Presidenza del Consiglio dei Ministri

QUADRO STRATEGICO NAZIONALE PER LA SICUREZZA DELLO SPAZIO CIBERNETICO

Dicembre 2013

Presidenza del Consiglio dei Ministri

QUADRO STRATEGICO NAZIONALE PER LA SICUREZZA DELLO SPAZIO CIBERNETICO

Dicembre 2013

Lista delle sigle e delle abbreviazioni

AG – Autorità Giudiziaria
AGCOM – Autorità per le Garanzie nelle Comunicazioni
AgID – Agenzia per l'Italia Digitale
APT – Advanced Persistent Threat
BYOD – Bring Your Own Device
ccTLD – Country Code Top Level Domain
CERT – Computer Emergency Response Team
CERT-SPC – Computer Emergency Response Team - Sistema Pubblico di Connettività
CISR – Comitato Interministeriale per la Sicurezza della Repubblica
CLUSIT – Associazione Italiana per la Sicurezza Informatica
CNA – Computer Network Attacks
CNAIPIC – Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche
CND – Computer Network Defence
CNE – Computer Network Exploitation
CNO – Computer Network Operations
CSBM – Confidence and Security Building Measures
CSDP – Common Security and Defence Policy
DAG – Dipartimento dell'Amministrazione Generale e del Personale e dei Servizi
DDoS – Distributed Denial of Service
DF – Digital Forensics
DIS – Dipartimento Informazioni per la Sicurezza
DNS – Domain Name System
DPCM – Decreto del Presidente del Consiglio dei Ministri
DSII – Direzione dei Sistemi Informativi e dell'Innovazione
EMEA – European, Middle East and Africa
ENISA – European Network and Information Security Agency
F.A. – Forze Armate
FF.PP. – Forze di Polizia
IC – Infrastrutture Critiche
ICE – Infrastrutture Critiche Europee
ICT – Information & Communication Technologies
IoT – Internet of Things
ISCOM – Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione
ISP – Internet Service Provider
IT – Information Technologies
MEF – Ministero dell'Economia e delle Finanze
NATO – North Atlantic Treaty Organization
NCIRC – NATO Computer Incident Response Capability
NSC – Nucleo per la Sicurezza Cibernetica
ONU – Organizzazione delle Nazioni Unite
OSCE – Organizzazione per la Sicurezza e la Cooperazione in Europa
PA – Pubblica Amministrazione
PMI – Piccole e Medie Imprese
R&S – Ricerca & Sviluppo
SCADA – Supervisory Control and Data Acquisition
SMS – Short Message Service
SOC – Security Operations Center
SPC – Sistema Pubblico di Connettività
TCP/IP – Transmission Control Protocol/Internet Protocol
QSN – Quadro Strategico Nazionale
UE – Unione Europea
ULS – Unità Locali di Sicurezza
UTM – Unified Threat Management

INDICE

PREFAZIONE

Lo sviluppo di Internet caratterizza la nostra era. È attraverso lo spazio cibernetico che sempre più si realizzano le fondamentali libertà di informazione, di espressione e di associazione del cittadino, viene perseguita la trasparenza della politica e l'efficienza dei servizi della Pubblica Amministrazione, si promuove la crescita e l'innovazione delle nostre aziende. Lo spazio virtuale rappresenta un'arena in cui ogni giorno si stabiliscono attraverso le frontiere geografiche miliardi di interconnessioni e si scambia conoscenza a livello globale, ridisegnando il mondo ad una velocità senza precedenti.

Il risiedere all'interno delle reti di una mole ogni giorno maggiore di saperi essenziali ai fini della sicurezza e della prosperità del sistema-Paese rende sempre più pressante l'esigenza di garantire, anche nello spazio cibernetico, il rispetto dei diritti e dei doveri, che già vigono nella società civile, nel tessuto economico e nella Comunità internazionale. L'arena digitale non è uno spazio al di fuori delle leggi, ed è nostra responsabilità lavorare affinché vi si affermino compiutamente i valori ed i princìpi democratici, oltre che le norme di rispetto dell'individuo, di eguaglianza e di libertà nelle quali crediamo. È peraltro solo in un ambiente contrassegnato da fiducia e rispetto reciproco che sarà possibile cogliere appieno le opportunità di crescita offerte dalle piattaforme digitali, assicurando lo sviluppo di uno spazio cibernetico aperto, affidabile e sicuro per il sistema finanziario, per le aziende e per i consumatori.

La crescente dipendenza delle società moderne dallo spazio cibernetico rende sempre più grave il danno che può giungere dalla compromissione delle reti o

da mirati attacchi attraverso di esse. Le minacce possono originare da qualsiasi punto della rete globale e spesso colpiscono gli anelli più deboli della catena, ossia i soggetti più fragili, o i sistemi meno protetti. Attraverso le reti possono compiersi crimini odiosi come lo scambio online di materiale pedopornografico, o realizzarsi furti e truffe che, oltre a danneggiare gravemente gli interessi privati, impediscono che si affermi il necessario livello di fiducia nella comunità digitale.

Il crimine informatico è una piaga che può decretare il fallimento delle aziende, la sottrazione del loro patrimonio tecnologico e che depaupera la ricchezza delle nazioni. Con sempre maggiore preoccupazione assistiamo inoltre al crescere di una minaccia ancora più insidiosa, che sfrutta le vulnerabilità dei sistemi informatici per sottrarre, spesso senza che ve ne sia nemmeno la cognizione, il frutto del nostro lavoro di ricerca e sviluppo nel campo delle nuove tecnologie e dei prodotti. Per un Paese come l'Italia, che fa dell'innovazione la pietra angolare della sua crescita e della sua competitività, il danno potenziale è incalcolabile. La sofisticazione degli attacchi informatici e la connessione in rete delle nostre infrastrutture crescono ad un ritmo tale che la stessa stabilità e sicurezza del Paese possono essere gravemente pregiudicate, ed è dunque indispensabile assicurare la migliore protezione degli assetti critici nazionali da attacchi che possono produrre enormi danni fisici e materiali, ad esempio attraverso la paralisi o l'alterazione d'interi sistemi che regolano il trasporto civile e le reti energetiche, o ancora i sistemi di comando e controllo militari. Ciò implica dunque la necessità di un concetto di difesa innovativo e compar-

tecipato con il mondo del privato, che in molti casi è al contempo proprietario e gestore degli assetti critici da tutelare, oltre che l'urgenza d'incorporare la dimensione informatica dei moderni conflitti nella dottrina strategica e nella pianificazione delle forze.

L'interdipendenza delle reti, l'asimmetricità della minaccia e la pervasività dello spazio cibernetico nella vita di ogni giorno rendono impossibile assicurare un accettabile livello di sicurezza online in assenza di un approccio olistico e di una forte unitarietà d'intenti. L'obiettivo non può che essere quello di potenziare a livello sistemico le nostre capacità di prevedere e prevenire un attacco, individuarlo nel momento in cui accade, reagire ad esso e mitigarne gli effetti, risalire ai responsabili, oltre che di ristabilire rapidamente la funzionalità originaria ed apprendere le lezioni del caso. A livello internazionale, l'Italia è impegnata tanto nei maggiori consessi multilaterali, in primis l'Unione Europea e la NATO, quanto a livello bilaterale, con i nostri principali partner, per favorire l'affermazione ed il rispetto di regole di comportamento nell'arena digitale coerenti con i nostri valori, oltre che per facilitare l'emergere di una governance condivisa a livello globale, indispensabile per far fronte alle grandi sfide della rivoluzione digitale in atto. A livello nazionale, è imperativo sviluppare un approccio coordinato e multi-dimensionale, che garantisca la più ampia convergenza dell'azione delle diverse Amministrazioni dello Stato attorno ad obiettivi pienamente condivisi e ampiamente partecipati con il mondo del privato, accademico e della ricerca scientifica.

In un clima economico-finanziario contrassegnato dalle ben note difficoltà di bilancio non possiamo permetterci alcuna duplicazione degli sforzi ed occorre saper ricercare ogni utile sinergia, tenendo a mente che gli stanziamenti che si renderanno – da parte di tutti – necessari rappresentano non solo un significativo risparmio rispetto al danno potenziale cui siamo soggetti, ma anche una straordinaria opportunità di crescita culturale, sociale ed economica.

In linea con quanto previsto dal DPCM del 24 gennaio 2013, il presente Quadro Strategico Nazionale per la sicurezza dello spazio cibernetico individua i profili e le tendenze evolutive delle minacce e delle vulnerabilità dei sistemi e delle reti d'interesse nazionale, specifica i ruoli ed i compiti dei diversi soggetti pubblici e privati ed individua gli strumenti e le procedure con cui perseguire l'accrescimento delle capacità del Paese di prevenire e rispondere in maniera compartecipata alle sfide poste dallo spazio cibernetico. Con l'allegato Piano Nazionale vengono inoltre individuate le priorità, gli obiettivi specifici e le linee d'azione per dare concreta attuazione a quanto descritto nel Quadro Strategico.

Con questi due documenti l'Italia si dota di una strategia attorno alla quale coordinare gli sforzi per rafforzare la nostra capacità di fare squadra per guardare con fiducia alle sfide di sicurezza dello spazio cibernetico e per fare avanzare l'interesse nazionale laddove sempre più si realizza la ricchezza delle nazioni.

EXECUTIVE SUMMARY

Il presente Quadro Strategico Nazionale è stato elaborato dal Tavolo Tecnico Cyber (TTC) che – istituito il 3 aprile 2013 in seno all'organismo collegiale permanente (c.d. CISR "tecnico") dopo l'entrata in vigore del DPCM 24 gennaio 2013 – opera presso il Dipartimento Informazioni per la Sicurezza. Ai lavori del TTC partecipano i rappresentanti cyber dei Dicasteri CISR (Affari Esteri, Interno, Difesa, Giustizia, Economia e Finanze, Sviluppo Economico) dell'Agenzia per l'Italia Digitale e del Nucleo per la Sicurezza Cibernetica.

La definizione di un Quadro Strategico Nazionale per la sicurezza dello spazio cibernetico non può prescindere da un inquadramento della minaccia che, in considerazione della sempre maggiore diffusione dell'impiego delle tecnologie ICT nella vita quotidiana – dal semplice pagamento di beni e servizi per via telematica alla gestione di infrastrutture critiche e strategiche nazionali – diverrà anch'essa più pervasiva e subdola, col rischio di venire ignorata o sottovalutata dai fruitori di tali tecnologie.

Nel *Capitolo 1, "Profili e tendenze evolutive delle minacce e delle vulnerabilità dei sistemi e delle reti di interesse nazionale"*, si intende fornire una panoramica delle principali minacce – dalla criminalità informatica allo sfruttamento delle tecnologie ICT per fini terroristici, dall'"hacktivismo" allo spionaggio cibernetico, dal sabotaggio per via informatica ai conflitti nella 5a dimensione – e delle vulnerabilità sfruttate per la conduzione di attacchi nello spazio cibernetico, sia di tipo tecnico che di tipo organizzativo e di processo.

Lo spazio cibernetico, tuttavia, è, in prima battuta, un insieme di nodi (i sistemi) e di collegamenti (le reti) che, attraverso la gestione di una mole sempre maggiore di dati, costituiscono una risorsa cruciale per gli Stati, le aziende, i cittadini e tutti gli attori che curano interessi politici, militari, economici e sociali affidandosi alle nuove tecnologie.

Al fine, quindi, di garantire al Paese la tutela di tali istanze, sono stati identificati, *nel Capitolo 2 "Strumenti e Procedure per potenziare le capacità cibernetiche del Paese*", gli indirizzi strategici che includono il mi-

glioramento, secondo un approccio integrato, delle capacità tecnologiche, operative e di analisi degli attori istituzionali; il potenziamento delle capacità di difesa delle Infrastrutture Critiche nazionali e degli attori di rilevanza strategica per il sistema-Paese; l'incentivazione della cooperazione tra istituzioni e imprese nazionali; la promozione e diffusione della cultura della sicurezza cibernetica; il rafforzamento delle capacità di contrasto alla diffusione di attività e contenuti illegali *on-line*; il rafforzamento della cooperazione nazionale in materia di sicurezza cibernetica.

A corollario di quanto sopra, in ***Allegato 1*** sono elencati i "***Ruoli e compiti dei soggetti pubblici***", mentre in ***Allegato 2*** è possibile consultare un breve "***Glossario***" dei termini tecnici impiegati, al fine di agevolare la lettura del documento anche da parte dei "non addetti ai lavori".

CAPITOLO 1

PROFILI E TENDENZE EVOLUTIVE DELLE MINACCE E DELLE VULNERABILITÀ DEI SISTEMI E DELLE RETI DI INTERESSE NAZIONALE

Introduzione

Definizione

Lo spazio cibernetico è l'insieme delle infrastrutture informatiche interconnesse, comprensivo di hardware, software, dati ed utenti, nonché delle relazioni logiche, comunque stabilite, tra di essi. Esso dunque comprende internet, le reti di comunicazione, i sistemi su cui poggiano i processi informatici di elaborazione dati e le apparecchiature mobili dotate di connessione di rete.

Una sfida complessa

La natura stessa dello spazio cibernetico e dell'informatizzazione, importanti fattori di trasformazione delle società contemporanee, fa emergere problemi culturali, sociali e politici inediti ed in relazione ai quali occorre elaborare e concordare soluzioni efficaci, coerenti e, in molti casi, innovative.

In una Comunità Internazionale ancora caratterizzata da significative divergenze circa le categorie tassonomiche utilizzate per definire la realtà politico-strategica e tecnologica dello spazio cibernetico e circa i valori ed i princìpi che debbono informare l'arena digitale, la ricerca di tali soluzioni, anche all'interno degli Stati più avanzati, non è semplice e richiede un attivo coinvolgimento del settore privato.

L'onere di trovare risposte alle nuove e complesse sfide che emergono dal *cyber*-spazio non può ricadere sulle sole istituzioni pubbliche, anche in considerazione del fatto che le reti sono in larghissima parte possedute ed operate da soggetti privati i quali devono, quindi, sapere e potere condividere aspettative e responsabilità per la protezione dello spazio cibernetico.

Esso costituisce un dominio virtuale di importanza strategica per lo sviluppo economico, sociale e culturale delle nazioni e proprio per questo è necessario equilibrare con attenzione il rapporto tra Stato ed individuo, tra esigenze di sicurezza nazionale e di ordine pubblico, da un lato, e libertà individuali, dall'altro.

Si pensi, ad esempio, come l'ininterrotto monitoraggio tecnico della funzionalità delle reti e la protezione dei dati che vi transitano siano essenziale presupposto per il pieno godimento del diritto

alla *privacy* e dell'integrità dei sistemi oppure, sempre a titolo di esempio, come possa essere complesso ricercare il giusto equilibrio tra il diritto alla *privacy* e la necessaria azione di contrasto a crimini come l'uso della rete per lo scambio di materiale pedopornografico, lo spaccio di stupefacenti, l'incitamento all'odio o la pianificazione di atti di terrorismo. Reati che, oltre a ledere specifici diritti, rappresentano un attacco all'idea stessa di un dominio cibernetico libero, democratico ed aperto.

Finalità

Il Quadro Strategico Nazionale ed il Piano Nazionale previsti dal DPCM del 24 gennaio 2013 mirano ad accrescere la capacità di risposta del Paese alle presenti e future sfide riguardanti il *cyber-space*, indirizzando gli sforzi nazionali verso obiettivi comuni e soluzioni condivise, nella consapevolezza che la protezione dello spazio cibernetico è un processo più che un fine, che la continua innovazione tecnologica introduce inevitabilmente nuove vulnerabilità, e che le caratteristiche stesse della minaccia cibernetica rendono la difesa, per ora, di tipo prevalentemente – anche se non esclusivamente – reattivo.

La minaccia cibernetica ed i suoi attori

Definizione

Con minaccia cibernetica intendiamo l'insieme delle condotte controindicate che possono essere realizzate nel e tramite lo spazio cibernetico ovvero in danno di quest'ultimo e dei suoi elementi costitutivi. La minaccia si sostanzia nei c.d. attacchi cibernetici: azioni più o meno automatizzate sulle reti da parte di singoli individui o organizzazioni, statuali e non, finalizzate a distruggere, danneggiare o ostacolare il regolare funzionamento dei sistemi, delle reti o dei sistemi attuatori di processo da essi controllati ovvero a compromettere l'autenticità, l'integrità, la disponibilità e la riservatezza dei dati ivi custoditi o che vi transitano.

Attualmente gli attacchi più sofisticati possono essere realizzati attraverso l'uso di c.d. "armi cibernetiche" – ossia *software* malevoli appositamente sviluppati (definiti "*malware*"), o un insieme di istruzioni informatiche – posti in essere con lo specifico intento di danneggiare o alterare un sistema informatico anche al fine di produrre danni fisici.

Una minaccia insidiosa

Una caratteristica saliente della minaccia cibernetica è la sua asimmetricità. L'attaccante infatti:

- può colpire a grandissima distanza, da dovunque nel mondo esista un accesso alla rete;
- potenzialmente può attaccare sistemi particolarmente sofisticati e protetti sfruttandone anche una sola vulnerabilità;
- può agire con tempi tali da non consentire un'efficace reazione difensiva;
- può rimanere anonimo o comunque non facilmente individuabile rendendo in tal modo estremamente complessa e difficile una corretta risposta da parte dell'attaccato.

La natura stessa della minaccia cibernetica, quindi, limita la deterrenza, fa prevalere tendenzialmente l'attacco sul-

la difesa e rende indispensabile, da parte dei soggetti principali che operano nel *cyber*-spazio (Governi ed aziende), l'implementazione di un continuo processo di analisi che permetta loro di adeguare gli standard e le procedure di sicurezza al contesto operativo e tecnologico in veloce cambiamento.

Tipi di minaccia

A seconda degli attori e delle finalità si usa distinguere la minaccia cibernetica in quattro macro-categorie. Si parla in tal caso di:

- criminalità cibernetica (*cyber-crime*): complesso delle attività con finalità criminali (quali, per esempio, la truffa o frode telematica, il furto d'identità, la

sottrazione indebita di informazioni o di creazioni e proprietà intellettuali);
- spionaggio cibernetico (*cyber-espionage*): acquisizione indebita di dati/informazioni sensibili, proprietarie o classificate;
- terrorismo cibernetico (*cyber-terrorism*): insieme delle azioni ideologicamente motivate, volte a condizionare uno stato o un'organizzazione internazionale;
- guerra cibernetica (*cyber-warfare*): insieme delle attività e delle operazioni militari pianificate e condotte allo scopo di conseguire effetti nel predetto ambiente.

L'impatto economico del cyber-crime

Il risiedere sulle reti di una mole sempre crescente di dati aziendali o relativi allo status patrimoniale degli individui grazie ai servizi di *cloud computing*, assieme al sempre maggiore utilizzo dello spazio cibernetico per attività finanziarie, economiche e commerciali, rendono gli attacchi cibernetici potenzialmente assai lucrativi esponendo l'attaccante, per giunta, ad un rischio relativamente basso.

I danni economici generati dal crimine informatico sono elevati. In particolar modo nei Sistemi-Paese come l'Italia, per i quali il furto del *know-how* scientifico, tecnologico ed aziendale comporta un danno diretto e grave alla capacità di rimanere innovativi e dunque di essere competitivi nei mercati internazionali. Inoltre, una parte dell'ingente quantità di capitali illecitamente ottenuti tramite i crimini informatici viene reinvestita nella ricerca di nuove vulnerabilità dei sistemi da attaccare e nello sviluppo di strumenti più sofisticati ed efficienti, rendendo il crimine cibernetico una minaccia sempre più seria e di primaria rilevanza per la stabilità, il benessere e la sicurezza del Paese.

Il mercato del computer crime

Il *computer crime market* rappresenta dunque un settore appetibile e redditizio sia per singoli *hackers* che per organizzazioni criminali che alimentano un mercato nero in cui è possibile commerciare contenuti illegali (ad esempio stupefacenti, materiale pedopornografico o protetto da *copyright*) e strumenti per realizzare, in proprio o con il supporto tecnico delle organizzazioni criminali stesse, reati contro il patrimonio (truffe, ricatti, estorsioni, furti, ecc.), sottrazione di dati sensibili e d'identità (ad esempio ai fini di riscatto o per perpetrare altri reati), riciclaggio di capitali illeciti, giochi d'azzardo e scommesse illegali.

Si registra, inoltre, un crescente coinvolgimento dei gruppi criminali che operano nel *cyber-space* in attività di spionaggio industriale nell'ambito delle quali, anche su mandato di imprese concorrenti, sottraggono (o concorrono a sottrarre) brevetti industriali, piani aziendali, studi e ricerche di mercato, analisi e descrizioni dei processi produttivi, ecc.

Il ruolo degli Stati

Benché lo spazio cibernetico sia una realtà che trascende, sotto molti punti di vista, le frontiere nazionali, gli Stati ne sono, certamente, gli attori più rilevanti nella misura in cui hanno la primaria responsabilità per la protezione di reti ed infrastrutture collocate sul proprio territorio, pur se detenute ed operate in massima parte dal settore privato.

Gli Stati, infatti, dispongono di adeguate risorse umane e finanziarie, oltre che della capacità di organizzare e gestire per lungo tempo organizzazioni complesse. In quanto tali, quindi, essi sono gli attori maggiormente in grado di sviluppare una robusta capacità operativa nello spazio cibernetico.

Se l'assicurare la protezione, la resilienza e la piena operatività delle proprie reti di comunicazione e controllo militari è, da sempre, un'esigenza vitale per ogni Stato, la creazione dello spazio cibernetico (che supporta oggigiorno il funzionamento di pressoché ogni infrastruttura critica nazionale, oltre che dei processi produttivi dell'industria e della fornitura di servizi al cittadino) ha imposto la necessità d'ampliare tale capacità alla difesa delle reti critiche nazionali.

Gli attacchi cibernetici più sofisticati, infatti, non solo sono potenzialmente in grado di danneggiare o paralizzare il funzionamento di gangli vitali dell'apparato statale e la fornitura di servizi essenziali ai cittadini, ma possono avere anche effetti potenzialmente distruttivi (soprattutto in prospettiva) se impiegati per indurre il malfunzionamento delle infrastrutture critiche (ad esempio reti di controllo del traffico aereo, dighe, impianti energetici, ecc.), generando danni materiali ingenti e la potenziale perdita di vite umane.

Il vantaggio strategico derivante dalla possibilità d'infliggere un rilevante danno ad assetti nazionali critici del nemico operando a distanza fa ritenere probabile che i futuri conflitti internazionali comprenderanno anche lo spazio cibernetico. Non sorprende, dunque, che la pianificazione delle forze, pressoché ovunque nel mondo, prenda in considerazione la necessità d'assicurare un adeguato livello di *cyber-defence* agli assetti critici nazionali.

Spionaggio, sabotaggio, guerra, supply chain threat

La difesa delle proprie reti implica lo sviluppo di un'efficiente e continua capacità di monitoraggio e di analisi degli attacchi. Si tratta di strumenti che alcuni Stati stanno sviluppando, attraverso proprie strutture o mediante il ricorso a strutture para-statali, con intenti anche offensivi. Attualmente, diversi Governi si sono dotati delle necessarie *capabilities* per penetrare le reti nazionali degli altri Stati (in uso sia alle autorità pubbliche che ai privati) a fini di spionaggio o per mappare i sistemi potenzialmente oggetto di un futuro attacco.

In tal senso è necessario segnalare come appaia concreto il rischio che alcuni Paesi mobilitino la propria industria nazionale al fine di alterare componenti *hardware* da essa prodotte acquisendo così la capacità di superare in maniera pressoché irrilevabile ogni difesa posta in essere dall'utilizzatore dell'assetto finito.

Hacktivism

Vi sono diverse tipologie di attacco motivate ideologicamente, con intento sostanzialmente dimostrativo, che mirano principalmente a creare un danno d'immagine e/o alla funzionalità temporanea di sistemi e reti: si tratta di attacchi, come i *Distributed Denial of Service* (DDoS), che, attraverso il coordinato utilizzo in remoto di reti di computer inconsapevoli (botnets), causano l'intenzionale sovraccarico dei server che ospitano un determinato servizio, o i *Web Defacements*, che alterano i dati di

un determinato sito internet per disinformazione, calunnia o semplice dileggio. In altri casi, attivisti fanno uso di *malware* non dissimili da quelli utilizzati da *hackers* e criminali informatici per sottrarre surrettiziamente dati di proprietà dei Governi, delle aziende o degli individui al fine di esporli pubblicamente, o anche solo per dimostrare le proprie capacità informatiche.

Uso illegale della rete

L'arena digitale è uno straordinario strumento per mettere in contatto tra loro, a livello globale, le persone. Esiste però anche il concreto rischio che questa piattaforma e l'ampio anonimato da essa consentito siano sfruttati da chi vuole utilizzare la rete per diffondere odio razziale, scambiare materiale illegale (ad esempio pedopornografico) o pianificare crimini, atti eversivi ed attentati terroristici. Benché non si possa dire che si sia in presenza di una minaccia cibernetica secondo la definizione sopra abbozzata, in quanto in questo caso la rete digitale viene utilizzata solo quale strumento di comunicazione, è evidente che la natura stessa dello spazio cibernetico rende la minaccia particolarmente insidiosa. Occorre pertanto affermare chiaramente che nel dominio cibernetico valgono le regole della convivenza civile e del rispetto reciproco che già vigono nella società. La sfida che si pone è dunque quella di preservare la libertà di espressione all'interno della rete, assicurando, al pari di

quanto avviene nei domini classici, che essa non venga utilizzata per attività che sarebbero illegali al di fuori della stessa.

Terrorismo

È possibile ipotizzare che nel prossimo futuro gruppi terroristici o singoli individui possano impiegare strumenti cibernetici offensivi ed utilizzarli contro obiettivi militari e civili. I *malware* potrebbero essere loro venduti già "pronti per l'uso" dalle organizzazioni criminali che operano nel *computer crime market* o essere sviluppati autonomamente, magari a partire dall'analisi di quelli già immessi nello spazio cibernetico (processi di *reverse engineering*). Si tratta di una minaccia per ora solo ipotetica, ma occorre vigilare affinché tali strumenti distruttivi rimangano fuori dalla portata di potenziali utilizzatori.

Evento inatteso, incidente

Il resoconto delle minacce che promanano dallo spazio cibernetico non sarebbe completo se non tenesse in considerazione che, in un dominio caratterizzato da una continua evoluzione tecnologica, non si possono escludere eventi inattesi che pongono sfide tecnologiche o di *governance* e che richiedono uno sforzo collettivo mirato e sistemico.

È necessario sottolineare come lo spazio cibernetico sia un dominio creato dall'uomo e, in quanto tale, potenzialmente fallibile. Occorre, quindi, sviluppare capacità per anticipare e prevenire eventi rari e inattesi assicurando la continuità di reti e sistemi per quei servizi che sono essenziali alla sicurezza ed alla stabilità del Paese.

Analisi delle vulnerabilità

Gli attacchi *cyber* minano la fiducia degli internauti nelle tecnologie ICT e la *business continuity* sfruttando vulnerabilità sia organizzative, sia di processo, sia tecniche, spesso in combinazione tra loro.

Le vulnerabilità organizzative e di processo sono riconducibili non solo alla mancata implementazione di misure per garantire la protezione da *malware* – attraverso, ad esempio, l'adozione di *best-practices* e di applicativi anti-virus e anti-spam aggiornati – ma anche all'assenza o alla non corretta attuazione di misure di sicurezza fisica che contemplino, ad esempio, la continuità del servizio e minimizzino l'impatto di eventi, anche naturali, dannosi sull'infrastruttura fisica.

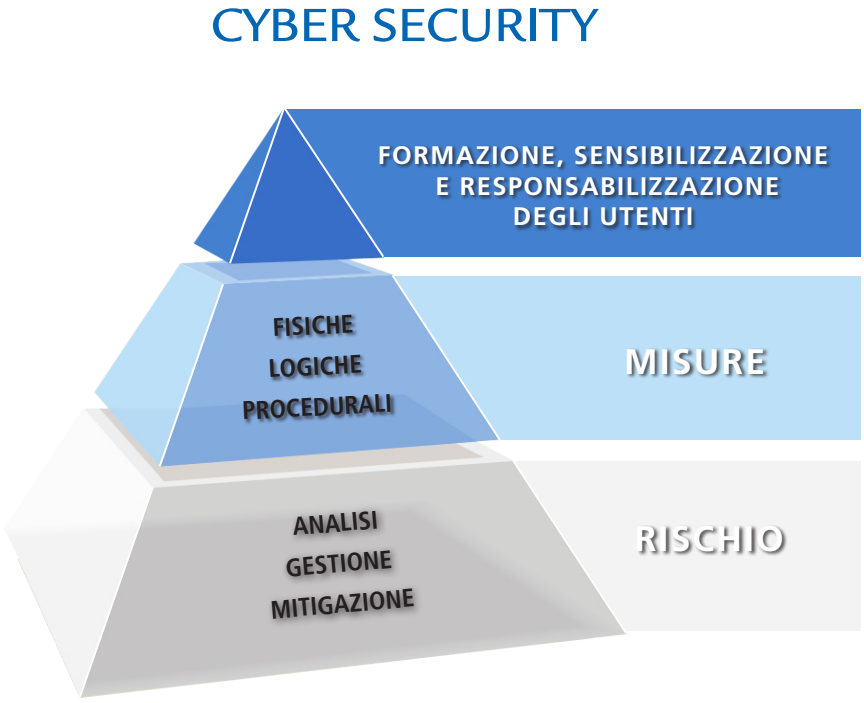
Le vulnerabilità tecniche, invece, sono dovute a falle di sicurezza del software applicativo, ovvero dei protocolli di comunicazione. Tra queste ultime, particolare rilievo assumono quelle che interessano il *Domain Name System* (DNS), il cui sfruttamento può avere ripercussioni sia sugli utenti che usufruiscono dei servizi di comunicazione elettronica sia sui gestori di infrastrutture critiche informatizzate. Tali vulnerabilità possono portare ad una indisponibilità del servizio ovvero possono avere effetti sull'integrità delle informazioni restituite dal *server* dei nomi di dominio. In entrambi i casi lo sfruttamento di tali vulnerabilità può determinare conseguenze estremamente serie in quanto l'impatto determinato dall'impossibilità di raggiungere un fondamentale nodo di controllo dell'infrastruttura potrebbe determinare un grave malfunzionamento della stessa.

Ne deriva, quindi, l'esigenza di limitare le sunnotate vulnerabilità, innanzitutto

attraverso un adeguato piano di prevenzione che faccia dell'analisi del rischio e della gestione e mitigazione del medesimo le fondamenta di una serie di misure di sicurezza fisica, logica e procedurale, che non possono prescindere da un'adeguata formazione, sensibilizzazione e responsabilizzazione del personale nell'adozione e nell'osservanza di tali misure.

Tali misure, funzionali ad una politica di sicurezza delle informazioni, si basano, in linea di principio, su:

- controllo degli accessi al fine di circoscrivere gli stessi al solo personale autorizzato e tracciabilità degli spostamenti dello stesso all'interno dell'ambiente di lavoro in modo da proteggere gli apparati da danneggiamenti, manomissioni o furti (misure di tipo fisico);
- impiego di prodotti certificati per ovviare al problema degli approvvigionamenti di prodotti e servizi tecnologici da fornitori esteri "a rischio", *software* antivirus aggiornato, sistemi di cifratura e di firma digitale, identificazione e autenticazione degli utenti, monitoraggio e tracciabilità degli accessi e delle funzioni svolte in rete da ciascun utente (misure di tipo logico);
- norme e procedure dirette a disciplinare gli aspetti organizzativi del processo della sicurezza, definizione di ruoli, compiti e responsabilità per la gestione di tutte le fasi del processo di sicurezza, adozione di specifiche procedure che completino e rafforzino le contromisure tecnologiche adottate, controlli sulla consistenza e sull'affidabilità degli apparati (misure di tipo procedurale).



CAPITOLO 2

STRUMENTI E PROCEDURE PER POTENZIARE LE CAPACITÀ CIBERNETICHE DEL PAESE

Indirizzi strategici

Al fine di garantire al Paese i benefici sociali ed economici derivanti da uno spazio cibernetico sicuro ed allo scopo di rafforzare le capacità nazionali di prevenzione, reazione e ripristino, il presente Quadro Strategico fissa gli **indirizzi strategici** che dovranno essere conseguiti attraverso uno sforzo nazionale che veda agire, in maniera sinergica e nell'ambito delle rispettive competenze, tutti gli attori che il DPCM 24 gennaio 2013 individua come nodi primari dell'architettura nazionale *cyber,* con un ruolo di raccordo e impulso del CISR. Essi sono così riassumibili:

1. **miglioramento, secondo un approccio integrato, delle capacità tecnologiche, operative e di analisi degli attori istituzionali interessati** per consentire agli stessi la messa a punto di azioni idonee ad analizzare, prevenire, mitigare e contrastare efficacemente i rischi di una minaccia multi-dimensionale;

2. **potenziamento delle capacità di difesa delle Infrastrutture Critiche nazionali e degli attori di rilevanza strategica per il sistema-Paese** assicurando la *business continuity* e, al contempo, la *compliance* con *standard* e protocolli di sicurezza internazionali;

3. **incentivazione della cooperazione tra istituzioni ed imprese nazionali** al fine di tutelare la proprietà intellettuale e di preservare le capacità di innovazione tecnologica del Paese;

4. **promozione e diffusione della cultura della sicurezza cibernetica** sia tra i cittadini che all'interno delle istituzioni, anche attraverso un sempre maggiore coinvolgimento del mondo della ricerca e delle università, al fine di accrescere il livello di consapevolezza e di conoscenza della minaccia e dei relativi rischi;

5. **rafforzamento delle capacità di contrasto alla diffusione di attività e contenuti illegali *on-line*** affinché siano rispettate le normative nazionali e internazionali;

6. **rafforzamento della cooperazione internazionale in materia di sicurezza cibernetica** nell'ambito delle Organizzazioni di cui l'Italia è membro e con i Paesi alleati;

Al fine di conseguire tali sei indirizzi strategici sono stati identificati 11 indirizzi operativi.

Indirizzi operativi

Sviluppo delle capacità del Sistema di informazione per la sicurezza della Repubblica, delle Forze di Polizia, delle Forze Armate e delle Autorità preposte alla Protezione ed alla Difesa Civile ai fini di una efficace prevenzione, identificazione, repressione, reazione, contrasto, neutralizzazione e mitigazione degli eventi nello spazio cibernetico, delle cause e degli effetti che questi hanno in particolare sui sistemi di comunicazione ed informazione e, di conseguenza, sulla società civile e sui beni e servizi a questa forniti.

Incremento delle capacità di monitoraggio e analisi preventiva al fine di anticipare le potenzialità e i rischi connessi alle innovazioni tecnologiche.

Sviluppo delle capacità di pianificazione e condotta delle operazioni militari nello spazio cibernetico.

Identificazione di un'Autorità nazionale NIS (*Network and Information Security*) che cooperi con le omologhe Autorità degli altri Paesi membri della UE e con la Commissione Europea, anche tramite la condivisione di informazioni, per contrastare rischi e incidenti relativi a reti e sistemi.

Potenziamento delle *partnership* pubblico-privato anche per realizzare un continuo, affidabile e sicuro scambio di informazioni tramite il quale gli operatori privati possano fornire informazioni sugli attacchi subìti e su anomalie registrate e ricevere, a loro volta, *assessment* sui rischi e sulle vulnerabilità sulla cui base, poi, adeguare i livelli di sicurezza.

La *partnership* pubblico-privato dovrà essere agevolata anche attraverso:

- la creazione di tavoli istituzionali congiunti con operatori del settore, nell'ambito dei quali la sicurezza dei sistemi informativi e delle reti di comunicazione dovrà prescindere da logiche concorrenziali;
- l'organizzazione di periodiche esercitazioni a livello nazionale che coinvolgano, accanto ai diversi attori pubblici, specifici operatori privati;
- l'obbligatorietà della segnalazione di incidenti informatici nei settori strategici alle Autorità competenti;
- la definizione di procedure operative e *template* per lo scambio informativo.

Scambio di esperienze tra privato e pubblico, allo scopo di implementare la reciproca conoscenza, anche attraverso l'istituzione di periodi formativi del personale interessato presso singole strutture aziendali o presso le Amministrazioni chiamate a tutelarne la sicurezza.

Definizione di un linguaggio di riferimento unico, chiaro e condiviso – da impiegare nei vari ambiti di applicazione – al fine di potenziare l'interoperabilità interministeriale e internazionale.

Predisposizione di questionari atti ad individuare il livello di competenza e consapevolezza (*security awareness*) di tutti gli attori coinvolti nella sicurezza cibernetica nazionale, al fine di individuare punti di forza e di debolezza e di predisporre, laddove necessario, adeguati interventi formativi e di sensibilizzazione.

Realizzazione di campagne di formazione, addestramento, informazione e sensibilizzazione a beneficio del personale della Pubblica Amministrazione, di quello delle imprese e della cittadinanza sulla minaccia, attuale e potenziale, sui rischi ad essa connessi e sull'impiego responsabile delle ICT.

Miglioramento e sperimentazione di attività formative e addestrative al fine di validare le attività cibernetiche di competenza dei vari attori con strumenti di simulazione, addestramento e *training on the job*, accentrando tali funzioni nei poli formativi e specialistici esistenti all'interno della Pubblica Amministrazione (quali, ad esempio, quelli delle F.A.), per evitare fenomeni come quello degli "*insider* inconsapevoli" e mitigare fattori di vulnerabilità come quelli legati a modelli organizzativi BYOD.

Introduzione di moduli di formazione nelle scuole di ogni grado per promuovere una cultura della sicurezza cibernetica.

Predisposizione, con il contributo della comunità accademico-scientifica, di ipotesi di intervento volte a migliorare gli *standard* ed i livelli di sicurezza dei sistemi e delle reti, identificando anche i necessari supporti di simulazione tecnica distribuita utili allo sviluppo di una capacità di formazione e addestramento collettiva.

Rafforzamento dei rapporti di cooperazione e collaborazione con le Organizzazioni internazionali delle quali l'Italia è parte, con i Paesi alleati e con le Nazioni amiche; partecipazione attiva del Paese alle iniziative e ai *fora* internazionali di trattazione della materia al fine di perseguire:

- *a livello globale*, la definizione di regole comuni e di un quadro di legittimità internazionale;
- *a livello europeo*, la tutela degli interessi vitali, strategici e contingenti dell'UE, dei flussi e degli scambi informatici legati al Mercato Unico; il raggiungimento di una capacità di resilienza cibernetica comune; una drastica riduzione del *cyber crime*; lo sviluppo di una politica di difesa cibernetica e

delle relative capacità operative in armonia con la *Common Security and Defence Policy*; lo sviluppo delle risorse tecnologiche e industriali per la sicurezza cibernetica e la condivisione dei princìpi di cui alla Strategia di sicurezza cibernetica dell'UE, nonché nel rispetto degli impegni assunti in sede di Consiglio d'Europa e OSCE;

- *a livello atlantico*, per preservare l'efficienza e l'interoperabilità dei dispositivi di difesa comune al fine soprattutto di incorporare nel processo di pianificazione della difesa in ambito NATO un'efficace postura contro attacchi cibernetici, a tutela degli interessi vitali, strategici e/o contingenti dello Stato e della NATO;
- *a livello bilaterale*, con quei Paesi di interesse strategico o potenziali destinatari di iniziative multilaterali di assistenza tecnica o *capacity-building*.

Partecipazione alle esercitazioni di *cyber security* organizzate dall'ENISA e dalla NATO al fine di verificare e migliorare l'efficacia degli assetti nazionali anche nell'ambito dei rapporti di cooperazione con altri Paesi.

La partecipazione al dibattito internazionale deve essere proiettata anche ad un efficace posizionamento strategico del relativo comparto industriale italiano.

5

Realizzazione della piena operatività del CERT nazionale (già individuato nell'ambito del Ministero dello Sviluppo Economico ai sensi dell'art. 16 bis del Decreto Legislativo 1 agosto 2003, n. 259) al fine di potenziare gli strumenti di rilevazione e contrasto delle minacce ed i meccanismi di risposta agli incidenti, tramite un sistema sicuro e riservato di condivisione delle informazioni.

Tale struttura definisce un modello di comunicazione condiviso con gli altri CERT ed uno schema di accreditamento al fine di individuare ruoli, domini di competenza e punti di contatto supportando la costruzione di un'adeguata *community* per la sicurezza nazionale.

Sviluppo del CERT nazionale sulla base di un modello cooperativo pubblico-privato finalizzato a supportare cittadini e imprese tramite azioni di sensibilizzazione, di prevenzione e di coordinamento della risposta ad eventi cibernetici su vasta scala.

Attivazione di meccanismi di cooperazione in ambito nazionale e internazionale, individuando nel CERT nazionale le funzioni di collegamento con altri CERT pubblici e privati operanti sul territorio e di interfaccia verso il CERT europeo e verso i CERT di altri Stati.

Sviluppo di una piattaforma di coordinamento tecnico e funzionale tra tutti i CERT esistenti che permet-

ta il flusso informativo necessario all'attività di prevenzione e risposta.

Sviluppo e piena operatività del CERT-PA, quale evoluzione del CERT-SPC previsto dal DPCM recante regole tecniche e di sicurezza SPC dell'1 aprile 2008. Il CERT-PA è il punto di riferimento delle pubbliche amministrazioni attivando l'escalation verso il CERT Nazionale secondo modelli e procedure unitarie. Esso collabora con i CERT della pubblica amministrazione a livello europeo ed internazionale, attraverso scambi informativi e procedure concordate.

Il CERT della Difesa segue le evoluzioni tecnico-funzionali e procedurali del NCIRC e il suo impiego dovrà essere previsto nei piani di operazione.

Garantire, attraverso proposte di intervento normativo ed organizzativo, la continua efficacia delle misure di sicurezza cibernetica adattando la legislazione all'evoluzione della tecnologia e dei suoi nuovi utilizzi.

Individuazione di *standard* per la sicurezza di prodotti e sistemi che implementano protocolli di sicurezza. Introduzione di processi di certificazione di conformità a tali *standard* e, ove necessario, implementazione di nuovi processi di approvvigionamento dei prodotti IT in ambito nazionale garantendo l'interoperabilità internazionale soprattutto con gli alleati della NATO e dell'UE.

Elaborazione ed adozione di norme tecniche che garantiscano la sicurezza delle informazioni (integrità, disponibilità e riservatezza) attraverso l'introduzione di metodologie di progettazione sicura dei prodotti e dei sistemi.

Miglioramento del supporto agli utenti, anche attraverso l'introduzione di opportuni incentivi di mercato al fine di promuovere la sicurezza dei prodotti disponibili.

Cooperazione con il comparto industriale per la definizione di piani per la sicurezza di reti e sistemi nonché per la tutela delle alte tecnologie.

Predisposizione di servizi pubblici di assistenza e collaborazione a supporto, in particolare, delle piccole e medie imprese (PMI).

Creazione di una *supply chain* virtuosa attraverso una metodologia predefinita e con il ricorso a meccanismi di *audit* sui sistemi e sui fornitori per incentivarne la verifica di affidabilità.

Sviluppo, all'interno della Pubblica Amministrazione, di un processo flessibile e celere di acquisizione, validazione, verifica e certificazione dei prodotti in armonia con la rapida evoluzione tecnologica del settore.

Previsione di incentivi volti a stimolare la competitività industriale nazionale e tecnologica in particolare: potenziando le attività di R&S da destinare a settori strategici delle F.A. ed ai centri di eccellenza nazionale per la realizzazione di strumenti ed applicazioni maggiormente resilienti e sicuri, nonché atti a garantire efficaci capacità operative.

Mantenimento di una stretta coerenza tra le comunicazioni strategiche e le attività condotte nell'ambiente cibernetico (che è nel contempo soggetto e oggetto di comunicazioni strategiche) affinché il sistema-Paese abbia maggiori strumenti di prevenzione e risposta agli eventi di tale natura.

Una strategia di dissuasione nei confronti di potenziali avversari o criminali può trovare supporto in una oculata comunicazione istituzionale sulle capacità nazionali di dissuasione e deterrenza nello spazio cibernetico.

Attribuzione, ai settori strategici della P.A. di adeguate risorse umane, finanziarie, tecnologiche e logistiche per il conseguimento degli obiettivi programmatici, a breve e medio termine e, di conseguenza, per un effettivo ed efficace perseguimento degli obiettivi indicati nel Quadro Strategico.

Implementazione di un sistema integrato di *Information Risk Management* nazionale in grado di:

- realizzare una struttura efficace per la prevenzione e la gestione del rischio nazionale;
- identificare ed individuare potenziali rischi di carattere nazionale;
- produrre politiche di riferimento per la gestione del rischio.

La centralità della partnership pubblico-privato (PPP)

Il DPCM 24 gennaio 2013 include tra gli attori dell'architettura nazionale preposta a garantire la protezione cibernetica e la sicurezza informatica nazionale, oltre ai soggetti pubblici, anche gli operatori privati che "forniscono reti pubbliche di comunicazione o servizi di comunicazione elettronica accessibili al pubblico, quelli che gestiscono infrastrutture critiche di rilievo nazionale ed europeo, il cui funzionamento è condizionato dall'operatività di sistemi informatici e telematici".

Ai sensi del citato provvedimento, tali soggetti sono tenuti a:

- comunicare al Nucleo per la Sicurezza Cibernetica (NSC) ogni significativa violazione della sicurezza o dell'integrità dei propri sistemi informatici;
- adottare le best practices e le misure finalizzate a conseguire la sicurezza cibernetica;
- fornire informazioni agli organismi di informazione per la sicurezza, consentendo anche l'accesso alle banche dati d'interesse ai fini della sicurezza cibernetica;
- collaborare alla gestione delle crisi cibernetiche contribuendo al ripristino della funzionalità dei sistemi e delle reti da essi gestiti.

Il partenariato pubblico-privato costituisce, pertanto, un principio imprescindibile per il successo di ogni strategia di sicurezza cibernetica. Nei sistemi economico-istituzionali moderni, infatti, gran parte delle infrastrutture che gestiscono servizi pubblici essenziali e quelle di rilevanza strategica per il sistema-Paese, sono affidate all'iniziativa di operatori economici privati. La necessaria collaborazione con questi ultimi ha dato vita ad appositi accordi finalizzati a rendere ancor più strutturata la cooperazione in tale ambito. Nell'ottica di un suo ulteriore rafforzamento, da conseguire attraverso un processo incrementale, le sinergie da sviluppare dovranno interessare, accanto ai soggetti menzionati, anche altre realtà nazionali che, al di là delle dimensioni, rappresentano segmenti di punta per lo sviluppo scientifico, tecnologico, industriale ed economico del Paese.

ALLEGATO 1

RUOLI E COMPITI DEI SOGGETTI PUBBLICI

Il DPCM del 24 gennaio 2013 ha delineato un assetto istituzionale preposto alla protezione cibernetica ed alla sicurezza informatica, nel quale i diversi attori interessati, sia pubblici sia privati, agiscono in maniera integrata allo scopo di ridurre le vulnerabilità dello spazio cibernetico, identificare le minacce, prevenire i rischi ed accrescere le capacità di risposta a situazioni di crisi.

Al vertice dell'architettura si colloca il **Presidente del Consiglio dei Ministri**, che adotta il Quadro Strategico ed il Piano Nazionale per la sicurezza dello spazio cibernetico, per la cui attuazione emana apposite direttive, supportato in ciò dal **Comitato Interministeriale per la Sicurezza della Repubblica** (CISR), il quale, oltre a elaborare proposte di intervento normativo, approva le linee di indirizzo dirette a favorire la collaborazione pubblico-privati nonché una politica di condivisione delle informazioni e per l'adozione di *best practices* e di misure per la sicurezza cibernetica. La verifica dell'attuazione delle misure previste dal Piano Nazionale per la sicurezza dello spazio cibernetico, quale emanazione del presente Quadro Strategico Nazionale, spetta ad un apposito **"organismo collegiale di coordinamento" (cd. CISR tecnico)**.

A supporto del vertice politico opera il **Comparto *intelligence***, che conduce attività di ricerca informativa, nonché provvede alla formulazione di analisi, valutazioni e previsioni sulla minaccia cibernetica, alla promozione della cultura della sicurezza cibernetica, ed alla trasmissione di informazioni rilevanti al Nucleo per la Sicurezza Cibernetica, oltre che ad altri soggetti – pubblici e privati – interessati all'acquisizione di informazioni.

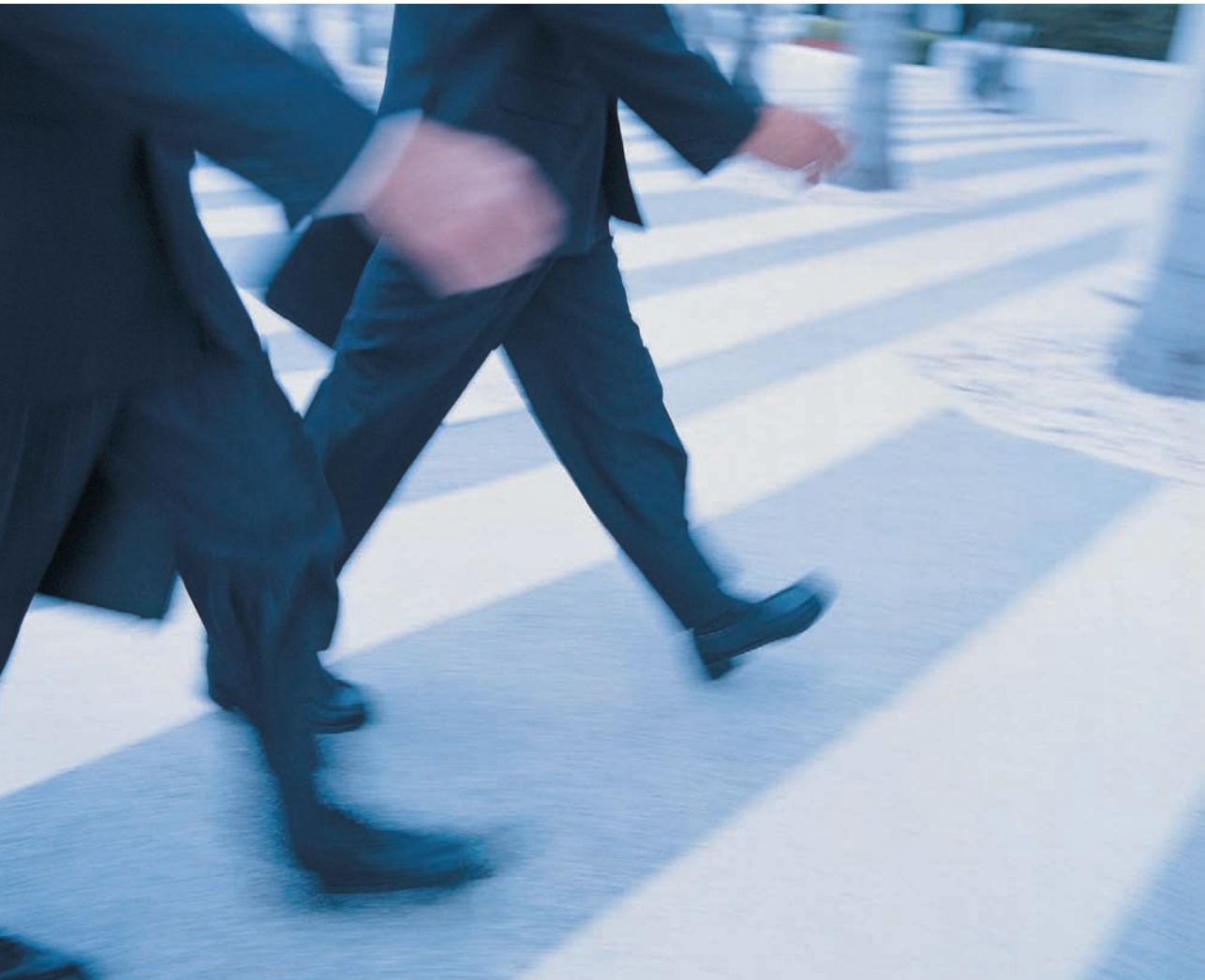
Il **Nucleo per la Sicurezza Cibernetica (NSC)**, istituito nell'ambito dell'Ufficio del Consigliere Militare presso la Presidenza del Consiglio dei Ministri, coordinando, nel rispetto delle rispettive competenze, i diversi attori che compongono l'architettura istituzionale, provvede alla prevenzione e preparazione ad eventuali situazioni

di crisi ed all'attivazione delle procedure di allertamento. Ai fini della *prevenzione e della preparazione ad eventuali situazioni di crisi*, ferma restando, in capo alle distinte Amministrazioni, la responsabilità, la titolarità, la custodia, tutela ed elaborazione dei dati e delle informazioni contenute nelle singole basi di dati e/o archivi telematici, il Nucleo:

- promuove la programmazione e la pianificazione operativa della risposta a situazioni di crisi cibernetica da parte dei soggetti pubblici e degli operatori privati interessati, e l'elaborazione delle procedure di coordinamento interministeriale per la gestione delle crisi;
- mantiene attiva (24/7) un'unità di allertamento e risposta;
- valuta e promuove procedure di condivisione delle informazioni per la diffusione di allarmi e per la gestione delle crisi;
- acquisisce informazioni – anche da operatori privati che forniscono reti pubbliche di comunicazione o servizi di comunicazione elettronica accessibili al pubblico, o che gestiscono infrastrutture critiche di rilievo nazionale ed europeo – in merito ad incidenti significativi concernenti violazioni di sicurezza o perdita dell'integrità. I soggetti privati collaborano attivamente alla gestione delle crisi e contribuiscono al ripristino della funzionalità dei sistemi e delle reti da essi gestiti;

- promuove e coordina lo svolgimento di esercitazioni interministeriali e la partecipazione a quelle internazionali;
- costituisce punto di riferimento nazionale per i rapporti con l'ONU, la NATO, la UE, altre organizzazioni internazionali ed altri Stati.

Ai fini dell'*attivazione delle azioni di risposta e ripristino*, invece, il Nucleo riceve le segnalazioni di evento cibernetico e diramа i relativi allarmi. Laddove l'evento assuma dimensioni, intensità o natura tali da incidere sulla sicurezza nazionale o non possa essere fronteggiato dalle singole amministrazioni competenti, ma richieda l'assunzione di decisioni coordinate in sede interministeriale, dichiara la situazione di crisi cibernetica e attiva il **Nucelo Interministeriale Situazione e Pianificazione** (NISP), quale **"Tavolo interministeriale di crisi cibernetica"**. Esso assicura che le attività di reazione e stabilizzazione di competenza delle diverse Amministrazioni ed enti vengano espletate in maniera coordinata, avvalendosi del ***Computer Emergency Response Team* (CERT) nazionale**, istituito presso il Ministero dello Sviluppo Economico.



RUOLI E COMPITI DEI DIVERSI SOGGETTI PUBBLICI

AGENZIA PER L'ITALIA DIGITALE

Perseguimento degli obiettivi definiti dall'Agenda Digitale Italiana attraverso il monitoraggio dei piani di ICT delle pubbliche amministrazioni e la promozione annuale di nuovi, in linea con l'Agenda digitale europea.

- Svolge attività di progettazione e coordinamento delle iniziative strategiche per la più efficace erogazione di servizi in rete della P.A. a cittadini ed imprese;
- detta indirizzi, regole tecniche e linee guida in materia di sicurezza informatica e di omogeneità dei linguaggi, delle procedure e degli *standard*, anche di tipo aperto, in modo da assicurare, tra l'altro, la piena interoperabilità e cooperazione applicativa tra i sistemi informatici della P.A. e tra questi e i sistemi dell'Unione Europea (D.L. 22 giugno 2012, n. 83, art. 20 co. 3 lit b);
- assicura la qualità tecnica e la sicurezza dei sistemi informativi pubblici e della loro rete di interconnessione per salvaguardare il patrimonio informativo della PA e garantire integrità, disponibilità e riservatezza dei servizi erogati ai cittadini, con livelli di servizio omogenei sul territorio nazionale, provvedendo anche alla loro piena integrazione a livello europeo. In particolare l'attività è riferita alle basi di dati di interesse nazionale, segnatamente a quelle identificate come critiche (art. 2-bis del D.L. 179/2012 come modificato dalla legge di conversione L. 221/2012);
- opera il CERT-SPC, CERT del Sistema Pubblico di Connettività, attuandone la trasformazione in CERT-PA, CERT della Pubblica Amministrazione, che garantisce la sicurezza cibernetica dei sistemi informativi della P.A., oltre che della loro rete di interconnessione, provvedendo al coordinamento delle strutture di gestione della sicurezza ICT – ULS, SOC e CERT, operanti negli ambiti di competenza. Il CERT-PA coopera con il CERT Nazionale e con

il CERT Difesa per il raggiungimento degli obiettivi di sicurezza nazionale;

- funge da snodo per incrementare la partecipazione italiana ai programmi europei e nazionali finalizzati allo sviluppo della società dell'informazione;
- segue i processi di informatizzazione dei documenti amministrativi, vigila sulla qualità dei servizi e sulla razionalizzazione della spesa in materia informatica, contribuisce alla diffusione dell'utilizzo delle tecnologie dell'informazione e della comunicazione allo scopo di favorire l'innovazione e la crescita economica, anche mediante l'accelerazione della diffusione delle Reti di nuova generazione;
- cura la promozione e diffusione delle iniziative di alfabetizzazione informatica mediante tecnologie didattiche innovative rivolte ai cittadini, ai dipendenti pubblici, anche mediante intese con la Scuola Superiore della P.A. e il Formez.

PRESIDENZA DEL CONSIGLIO DEI MINISTRI

DIS, AISE, AISI

Attività informativa finalizzata a rafforzare la protezione cibernetica e la sicurezza informatica nazionali.

- Il DIS e le Agenzie svolgono la propria attività nel campo della sicurezza cibernetica avvalendosi degli strumenti e secondo le modalità e le procedure stabilite dalla legge n. 124/2007, così come modificata dalla legge 133/2012. A tal fine, il Direttore Generale del DIS, sulla base delle direttive adottate dal Presidente del Consiglio dei Ministri – volte a rafforzare le attività di informazione per la protezione delle infrastrutture critiche (materiali e immateriali), con particolare riguardo alla protezione cibernetica e alla sicurezza informatica nazionali – e alla luce degli indirizzi generali e degli obiettivi fondamentali individuati dal CISR, cura il coordinamento delle attività di ricerca informativa finalizzate a rafforzare la protezione cibernetica e la sicurezza informatica nazionali;

- il DIS, attraverso i propri uffici:
  - assicura il supporto al Direttore generale per l'espletamento delle attività di coordinamento;
  - provvede, sulla base delle informazioni, analisi e rapporti provenienti dai servizi di informazione per la sicurezza, dalle F.A. e FF.PP., dalle amministrazioni dello Stato e da enti di ricerca anche privati, e alla luce delle acquisizioni provenienti dallo scambio informativo tra l'AISE, l'AISI e le FF.PP., e dei dati acquisiti da pubbliche amministrazioni e dai soggetti erogatori di servizi di pubblica utilità, alla formulazione di analisi, valutazioni e previsioni sulla minaccia cibernetica;
  - provvede, in base a quanto disposto dal DPCM 24 gennaio 2013, alla trasmissione di informazioni rilevanti ai fini della sicurezza cibernetica al Nucleo per la sicurezza cibernetica, alle pubbliche amministrazioni e agli altri soggetti, anche privati, interessati all'acquisizione di informazioni per la sicurezza;
  - definisce, in base a quanto disposto dal DPCM 22 luglio 2011, le misure di sicurezza cibernetica che devono essere adottate a protezione dei sistemi e delle infrastrutture informatiche che trattano informazioni classificate o coperte

dal segreto di Stato, provvedendo alle relative omologazioni tecniche e valutando le eventuali violazioni di sicurezza o compromissioni di informazioni classificate conseguenti ad eventi accidentali o intenzionali;

- le Agenzie, ciascuna nell'ambito delle rispettive attribuzioni, svolgono, secondo gli indirizzi definiti dalle direttive del Presidente del Consiglio dei Ministri e le linee di coordinamento delle attività di ricerca informativa stabilite dal Direttore Generale del DIS, le attività di ricerca e di elaborazione informativa rivolte alla protezione cibernetica e alla sicurezza informatica nazionali;
- il DIS e le Agenzie corrispondono con le pubbliche amministrazioni, i soggetti erogatori di servizi di pubblica utilità, le università e con gli enti di ricerca, stipulando a tal fine apposite convenzioni. Per le stesse finalità, le pubbliche amministrazioni ed i soggetti erogatori di servizi di pubblica utilità consentono l'accesso del DIS e delle Agenzie ai propri archivi informatici secondo le modalità e con le procedure previste dal DPCM n. 4/2009;
- il DIS pone in essere ogni iniziativa volta a promuovere e diffondere la conoscenza e la consapevolezza in merito ai rischi derivanti dalla minaccia cibernetica e sulle misure necessarie a prevenirli, anche sulla base delle indicazioni del comitato scientifico;
- il DIS redige il documento di sicurezza nazionale concernente le attività relative alla protezione delle infrastrutture critiche, materiali e immateriali, nonché alla protezione cibernetica e alla sicurezza informatica, da allegare alla relazione annuale al Parlamento sulla politica dell'informazione per la sicurezza.

MINISTERO DEGLI AFFARI ESTERI

Rappresenta nei massimi consessi politici multilaterali e internazionali la posizione nazionale.

- Assicura coerenza alla promozione e tutela degli interessi italiani in materia nelle sedi e ai vari livelli internazionali di trattazione;
- coordina la partecipazione e l'impegno italiano, ivi incluso il contributo del settore privato e dell'accademia, presso i diversi *fora* multilaterali di trattazione della materia;
- negozia, in concorso con gli altri organi nazionali competenti, le intese e gli accordi internazionali di disciplina della materia, verificandone la compatibilità e l'opportunità rispetto alle linee strategiche di proiezione internazionale del Paese negli specifici *volet* di declinazione (politiche di sicurezza, tutela dei diritti umani e della libertà fondamentali, contrasto alle minacce transnazionali, salvaguardia e sviluppo dei flussi finanziari, economici e commerciali, ecc.);
- collabora al recepimento interno degli obblighi internazionalmente assunti e dei nuovi orientamenti di disciplina della materia in ambito internazionale (*soft law*, CSBM);
- coordina e assicura i servizi e le attività, ivi inclusa l'adeguata sensibilizzazione e formazione del personale, per garantire la protezione, la resilienza e l'efficienza dei sistemi informativi e di comunicazione sicura presso la Farnesina e la Rete diplomatico-consolare;
- partecipa alle *community* di sicurezza del Sistema Pubblico di Connettività (SPC), attraverso la c.d. Unità Locale di Sicurezza (CERT-MAE), ufficialmente accreditata presso il CERT-SPC.

MINISTERO DELL'INTERNO

Autorità nazionale di pubblica sicurezza

Tutela dell'ordine e della sicurezza pubblica, di soccorso pubblico e difesa civile anche a fronte delle minacce che interessano lo spazio cibernetico o da questo promanano con impatto sulla popolazione, sulle istituzioni, sulle imprese e sulla continuità dell'attività del governo.

- Assicura, attraverso il Dipartimento della Pubblica Sicurezza, la prevenzione ed il contrasto dei crimini informatici;
- garantisce, attraverso la Polizia Postale e delle Comunicazioni, l'integrità e la funzionalità della rete informatica, ivi compresa la protezione delle infrastrutture critiche informatizzate (attraverso il Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche - CNAIPIC), la prevenzione ed il contrasto degli attacchi informatici alle strutture di livello strategico per il Paese, la sicurezza e la regolarità dei servizi di telecomunicazione, il contrasto della pedopornografia *online*, nonché il contrasto degli illeciti concernenti i mezzi di pagamento e il diritto d'autore in tutti i casi in cui l'utilizzo distorto dello strumento informatico o delle tecnologie di rete rappresenti il modo esclusivo o assolutamente prevalente di perpetrazione degli stessi;
- concorre alla prevenzione e al contrasto delle attività terroristiche e di agevolazione del terrorismo condotte con mezzi informatici;
- assicura attività di prevenzione e contrasto a fronte dell'ampia tipologia di crimini informatici;
- opera in proiezione preventiva rispetto al crimine informatico attraverso costanti iniziative di sensibilizzazione dei cittadini al tema della sicurezza informatica.

MINISTERO DELLA DIFESA

Difesa dello Stato, missioni per la realizzazione della pace e sicurezza e concorso alla salvaguardia delle libere istituzioni.

- Definisce e coordina la politica militare, la *governanc*e e le capacità militari nell'ambiente cibernetico;
- pianifica, conduce e sostiene operazioni (*Computer Network Operations – CNO*) nello spazio cibernetico atte a prevenire, localizzare, difendere (attivamente e in profondità), contrastare e neutralizzare ogni possibile minaccia e/o azione avversaria cibernetica, portata alla reti, ai sistemi ed ai servizi della Difesa sul territorio nazionale o nei teatri operativi fuori dai confini nazionali, nel quadro della propria missione istituzionale. In tale quadro, la Difesa negozia le intese e gli accordi internazionali di disciplina della materia, coordina le proprie attività nel settore *cyber*-militare con NATO, EU e le Difese di altri Paesi amici e alleati;
- contribuisce al flusso informativo a supporto delle operazioni cibernetiche delle F.A. oltre i confini nazionali ai sensi della legge 3 agosto 2007, n.124 e successive modifiche;
- concorre alla prevenzione e al contrasto delle attività terroristiche e di agevolazione al terrorismo condotte con mezzi informatici contro le F.A. in campo nazionale o in operazioni fuori dai confini nazionali ai sensi della legge 3 agosto 2007, n. 124 e successive modifiche;
- assicura tutti quei servizi e quelle attività necessari a garantire la protezione, la resilienza e l'efficienza del Sistema Militare e concorre alle attività di reazione e stabilizzazione rispetto a situazioni di crisi di natura cibernetica nazionale attraverso collegamenti funzionali e tecnici del CERT Difesa con il CERT Nazionale ed il CIRC della NATO;
- concorre alla prevenzione e al contrasto degli attacchi ai sistemi di comunicazione e informazione di rilevanza strategica per gli interessi nazionali;
- assicura la formazione e l'addestramento del proprio personale e mette a disposizione i propri centri di formazione in favore delle altre Amministrazioni.

MINISTERO DELL'ECONOMIA E DELLE FINANZE

Tutela il risparmio nazionale nella sua accezione più ampia (dalle regolamentazione dei mercati finanziari alle società partecipate), essa gestisce inoltre l'accertamento e riscossione dei tributi, ed in questo ambito l'Anagrafe tributaria.

- Il MEF, nel suo complesso e per il tramite dei propri Dipartimenti, Agenzie Fiscali e della Guardia di Finanza, è responsabile di numerose Infrastrutture Critiche Informatizzate Nazionali ed è dotato di una complessa organizzazione di sicurezza;
- partecipa attivamente alle *community* di sicurezza del Sistema Pubblico di Connettività (SPC), attraverso le c.d. Unità Locali di Sicurezza, ULS MEF/Sogei e ULS DF/Sogei, ufficialmente accreditate presso il CERT-SPC, che curano il coordinamento delle attività di prevenzione e gestione degli incidenti nell'ambito del SPC;
- in ambito MEF sono operativi enti e strutture organizzative all'interno delle quali operano unità preposte a garantire la sicurezza informatica delle proprie reti e sistemi, ovvero a svolgere compiti di prevenzione e repressione delle frodi di carattere economico/finanziario realizzate attraverso le reti telematiche e le tecnologie informatiche (Guardia di Finanza).

MINISTERO DELLO SVILUPPO ECONOMICO

Dipartimento per le Comunicazioni

Promuove, sviluppa e disciplina il settore delle comunicazioni elettroniche.

- È l'Autorità nazionale di regolamentazione in materia di sicurezza ed integrità delle reti di comunicazione elettronica, ai sensi dell'art. 16 bis del d.lvo n. 259 del 2003, relazionandosi su tali materie con organismi nazionali ed internazionali;
- ai sensi del predetto decreto:
  - individua le misure di natura tecnico-organizzativa di sicurezza e integrità delle reti e verifica il rispetto delle stesse da parte degli operatori di rete e fornitori di servizi di comunicazioni elettroniche;
  - riceve dagli operatori di reti e fornitori di servizi le segnalazioni relative ad incidenti con impatto significativo per il successivo inoltro alla Commissione Europea e all'Agenzia ENISA;
  - svolge le funzioni di CERT nazionale;
  - rappresenta, per il tramite del Direttore dell'Istituto Superiore delle Comunicazioni e delle tecnologie dell'informazione, il Paese nell'ambito della Agenzia europea per la sicurezza delle reti e dell'informazione (ENISA);
- l'ISCOM:
  - è l'Organismo di Certificazione della Sicurezza Informatica (OCSI);
  - partecipa alle iniziative coordinate dall'Agenzia ENISA in materia di protezione delle infrastrutture critiche informatizzate;
  - partecipa ai lavori in diversi contesti internazionali ed europei in materia di *Internet Governance;*
  - effettua la vigilanza nell'ambito del Registro Italiano ccTLD"it";
  - è coinvolto nel programma comunitario *safer* internet;
  - svolge attività di ricerca in collaborazione con Enti di ricerca ed Università nei diversi settori delle comunicazioni elettroniche al fine di individuare azioni concrete per l'attuazione degli obiettivi perseguiti dall'Agenda Digitale Europea;

- l'Osservatorio Permanente per la Sicurezza e la Tutela delle Reti e delle Comunicazioni – presieduto dal Capo del Dipartimento per le Comunicazioni – cura la formazione della cultura della sicurezza, la redazione del repertorio delle prestazioni obbligatorie che gli *Internet Service Providers* (ISPs) devono mettere a disposizione dell'AG, la promozione dell'accesso ad Internet, ecc.

ALLEGATO 2

GLOSSARIO

AGCOM – Autorità per le Garanzie nelle Comunicazioni
Autorità indipendente istituita dalla legge 249 del 1997, avente il duplice compito di assicurare, da un lato, la corretta competizione degli operatori sul mercato e, dall'altro, di tutelare i consumi e le liberta fondamentali dei cittadini.

APT – Advanced Persistent Threat
Minaccia consistente in un attacco mirato, volto ad installare una serie di *malware* all'interno delle reti del bersaglio al fine di riuscire a mantenere attivi dei canali che servono a far uscire informazioni di valore dalle reti dell'ente obiettivo.

BYOD – Bring Your Own Device
Politica che permette ai dipendenti di un'azienda di portare i propri dispositivi mobili (pc portatili, smartphone e tablet) sul posto di lavoro e di impiegarli per accedere ad informazioni e ad applicazioni aziendali come, ad esempio, la posta elettronica.

***cc*TLD – Country Code Top Level Domain**
Ultima parte del nome di dominio Internet usato da uno Stato. È costituito da due lettere: ".it" per l'Italia.

CERT – Computer Emergency Response Team
Organizzazione con compiti di prevenzione e di coordinamento della risposta ad eventi cibernetici. Diversi CERT svolgono anche funzioni di formazione ed informazione nei confronti degli utenti.

CERT-PA – *Computer Emergency Response Team* – Pubblica Amministrazione
Evoluzione del CERT-SPC (cfr. voce successiva) con competenza estesa ai sistemi informativi della Pubblica Amministrazione ed ai servizi erogati per il loro tramite, oltre che alla rete di interconnessione. Esso ha il compito di supportare e coordinare la PA nella prevenzione, risposta e rientro dagli incidenti.

CERT-SPC – Computer Emergency Response Team - Sistema Pubblico di Connettività
Struttura responsabile, a livello nazionale, per la prevenzione, il monitoraggio, il coordinamento informativo e l'analisi degli incidenti di sicurezza in ambito SPC. Essa ha anche il compito di assicurare l'applicazione di metodologie coerenti ed uniformi per la gestione degli incidenti informatici. Il CERT-SPC è referente delle Unità Locali di Sicurezza (ULS) istituite per ogni dominio connesso al SPC.

CNA – Computer Network Attack
Attività condotte nel e attraverso il *cyber*-spazio allo scopo di manipolare, interrompere il flusso, negare, degradare o distruggere le informazioni presenti nei computer o nelle reti di computer, ovvero gli stessi computer o reti di computer.

CNAIPIC – Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche
Il CNAIPIC, previsto dalla legge 155 del 2005 ed istituito con Decreto del Ministro dell'Interno del 9 febbraio 2008, è costituito in seno al Servizio di Polizia Postale e delle Comunicazioni, organo per la sicurezza e per l'integrità dei servizi di telecomunicazione del Ministero dell'Interno, Autorità Nazionale di Pubblica Sicurezza. Il centro, per espressa previsione normativa, ha il compito di garantire la prevenzione e la repressione dei crimini informatici rivolti verso le infrastrutture critiche o di rilevanza nazionale, anche attraverso rapporti di *partnership* definiti in apposite convenzioni con i responsabili delle strutture interessate.

CND – Computer Network Defence
Azioni intraprese con l'uso di reti di computer per proteggere, monitorare, analizzare, rilevare e contrastare le attività non autorizzate condotte verso sistemi informatici e reti di computer.

CNE – Computer Network Exploitation
Operazioni condotte nel *cyber*-spazio al fine di acquisire informazioni da sistemi informatici o reti *target* o avversarie. Trattasi di attività di *intelligence* o di attività prodromica ad un attacco *cyber*.

CNO – Computer Network *Operations*
Con tale termine si identificano genericamente attività di Computer Network Attack (CNA), Computer Network Defence (CND) e Computer Network Exploitation (CNE).

CPS – Cyber Physical System
Sistema informatico che gestisce e controlla entità fisiche in settori quali le infrastrutture civili, il settore aerospaziale, dei trasporti, sanitario, energetico e dei processi produttivi.

CSBM – Confidence and Security Building Measures
Misure volte a prevenire o a risolvere ostilità fra Stati e ad evitare un loro inasprimento, tramite lo sviluppo della fiducia reciproca. Tali misure possono avere natura formale o informale, unilaterale, bilaterale o multilaterale, militare o politica.

DoS – Denial of Service
Attacco volto a rendere un sistema informatico o una risorsa non disponibile ai legittimi utenti attraverso la saturazione delle risorse ed il sovraccarico delle connessioni di rete dei sistemi server.

DDoS – Distributed Denial of Service
Attacco DoS lanciato da un gran numero di sistemi compromessi ed infetti (BotNet).

DF – Digital Forensics
Disciplina – anche detta computer forensics o informatica forense – che si occupa dell'identificazione, della conservazione, dell'analisi e della documentazione dei reperti informatici al fine di presentare valide prove digitali in sede processuale sia civile che penale.

DNS – Domain Name System
Sistema di denominazione del dominio consistente in un database distribuito che converte in automatico un indirizzo web in un codice numerico di protocollo Internet (indirizzo IP) che identifica il server web che ospita il sito.

ENISA – European Network and Information Security Agency
Agenzia dell'Unione Europea volta a garantire un elevato livello di sicurezza delle reti e dell'informazione attraverso pareri tecnici alle autorità nazionali e alle istituzioni dell'UE, lo scambio di buone pratiche, lo sviluppo dei contatti tra le istituzioni comunitarie, le autorità nazionali e le imprese, e la promozione di una cultura della sicurezza.

Exploit
Codice che sfrutta un bug o una vulnerabilità di un sistema informatico.

IC – Infrastrutture Critiche
Infrastruttura, ubicata in uno Stato membro dell'Unione Europea, che è essenziale per il mantenimento delle funzioni vitali della società, della salute, della sicurezza e del benessere economico e sociale della popolazione ed il cui danneggiamento o la cui distruzione avrebbe un impatto significativo in quello Stato, a causa dell'impossibilità di mantenere tali funzioni (art. 2 lit. b) Direttiva 2008/114/CE);

ICE – Infrastrutture Critiche Europee
Infrastruttura critica ubicata negli Stati membri dell'UE il cui danneggiamento o la cui distruzione avrebbe un significativo impatto su almeno due Stati membri. La rilevanza di tale impatto è valutata in termini intersettoriali. Sono compresi gli effetti derivanti da dipendenze intersettoriali in relazione ad altri tipi di infrastrutture (art. 2 lit. e) Direttiva 2008/114/CE).

Ingegneria sociale
Arte di manipolare psicologicamente le persone affinché compiano determinate azioni o rivelino informazioni confidenziali, come le credenziali di accesso a sistemi informatici.

IoE – Internet of Everything
Rete in cui persone, oggetti, dati e processi sono connessi tra loro attraverso Internet, e nella quale le informazioni vengono trasformate in tempo reale in azioni, creando così nuove e ad oggi inimmaginabili opportunità di *business*.

IoT – Internet of Things

Neologismo riferito all'estensione di Internet al mondo degli oggetti, i quali si rendono riconoscibili e acquisiscono intelligenza grazie al fatto di poter comunicare dati su se stessi e accedere ad informazioni aggregate da parte di altri. L'obiettivo è di far sì che il mondo elettronico tracci una mappa di quello reale, dando un'identità elettronica alle cose e ai luoghi dell'ambiente fisico. I campi di applicabilità sono molteplici: dalle applicazioni industriali (processi produttivi), alla logistica e all'infomobilità, fino all'efficienza energetica, all'assistenza remota e alla tutela ambientale.

ISP – Internet Service Provider

Società che offre connessione e servizi Internet a pagamento tramite linea telefonica quali connessioni Dialup e ISDN oppure a banda larga come fibre ottiche o DSL.

Malware

Contrazione di *malicious software*. Programma inserito in un sistema informatico, generalmente in modo clandestino, con l'intenzione di compromettere la riservatezza, l'integrità o la disponibilità dei dati, delle applicazioni o dei sistemi operativi dell'obiettivo. A tale categoria generica appartengono in via esemplificativa: virus, worm, trojan horse, backdoor, spyware, dialer, hijacker, rootkit, scareware, rabbit, keylogger, bombe logiche, ecc.

Phishing

Attacco informatico avente, generalmente, l'obiettivo di carpire informazioni sensibili (userid, password, numeri di carte di credito, PIN) con l'invio di false e-mail generiche a un gran numero di indirizzi. Le e-mail sono congegnate per convincere i destinatari ad aprire un allegato o ad accedere a siti web falsi. Il phisher utilizza i dati acquisiti per acquistare beni, trasferire somme di denaro o anche solo come "ponte" per ulteriori attacchi.

Reverse engineering

Analisi volta a comprendere il funzionamento di prodotti *hardware* e *software* al fine di reingegnerizzarli, ad esempio, per migliorarne il funzionamento o per impiegarli per fini diversi e ulteriori rispetto a quelli originari.

SCADA – Supervisory Control and Data Acquisition

Sistemi impiegati per il monitoraggio ed il controllo di impianti e dispositivi in settori quali il controllo del traffico (aereo, ferroviario, automobilistico), della gestione dei sistemi di trasporto dei fluidi (acquedotti, gasdotti, oleodotti, ecc.), della distribuzione dell'energia elettrica, della gestione delle linee di produzione che realizzano i processi industriali, e del telerilevamento ambientale.

SOC – Security Operations Center

Centro che fornisce servizi finalizzati alla sicurezza dei sistemi informativi di un'azienda (SOC interno) o di clienti esterni. Un SOC può anche fornire servizi di *incident response*: in questo caso svolge la funzione di *Computer Security Incident Response Team* (CSIRT), anche se spesso tale funzione fa capo ad un organo separato dell'azienda.

TCP/IP – Transmission Control Protocol/Internet Protocol
Insieme di *standard* di protocolli sviluppato nella seconda metà degli anni '70 dalla *Defence Advanced Research Project Agency* (DARPA), al fine di consentire la comunicazione tra diversi tipi di computer e reti di computer. Il TCP/IP è, infatti, impiegato da Internet.

UTM – Unified Threat Management
Prodotto di sicurezza integrato a protezione da minacce multiple, composto da un *firewall*, *software* antivirus, e sistemi di filtraggio spam e dei contenuti.

Web defacement
Attacco condotto contro un sito web e consistente nel modificare i contenuti dello stesso limitatamente alla *home-page* ovvero includendo anche le sottopagine del sito.

Il Presidente del Consiglio dei Ministri

N.0012956/2.1.1.(36) GAB.UGLG
del 30/01/2014 D002 I

VISTA la legge 3 agosto 2007, n. 124, recante "Sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto", come modificata e integrata dalla legge 7 agosto 2012, n. 133, e, in particolare, l'art. 1, comma 3-*bis*;

VISTO il decreto del Presidente del Consiglio dei ministri del 24 gennaio 2013, recante "Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale" e, in particolare, gli artt. 3 e 4;

VISTA la proposta del Comitato interministeriale per la sicurezza della Repubblica formulata nella seduta del 17 dicembre 2013;

DISPONE

Articolo 1

1. È adottato il Quadro strategico nazionale per la sicurezza dello spazio cibernetico, di cui all'art. 3, comma 1, lett. *a*), della Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale, allegato al presente decreto.

Roma, 27 GEN. 2014

PRESIDENZA DEL CONSIGLIO DEI MINISTRI
SEGRETARIATO GENERALE
UFFICIO DEL BILANCIO E PER IL RISCONTRO
DI REGOLARITA' AMMINISTRATIVO-CONTABILE
VISTO E ANNOTATO AL N. 230/2014
Roma, 4.2.2014
IL REVISORE
IL DIRIGENTE

Reg.to ALLA CORTE DEI CONTI
Addì 7 FEB. 2014
n. 318