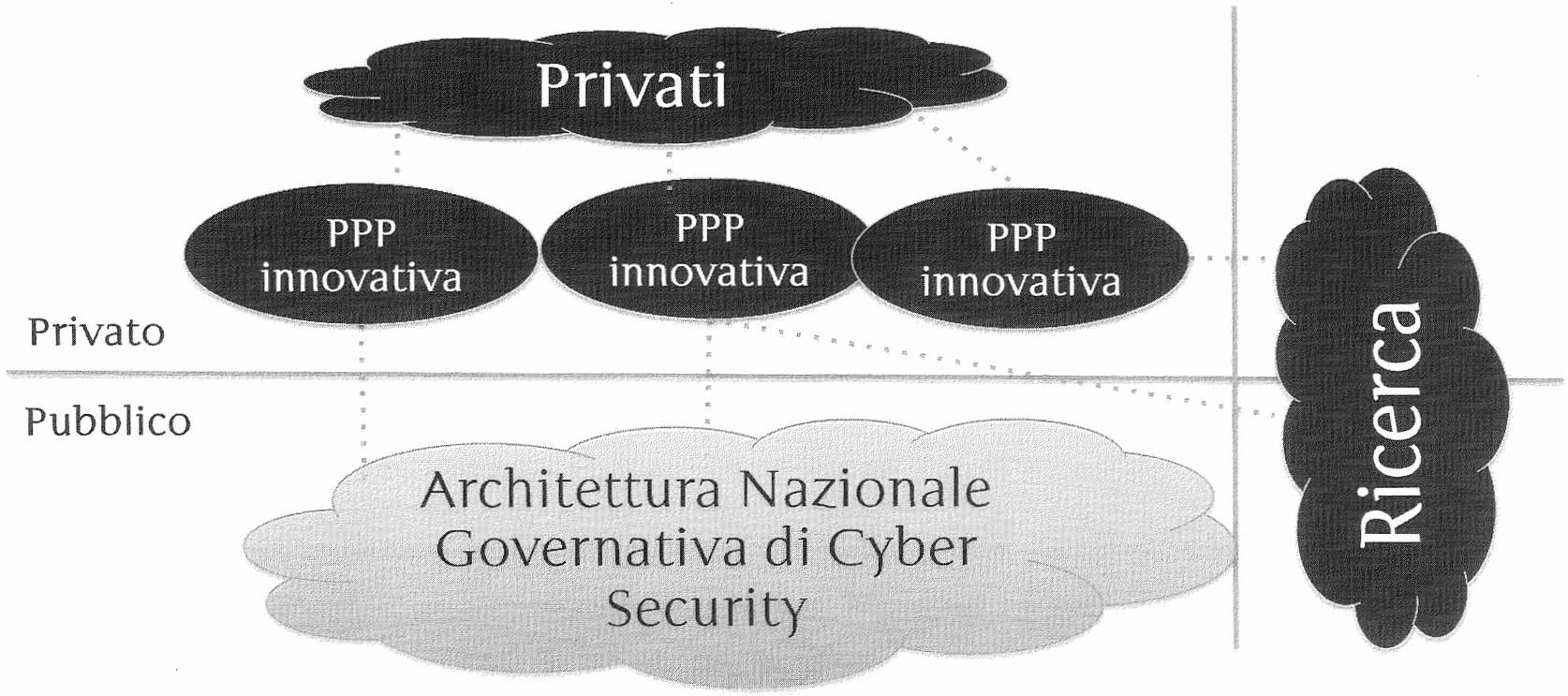
cini Cyber Security National Lab

PPP innovative

- Tuttavia anche se otteniamo la migliore architettura cyber istituzionale possibile
- Per acquisire ancora piu' velocità abbiamo bisogno che il pubblico interagisca fortemente con Privato e Accademia

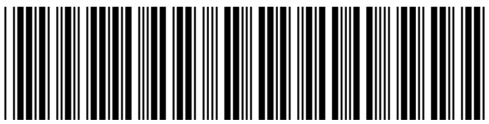
cini Cyber Security National Lab

"The Italian way" per accelerare



cini Cyber Security National Lab

Stampato su carta riciclata ecologica



17STC0016670