quaderni IAI

ISSN 0075-1448

Cybersecurity: Unione europea e Italia Prospettive a confronto

Claudia Cencetti

Edizioni Nuova Cultura

IAI
Istituto Affari Internazionali

Quaderni IAI

Cybersecurity: Unione europea e Italia Prospettive a confronto

di Claudia Cencetti

Edizioni Nuova Cultura

Claudia Cencetti ha partecipato nel corso del 2013/2014 al programma di formazione laureandi nel campo della sicurezza e difesa, avviato dallo IAI nel 1998, e ha preparato questo Quaderno IAI, che rappresenta una rielaborazione della sua tesi di laurea magistrale. L'autrice si è laureata in "Relazioni internazionali e Studi europei" presso la Scuola di Scienze politiche "Cesare Alfieri" dell'Università degli Studi di Firenze.

Quaderni IAI
Direzione: Natalino Ronzitti
Prima edizione agosto 2014 - Edizioni Nuova Cultura

Per Istituto Affari Internazionali (IAI)
Via Angelo Brunetti 9 - I-00186 Roma
www.iai.it

Copyright © 2014 Edizioni Nuova Cultura - Roma
ISBN: 9788868123642
Copertina: Marco Pigliapoco
Composizione grafica: Marco Pigliapoco
È vietata la riproduzione non autorizzata, anche parziale, realizzata con qualsiasi mezzo, compresa la fotocopia, anche ad uso interno o didattico.

Indice

Indice di tabelle, grafici e figure

Lista delle abbreviazioni

ADI	Agenda digitale italiana
AgID	Agenzia per l'Italia digitale
AISE	Agenzia informazione e sicurezza esterna
AISI	Agenzia informazione e sicurezza interna
ANR	Autorità nazionale di regolamentazione
ASEAN	Association of South-East Asian Nations
BEREC	Body of European Regulators for Electronic Communications
CCD COE	Cooperative Cyber Defence Centre of Excellence
CENSec	Centro di eccellenza nazionale sulla cybersecurity
CERT	Computer Emergency Response Team
CERT-Difesa	Computer Emergency Response Team del Ministero della Difesa
CERT-EU	Computer Emergency Response Team of the European Union
CERT-PA	Computer Emergency Response Team della Pubblica Amministrazione
CIIP	Critical Information Infrastructure Protection
CIRC	Computer Incident Response Capability
CIS Sapienza	Cyber Intelligence and Information Security Centre, Sapienza Università di Roma
CISR	Comitato interministeriale per la sicurezza della Repubblica
CNAD	Conference of National Armaments Directors
CNAIPIC	Centro nazionale anticrimine informatico per la protezione delle infrastrutture critiche
CNCPO	Centro nazionale per il contrasto della pedopornografia online

CNET	Communications Networks
CNIPA	Centro nazionale per l'informatica nella Pubblica Amministrazione
COPASIR	Comitato parlamentare per la sicurezza della Repubblica
CoPS	Comitato politico strategico
CSIS	Center for Strategic and International Studies
CWC	Cyber Warfare Conference
DPCM	Decreto del presidente del Consiglio dei ministri
DDoS	Distributed Denial of Service
DG CONNECT	Directorate General for Communications Networks
DigitPA	Ente nazionale per la digitalizzazione della Pubblica Amministrazione
DIS	Dipartimento informazioni per la sicurezza
DNS	Domain Names System
DSCI	Data Security Council of India
EC3	European Cyber Crime Centre
ECI	European Critical Infrastructure
EDA	European Degence Agency
EISAS	European Information Sharing and Alert System
ENISA	European Network and Information Security Agency
EPCIP	European Programme for Critical Infrastructure Protection
Europol	European Police Office
GAT	Gruppo anticrimine tecnologico
GNL	Gas naturale liquefatto
ICANN	International Corporation for Assigned Names and Numbers
ICSPA	International Cyber Security Protection Alliance
ICT	Information and Communications Technology
IIS	Internet Interconnected Site
INFOSEC	Information Security

IP	Internet Protocol
ISCOM	Istituto superiore delle comunicazioni e delle tecnologie dell'informazione
ISMS	Information Security Management System
ISO	International Organization for Standardization
ISP	Internet Service Provider
IT	Information Technology
NBCR	Nuclear, Biological, Chemical and Radiological
NIAG	NATO Industrial Advisory Group
NIS	Network and Information Security
NISP	Nucleo interministeriale di situazione e pianificazione
NPM	Nucleo politico militare
OCSI	Organismo di certificazione della sicurezza informatica
OCSE	Organizzazione per la cooperazione economica e lo sviluppo
ONU	Organizzazione delle Nazioni Unite
OSA	Organizzazione degli Stati americani
OSCE	Organizzazione per la sicurezza e la cooperazione in Europa
PA	Pubblica Amministrazione
PDCA	Plan-Do-Check-Act
PdCM	Presidenza del Consiglio dei ministri
PIC	Protezione infrastrutture critiche
PN	Piano nazionale per la protezione cibernetica e la sicurezza informatica
PPP	Public-Private Partnership
PSDC	Politica di sicurezza e difesa comune
QSN	Quadro strategico nazionale per la sicurezza dello spazio cibernetico
R&S	Ricerca e sviluppo
Ra.C.I.S.	Raggruppamento investigazioni scientifiche
RFI	Rete ferroviaria italiana

SCADA	Supervisory Control and Data Acquisition
SDA	Security & Defence Agenda
SIOI	Società italiana per l'organizzazione internazionale
SIS	Sezioni investigative scientifiche
SOC	Security Operations Center
STELMILIT	Scuola telecomunicazioni Forze Armate di Chiavari
TTC	Tavolo tecnico cyber
UE	Unione europea

Executive Summary

Negli ultimi venti anni, la diffusione delle nuove tecnologie dell'informazione e delle comunicazioni ha progressivamente focalizzato il centro delle attività umane di carattere sociale, politico ed economico all'interno di una nuova dimensione, denominata cibernetica. Lo straordinario aumento dell'utilizzo di internet ha contribuito allo sviluppo del settore ICT, con un notevole impatto su tutte le funzioni della società moderna. Lo spazio cibernetico ha permesso immense opportunità di sviluppo economico, grazie alle quali le economie dei paesi più avanzati hanno subito una forte accelerazione. Tuttavia, l'incremento delle opportunità è stato accompagnato da un parallelo incremento delle vulnerabilità. Infatti, la digitalizzazione dei servizi e delle informazioni ha inevitabilmente accresciuto l'esposizione al rischio: il pericolo di furto, manomissione e compromissione dei dati nello spazio cibernetico ha evidenziato la necessità di mettere in sicurezza le attività in esso condotte.

Il crimine informatico costituisce la piaga maggiore della sicurezza delle reti e delle informazioni, a livello di portata e di danni economici. Il costo del cybercrime è in continua crescita, provocando un ingente trasferimento di risorse al di fuori delle economie nazionali. Inoltre, strutture pubbliche che gestiscono quotidianamente dati ed informazioni digitali riguardanti cittadini si trovano a doverne garantire non solo la disponibilità e l'integrità, ma anche la riservatezza. Anche le aziende private, il cui funzionamento si regge su infrastrutture informatizzate, hanno l'esigenza di assicurare la continuità dei servizi erogati, proteggendoli da possibili eventi di natura cibernetica. Soprattutto, le infrastrutture considerate critiche per la nazione, in quanto fornitrici di servizi essenziali, quali luce, gas, acqua, ecc., hanno il dovere di garantire il normale svolgimento della vita quotidiana dei cittadini. A questo proposito, lo Stato ha un interesse strategico e nello stesso tempo un dovere nel tutelare le proprie infrastrutture critiche, il cui danneggiamento rappresenta sia una perdita economica sia una minaccia alla sicurezza nazionale.

Oggi, il fattore ICT costituisce l'asse portante delle economie di molti paesi ed una risorsa critica sulla quale poggia gran parte del settore

industriale. L'impatto dell'economia digitale sulla vita economica dei paesi necessita delle dovute riflessioni e azioni da parte delle autorità di governo, affinché sia possibile trarne i maggiori benefici e limitarne i potenziali rischi. La protezione dello spazio cibernetico assume una rilevanza notevole, al fine di assicurare la crescita economica e favorire l'uso consapevole e responsabile dei mezzi informatici da parte degli utenti. Soprattutto, tale protezione si rivela essenziale per quanto concerne il contrasto al crimine informatico e la messa in sicurezza delle infrastrutture critiche nazionali informatizzate. Questi due aspetti costituiscono l'ossatura fondamentale delle politiche europee e degli stati membri, in ambito sicurezza cibernetica.

A livello europeo, il panorama si presenta alquanto diversificato. Nel febbraio 2013 l'Unione europea ha adottato la propria strategia di cybersicurezza, invitando tutti gli stati membri a fare altrettanto. Attualmente, sono 16 gli stati europei che hanno provveduto a dotarsi di un simile documento, di cui cinque – Finlandia, Italia, Romania, Spagna e Ungheria – nel 2013. Questo dato è rappresentativo della recente consapevolezza generale della problematica e del ruolo guida dell'UE nel favorire la predisposizione degli strumenti adeguati di sicurezza cibernetica.

In Europa il Regno Unito rappresenta probabilmente la realtà più avanzata dal punto di vista della cybersecurity, anche in seguito alla significativa influenza degli Stati Uniti riguardo ad alcune dinamiche. A partire dai primi anni del 2000, il paese ha gradualmente predisposto un articolato sistema di controllo e gestione del rischio della minaccia cibernetica, attraverso l'individuazione e creazione di organizzazioni specifiche ed unità di risposta alle situazioni di emergenza. Nel 2011, inoltre, il Regno Unito ha istituito un fondo finanziario *ad hoc* per gli obiettivi di cybersecurity, dotato di 650 milioni di sterline per il quadriennio 2011-2014. Recentemente, il programma è stato riconfermato, attraverso la destinazione di ulteriori 210 milioni di sterline per il biennio 2015-2016. Il percorso seguito dal Regno Unito può servire da esempio ed ispirazione per quei paesi che non si sono ancora dotati degli adeguati strumenti di cybersecurity e così contribuire ad individuare *best practices* valide internazionalmente, che l'Unione europea si impegna a promuovere e diffondere.

Nel novero degli stati membri virtuosi rientra anche l'Estonia, che è stata il primo paese europeo a dotarsi di una strategia per la cybersecurity nel 2008. Nel maggio 2007 essa è stata bersaglio di una serie

di attacchi cibernetici su larga scala, per un periodo di alcune settimane, durante le quali sono state interrotte le normali funzioni dei siti internet ufficiali di alcune organizzazioni, tra cui il Parlamento, tali ministeri, alcune testate giornalistiche e determinate banche ed emittenti televisive e radiofoniche. Questi accadimenti hanno inciso sulla decisione delle autorità estoni di elaborare una Strategia nazionale di sicurezza cibernetica. Gli attacchi del 2007 non hanno causato grosse perdite all'Estonia quale sistema paese – anche se, in considerazione dell'alto livello di digitalizzazione del paese, sono state rilevanti – ma hanno contribuito a diffondere una certa consapevolezza tra gli stati europei della necessità di dotarsi degli adeguati sistemi di sicurezza per le proprie reti informatiche, per garantirne la continuazione delle funzioni, anche in caso di attacco. I cyber attack contro l'Estonia hanno suscitato l'attenzione della comunità internazionale, aprendo il dibattito sulla possibilità di conflitti internazionali via mezzi informatici.

Il tema della cyber warfare sta gradualmente acquisendo una notevole importanza ai fini delle logiche di difesa nazionale, considerato che il concetto tradizionale di conflitto tra stati è in continua evoluzione: infatti, oggi, esso ha maggiore probabilità di manifestarsi tramite il furto di informazioni riservate (cyber spionaggio) o la paralisi di infrastrutture critiche nazionali piuttosto che tramite mezzi militari convenzionali. La guerra tradizionale ha sempre meno occasione di verificarsi, in contesti di tensione tra stati avanzati, e le nuove frontiere delle minacce alla sicurezza nazionale attengono sempre più alla dimensione cibernetica. Il caso estone ha portato questa verità all'attenzione degli stati europei, anche se un collegamento diretto tra gli eventi del 2007 e la cyber warfare non è possibile, tanto meno condiviso a livello internazionale.

Per una trattazione dettagliata della relazione tra cyber warfare e diritto internazionale, si rimanda ai testi di Roscini e di Schmitt[1]. Un approfondimento delle strategie nazionali di Regno Unito ed Estonia è disponibile nell'elaborato integrale di tesi di laurea, da cui il presente quaderno è tratto (si veda introduzione).

Rispetto alla media europea, l'Italia ha registrato un ritardo nella predisposizione delle adeguate politiche di cybersecurity, giungendo

[1] Marco Roscini, *Cyber operations and the use of force in International Law*, Oxford , Oxford University Press, 2014. Michael N. Schmitt, *Tallinn Manual on the International Law applicable to Cyber Warfare*, Cambridge, Cambridge University Press, 2013.

all'approvazione di una propria strategia nazionale solo nel dicembre 2013. Ad inaugurare questo anno di crescente interesse per la materia è stato il Decreto del presidente del Consiglio dei ministri (DPCM) del 24 gennaio 2013, *Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica*, che ha definito l'architettura istituzionale deputata alla sicurezza nazionale relativamente alle infrastrutture critiche informatizzate[2]. A dicembre 2013 il *Quadro strategico nazionale per la sicurezza dello spazio cibernetico* ed il relativo *Piano nazionale per la protezione cibernetica e la sicurezza informatica* hanno stabilito gli indirizzi strategici e quelli operativi per la messa in sicurezza delle attività condotte nel cyber spazio.

I documenti del 2013 hanno segnato una svolta nella storia della trattazione italiana della questione della cybersecurity, contribuendo in maniera significativa allo sviluppo in materia. Con essi, sono stati individuati i principali organi di governo incaricati di gestire la sicurezza informatica in Italia ed una Strategia appositamente dedicata. Tuttavia, ad oggi, l'Italia non dispone ancora di un proprio CERT (Computer Emergency Response Team) nazionale, che sia in grado di rilevare le minacce che si originano nel cyber spazio, rispondere agli attacchi informatici e ripristinare le funzioni dei servizi eventualmente compromesse. La realizzazione di una simile struttura consentirebbe anche azioni di coordinamento in materia, attraverso la messa a punto di una rete europea di CERT nazionali, capeggiata dal CERT-EU, attualmente non ancora completata. L'Italia dispone di un CERT-Difesa e di un CERT-PA – quest'ultimo inaugurato nel gennaio 2014 – ma la creazione del CERT nazionale costituisce un'urgente priorità.

I progressi del 2013 hanno introdotto elementi nuovi nel contesto normativo italiano relativo alla sicurezza informatica, delineando una situazione di maggiore consapevolezza dei rischi e delle opportunità derivanti dalla dimensione cibernetica. A questo punto, sarebbe utile consolidare questo impegno nel prossimo futuro, attraverso la predisposizione di un adeguato *framework* legale, che ben si inserisca nei più alti contesti europeo ed internazionale.

Attualmente, gli obiettivi primari di cybersecurity – a livello nazionale, europeo ed internazionale – sono il contenimento del crimine informatico, la protezione delle infrastrutture critiche informatizzate

[2] Decreto del Presidente del Consiglio dei Ministri del 24 gennaio 2013 (G.U. n. 66 del 19 marzo 2013).

e la tutela delle informazioni personali in formato digitale. Il conseguimento di questi obiettivi si basa sull'azione di governo dei singoli stati, in quanto attori principalmente responsabili per la sicurezza e la crescita economica nazionali, ma dipende in modo cruciale anche dalla realizzazione della cooperazione europea ed internazionale e dalla necessaria istituzionalizzazione di partnership pubblico-privato.

Introduzione

Il presente quaderno intende indagare la questione della cybersecurity in Europa che, con crescente importanza, impatta sulla sicurezza e crescita economica degli stati nazionali. Il testo prende in esame i principali sviluppi registrati in materia, all'interno di due realtà distinte, ma tra loro necessariamente collegate: Unione europea e Italia. Entrambi i casi qui oggetto di studio sono strutturati secondo una rassegna delle politiche ed iniziative interne più significative in ambito cyber, che hanno gradualmente portato all'approvazione di una strategia *ad hoc* per la cybersecurity.

L'obiettivo di questo studio è quello di definire la posizione italiana nello scenario europeo, attraverso un'analisi del percorso normativo verso la maturazione della consapevolezza delle nuove esigenze legate alla sicurezza cibernetica. A tal fine, i progressi raggiunti dall'Italia, negli ultimi anni, sono stati valutati a partire dalle linee guida individuate dall'ENISA (European Network and Information Security Agency) nel manuale *National Cyber Security Strategies*[3], pubblicato nel 2012 e rivolto a tutti quegli stati che non si sono ancora dotati degli strumenti necessari per gestire efficacemente la questione della cybersecurity. Sulla base di questo testo, è stato possibile delineare lo stato dell'arte della sicurezza cibernetica in Italia, prima e dopo il 2013, che ha segnato una svolta nella storia della trattazione nazionale di questa materia.

Il lavoro è stato realizzato nell'ambito dell'attività "Formazione laureandi" del Programma Sicurezza e Difesa dell'Istituto affari internazionali e costituisce un estratto dalla tesi di laurea intitolata *Le politiche di cybersecurity nel contesto europeo e italiano. Analisi e confronto di alcuni casi studio*, redatta a conclusione del corso di studi di Relazioni internazionali della Scuola di Scienze politiche "Cesare Alfieri" dell'Università di Firenze. Il testo integrale dell'elaborato di tesi prende in esame, oltre ad UE e Italia, altri due casi nazionali: Regno Unito ed Estonia, selezionati per la loro rilevanza in materia. Questi, infatti, si caratterizzano quali realtà particolarmente avanzate in Europa - a livello normativo, tecno-

[3] ENISA, *National Cyber Security Strategies. Practical Guide on Development and Execution*, December 2012, http://europa.eu/!gC63Tk.

logico ed operativo - che, quindi, possono servire da esempio per quei paesi che non si sono ancora dotati di politiche e strumenti adeguati per fronteggiare le minacce che si originano nel cyber spazio o comunque da fonte di ispirazione per migliorare politiche e strumenti già esistenti[4]. La presente ricerca si è basata su fonti aperte documentali ed elementi puntuali di attualità, anche provenienti da addetti ai lavori, reperiti nell'ambito di conferenze ed interviste.

In seguito alla crescente e sempre più significativa penetrazione delle tecnologie dell'informazione e delle comunicazioni in tutte le funzioni della società moderna, il tema della cybersecurity ha gradualmente acquisito un'importanza strategica, ai fini della sicurezza nazionale e della crescita economica degli stati. Le nuove minacce che emergono dal cyber spazio mettono a dura prova la capacità degli stati di fronteggiarle adeguatamente, necessitando di un continuo adeguamento normativo e della pronta predisposizione degli opportuni strumenti di contrasto. Inoltre, la natura peculiare della minaccia cibernetica si presta ad un coordinamento più ampio, che travalichi i confini nazionali per una gestione partecipata della minaccia, tendenzialmente difficile da realizzare.

Elaborazione e continuo aggiornamento di un adeguato *framework* legale nazionale e promozione della cooperazione internazionale si rivelano due aspetti fondamentali della cybersecurity, *conditio sine qua non* per il progresso in materia.

A differenza delle tradizionali minacce, quelle informatiche presentano alcune particolarità: compressione spazio-temporale, trasversalità, asimmetricità, a-territorialità e continua mutevolezza. Queste caratteristiche generano una serie di problematiche, che rendono alquanto ardua l'azione comprensiva di contenimento della minaccia.

Ad esempio, il breve intervallo che intercorre tra il lancio di un attacco informatico e le sue conseguenze non consente di organizzare risposte secondo parametri spazio-temporali tradizionali. Così, anche il processo governativo di *decision-making* in risposta a questi eventi si mostra compresso. Inoltre, la trasversalità della minaccia, che consiste nella possibilità di lanciare un attacco informatico rivolto contro un determinato

[4] Per una trattazione dettagliata di questi due casi studio, si rimanda alla suddetta tesi, consultabile presso la Biblioteca del Polo delle Scienze sociali dell'Università di Firenze e nel sito del Catalogo delle tesi di laurea dell'ateneo fiorentino, tramite accesso con credenziali Unifi: http://www.sba.unifi.it/CMpro-v-p-222.html.

obiettivo rimbalzando prima il virus su altri dispositivi, rende difficile la localizzazione della sua origine. Un caso famoso di questo genere è la cosiddetta *botnet*, che sfrutta una serie di computer per perpetuare un certo attacco, senza che i loro proprietari ne siano consapevoli. L'uso di *botnet* non consente di risalire facilmente all'autore dell'attacco.

L'attacco informatico è stato paragonato a quello asimmetrico, nel quale i rapporti di forza risultano sbilanciati, in seguito allo scontro tra due soggetti di natura diversa. Un esempio di scontro asimmetrico è il conflitto tra l'esercito di uno stato ed un'organizzazione terroristica o di guerriglieri. L'attacco asimmetrico è caratterizzato da una serie di elementi: vantaggio dell'attaccante, non discriminazione tra obiettivi militari e civili, difficoltà nel risalire all'origine dell'attacco ed attribuirne la responsabilità ai colpevoli, crollo delle logiche di deterrenza e rappresaglia.

Infine, la possibilità di effettuare tali attacchi da notevoli distanze geografiche complica non solo l'operazione di tracciabilità, ma anche quella di perseguire e punire i responsabili. La minaccia cibernetica è in continua ed incessante evoluzione: pertanto, appare piuttosto difficile riuscire a tracciarne un profilo completo ed elaborare politiche e strumenti adeguati di risposta.

Considerate le problematiche associate alla cyber threat, è evidente la necessità per gli stati di intervenire attivamente, per essere in grado di fronteggiare i rischi e pericoli provenienti dal cyber spazio. Ciò non può prescindere dalla realizzazione della cooperazione internazionale, la quale si rivela essenziale, al fine di contenere questa nuova tipologia di minaccia alla sicurezza nazionale degli stati. Al crescere dell'interessamento generale per questa materia, si rivela importante valutare quello che l'Unione europea e l'Italia, nello specifico, hanno fatto e si propongono di fare, per garantire la sicurezza dello spazio cibernetico e del sistema paese nel suo complesso.

1.
Unione europea

Il presente capitolo si propone di indagare la questione della cybersecurity in Europa, attraverso la rassegna dei documenti ufficiali maggiormente rilevanti che hanno portato all'approvazione, nel febbraio 2013, della *Strategia dell'Unione europea per la cibersicurezza*. Verrà fatto riferimento al concetto di cybersecurity per come questo è presentato all'interno della strategia, intendendo con esso l'insieme di precauzioni ed interventi "che si possono prendere per proteggere il ciberdominio, in campo sia civile che militare, nei confronti delle minacce associate o che possono nuocere alle loro reti e infrastrutture di informazione interdipendenti"[5], al fine di preservare la disponibilità ed integrità delle reti e delle infrastrutture e la riservatezza delle informazioni ivi contenute. Questa precisazione si presenta opportuna per chiarire il significato del concetto di cybersecurity nel contesto europeo, considerata la riscontrata ambiguità del termine a livello generale. Infatti, ad oggi non esiste una definizione di cybersecurity universalmente accettata e questo contribuisce a complicare non solo l'attività di raccordo politico, ma anche quella di ricerca scientifica.

All'interno dell'Unione europea, i primi documenti ufficiali attinenti la sicurezza delle reti e delle informazioni risalgono agli inizi del 2000, a testimonianza del fatto che questa tematica è relativamente nuova ed in continua evoluzione. La cybersecurity in Europa rappresenta, allo stato attuale delle cose, un vero *work in progress*. L'approvazione della strategia di cybersecurity dell'Unione europea (7 febbraio 2013) è la base per la necessaria evoluzione verso l'elaborazione di strumenti più specifici dal punto di vista operativo, come ad esempio il relativo piano d'azione. La strategia del 2013 segna un importante spartiacque nella trattazione della cybersecurity, non certo un punto di arrivo. Il cammino europeo verso il 2013 è stato caratterizzato dalla progressiva definizione delle nuove minacce emergenti dal cyber spazio e dalla conseguente predispo-

[5] Commissione europea, *Strategia dell'Unione europea per la cibersicurezza: un ciberspazio aperto e sicuro*, (JOIN(2013)1), 7 febbraio 2013, p. 3, nota 4.

sizione degli strumenti di riposta. L'approccio europeo alla cybersecurity ha proceduto, in questi anni, a passi relativamente lenti, soprattutto se paragonati a quelli di alcuni paesi come Stati Uniti o Regno Unito, ma ciò è largamente dovuto all'assetto stesso dell'Unione, che, ovviamente, deve mettere d'accordo molti e più diversi punti di vista nazionali. Pertanto, l'UE ha registrato un ritardo nella formulazione di una propria strategia, il cui significato è da apprezzare, nella prospettiva di una più che auspicabile evoluzione delle capacità dell'Unione di affrontare la questione della cybersecurity. Questo perché la tematica necessita di un'adeguata trattazione non solo a livello nazionale, ma anche e soprattutto a livello UE, considerato che la cybersecurity è per definizione una questione che travalica i confini nazionali, necessitando una gestione multinazionale, e il ruolo guida che l'Unione mira a rivestire per gli stati membri.

1.1 Evoluzione delle politiche europee in ambito cyber

L'UE ha iniziato ad occuparsi di cybersecurity agli inizi del 2000. I primi documenti cercano di individuare le aree di priorità in ambito di sicurezza delle reti e restano significativi proprio per l'idea che forniscono dell'impostazione e delle priorità originarie dell'Unione. È significativo mettere in evidenza che il termine specifico "cybersecurity" non compare all'interno di questi primi documenti e non comparirà fino all'elaborazione della relazione del 2008 sull'implementazione della strategia europea in materia di sicurezza del 2003 (si veda oltre). Fino a quel momento, infatti, si parlerà di cybercrime e di protezione dei dati personali e delle infrastrutture critiche, senza esplicito riferimento al concetto più comprensivo di cybersecurity.

Nel 2000 la Commissione ha elaborato una comunicazione sul cybercrime[6] che tratta due questioni fondamentali della cybersecurity: la sicurezza delle infrastrutture dell'informazione e la lotta al crimine informatico. Questi macro-aspetti della cybersecurity costituiscono il nocciolo duro della visione europea, che dal 2000 mantiene queste due priorità in cima alla *to do list* per la sicurezza cibernetica.

[6] Commissione europea, *Creare una società dell'informazione sicura migliorando la sicurezza delle infrastrutture dell'informazione e mediante la lotta alla criminalità informatica. eEurope 2002* (COM(2000)890), 26 gennaio 2001.

Nel 2001 la Commissione ha presentato un documento[7] interamente dedicato alla definizione della NIS (Network and Information Security), che si propone la realizzazione di una politica europea in materia. Il testo – approvato nel mese di giugno, ovvero prima dell'attentato alle torri gemelle – testimonia la volontà autonoma dell'Unione di seguire un proprio percorso in questo campo. All'interno del documento si trova una definizione della NIS, che viene intesa come "la capacità di una rete o di un sistema d'informazione di resistere, ad un determinato livello di riservatezza, ad eventi imprevisti o atti dolosi che compromettono la disponibilità, l'autenticità, l'integrità e la riservatezza dei dati conservati o trasmessi e dei servizi forniti o accessibili tramite la suddetta rete o sistema"[8].

Di seguito alla definizione, il documento presenta un quadro generale delle minacce alla sicurezza che possono impattare sulla NIS. Tali minacce sono classificate in base alla loro natura e non anche all'ordine di importanza:

1) intercettazione delle comunicazioni;
2) accesso non autorizzato a computer e reti informatiche;
3) caduta della rete;
4) esecuzione di software "maligni" che modificano o distruggono i dati;
5) usurpazione di identità;
6) incidenti ambientali ed eventi imprevisti.

Mentre risulta abbastanza chiaro comprendere i primi due punti, è forse necessario spiegare cosa si intende con gli altri. Il terzo punto tratta i cosiddetti "disruptive attack", i quali comportano l'interruzione delle funzioni di un'infrastruttura, che può essere anche un'infrastruttura critica. Tale interruzione colpisce i fruitori del servizio e, nel caso di una infrastruttura critica, può interessare il sistema paese nel suo complesso, con possibilità di gravi danni economici. Il quarto punto è rappresentato dall'esecuzione di software maligni in grado di infettare i computer per provocare anche la modifica o la distruzione di dati. Questa è una realtà nota alla maggioranza degli utenti di internet. Il costo associato a questi attacchi risulta tutt'altro che trascurabile. Di seguito, l'usurpazione di

[7] Commissione europea, *Sicurezza delle reti e sicurezza dell'informazione: proposta di un approccio strategico europeo* (COM(2001)298), 6 giugno 2001.

[8] Ibidem, par. 2.1.

identità, da un lato, arreca danni all'immagine dei diretti interessati e, dall'altro, può mascherare come affidabili siti, blog e quant'altro in realtà contenenti software maligni in grado di introdurre virus nelle pagine personali degli utenti che vi accedono. Infine, la categoria degli incidenti ambientali ed eventi imprevisti comprende tutti quei casi che sfuggono alla volontà umana. Spesso, questi derivano da eventi naturali, quali catastrofi od incidenti, ma possono anche presentarsi come diretta conseguenza dell'errore umano. L'inevitabile correlazione tra reti cibernetiche e reti fisiche comporta questo tipo di problematiche, molto difficili da contrastare. Come ha sostenuto David Omand, visiting professor del King's College di Londra e segretario permanente dell'Home Office del Regno Unito, l'interruzione di un servizio è più probabile sia dovuta ad un incidente ambientale piuttosto che ad un attacco deliberato, pertanto la distinzione tra minacce maligne ed eventi accidentali si rivela meno importante che la definizione dei tempi massimi previsti per il recupero del servizio[9].

Nei primi anni 2000 altri due documenti hanno segnato l'inizio di un interessamento europeo alle dinamiche scaturite dal processo di digitalizzazione: il documento del 2000 *eEurope*[10] e quello del 2002 *eEurope 2005*[11]. Questi si inseriscono all'interno della visione presentata dalla strategia di Lisbona del 2000, intesa a far diventare l'Europa l'economia basata sulla conoscenza "più competitiva e più dinamica del mondo"[12] entro il 2010, ed esprimono la necessità per l'Europa di dotarsi di moderni servizi pubblici offerti sulla rete e di un'affidabile infrastruttura di protezione dell'informazione.

Ancora nel 2002 sono state approvate tre importanti direttive in materia di NIS: la direttiva 2002/21/CE, che istituisce un quadro normativo comune per le reti ed i servizi di comunicazione elettronica; la direttiva 2002/19/CE, relativa all'accesso alle reti di comunicazione elettronica e alle risorse correlate e all'interconnessione delle medesime; e la

[9] David Omand, "The steps needed to protect the EU's critical infrastructure against cyber-attack", in *Europe's World*, No. 25 (Autumn 2013), p. 112-118, http://europesworld.org/?p=176.

[10] Commissione europea, *eEurope. Una società dell'informazione per tutti* (COM(2000)130), 8 marzo 2000.

[11] Commissione europea, *eEurope 2005: una società dell'informazione per tutti* (COM(2002)263), 28 maggio 2002.

[12] Ibidem, p. 7.

direttiva 2002/20/CE, relativa alle autorizzazioni per le reti ed i servizi di comunicazione elettronica. Esse sono state tutte abrogate, in seguito all'approvazione nel 2009 di una nuova direttiva "*framework*", di cui si dirà più avanti.

Nel 2003 l'UE ha elaborato una propria strategia in materia di sicurezza. Il testo della strategia non fa menzione del termine "cybersecurity", ma individua una "dipendenza europea da un'infrastruttura interconnessa nel settore dei trasporti, dell'energia, dell'*informazione* ed altri, e la conseguente vulnerabilità dell'Europa sotto questo profilo" (corsivo aggiunto)[13].

La strategia europea per la sicurezza è ancora in vigore, non essendo mai stata modificata né aggiornata. Dopo una relazione sulla sua implementazione nel 2008[14], il progetto di una nuova strategia non è mai giunto a termine, lasciando in vigore il testo del 2003. Una revisione del documento sarebbe auspicabile, in considerazione del fatto che le minacce alla sicurezza sono in continua evoluzione, proprio come dimostra l'emergere della questione cyber negli ultimi dieci anni: il peso crescente che questo tema sta acquisendo a livello globale meriterebbe di essere menzionato all'interno di ogni strategia di sicurezza, anche dell'Unione europea. Il termine "cybersecurity" compare per la prima volta proprio nel testo in lingua inglese[15] della suddetta relazione del 2008 (si veda oltre), ma resta ancora fuori da quello della strategia di sicurezza ufficialmente in vigore.

1.2 L'ENISA

Il 2004 è stato un anno molto importante per l'avanzamento della cybersecurity in Europa, poiché l'Unione ha approvato il regolamento (CE) 460/2004 che istituisce l'Agenzia europea di sicurezza delle reti e dell'informazione – meglio conosciuta con l'acronimo inglese ENISA – "[a]l fine di assicurare un alto ed efficace livello di sicurezza delle reti e dell'informazione nell'ambito della Comunità e di sviluppare una cultura in

[13] Consiglio dell'Unione europea, *Un'Europea sicura in un mondo migliore. Strategia europea in materia di sicurezza*, 12 dicembre 2003, p. 2.

[14] Consiglio dell'Unione europea, *Relazione sull'attuazione della strategia europea in materia di sicurezza. Garantire sicurezza in un mondo in piena evoluzione* (S407/08), 11 dicembre 2008.

[15] La versione in italiano riporta la traduzione "sicurezza informatica".

materia di sicurezza delle reti e dell'informazione"[16]. L'agenzia ha il compito di assistere la Commissione e la comunità degli stati membri, accrescendone le capacità di prevenire e affrontare i problemi di sicurezza delle reti e dell'informazione e di reagirvi[17], fornendo loro assistenza e consulenza e contribuendo allo sviluppo generale di un alto livello di competenze. Infine, l'agenzia contribuisce a promuovere e diffondere una nuova cultura della sicurezza, affinché la questione della cybersecurity venga adeguatamente affrontata a livello europeo e soprattutto nazionale, tramite la predisposizione degli strumenti legali opportuni. Nel maggio 2013, con il regolamento (UE) 526/2013[18], la Commissione ha esteso e rafforzato il mandato dell'ENISA fino al 2020, facendo così dell'agenzia il vero punto di riferimento europeo per la cybersecurity.

L'attività principale dell'ENISA è quella di coordinare l'operato degli stati membri e favorire il dialogo intra-europeo, attraverso l'elaborazione di linee guida e l'individuazione di *best practices*. A questo scopo, l'agenzia pubblica molti documenti, disponibili online e liberamente consultabili, per cercare di tenere aggiornato lo stato dell'arte della cybersecurity in Europa e stimolare il confronto tra i vari stati, nell'intento che si affermino le pratiche più avanzate.

Notevole è l'impegno che l'agenzia ha dimostrato e continua a dimostrare nello stimolare gli stati membri ad adottare una propria strategia nazionale di sicurezza cibernetica: è fondamentale il manuale *National Cyber Security Strategies*, pubblicato nel 2012 e rivolto a tutti quegli stati che non si sono ancora dotati degli strumenti necessari per gestire efficacemente la questione della cybersecurity.

La guida si rivolge non solo al settore pubblico ma anche a quello privato[19], nell'auspicio di rivelarsi utile per l'elaborazione congiunta di strategie nazionali di sicurezza cibernetica. Nello specifico, il testo propone un modello semplificato del tipo *lifecycle* per lo sviluppo, la valutazione

---

[16] Regolamento (CE) n. 460/2004 del 10 marzo 2004 che istituisce l'Agenzia europea per la sicurezza delle reti e dell'informazione, art. 1.1.

[17] Ibidem, art. 2.1.

[18] Regolamento UE 526/2013 del 21 maggio 2013 relativo all'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (ENISA) e che abroga il regolamento (CE) n. 460/2004, 2013.

[19] "This guide aims to provide useful and practical recommendations to relevant public and private stakeholders on the development, implementation and maintenance of a cyber-security strategy". ENISA, *National Cyber Security Strategies. Practical Guide on Development and Execution*, cit., par. 1.2.

ed il mantenimento della suddetta strategia, in ambito nazionale. Tale modello si suddivide in due fasi cruciali: quella di sviluppo ed esecuzione e quella di valutazione ed aggiustamento, nell'ambito di una struttura del tipo "*Plan-Do-Check-Act*" (PDCA). La guida definisce nel dettaglio ogni singola fase del processo di costruzione ed implementazione di una strategia di cybersecurity nazionale, ponendosi a supporto dell'operato degli stati. Il testo merita di essere annoverato tra i documenti più importanti prodotti dall'ENISA.

L'operato dell'agenzia è estremamente importante per quanto riguarda la promozione della cooperazione in ambito cybersecurity e a questo scopo è stato istituito un chiaro meccanismo di *incident reporting*, per incentivare gli *internet and service provider* (ISP) a rendere pubblici gli attacchi cibernetici subiti, coinvolgendo le autorità nazionali competenti e, di seguito, le istituzioni europee interessate e gli altri stati. Il meccanismo istituisce un vasto sistema di notificazione e scambio di informazioni tra tutti gli attori coinvolti: i *provider*, gli utenti, le autorità nazionali competenti, l'ENISA e la Commissione. Nello specifico, spetta a questi ultimi due - Commissione ed ENISA - adottare le misure di sicurezza opportune ed indirizzarle verso le autorità nazionali competenti ed i *provider*.

Risulta, quindi, chiaro che il sistema di *reporting* è basato sull'idea di collocare le istituzioni europee al vertice della struttura operativa, così da poter garantire una guida sovranazionale alle azioni da intraprendere nei casi specifici. La realtà dei fatti, però, scoraggia questo disegno, considerato che solo in pochi casi gli incidenti informatici vengono comunicati a chi di dovere e che, nella migliore delle ipotesi, questo può avvenire anche molti mesi dopo che si è verificato l'incidente. Esiste molta riluttanza nel rendere pubblici gli attacchi subiti, per ragioni di immagine e reputazione: molto spesso le imprese, ma anche gli stati stessi, preferiscono tacere al riguardo per non intaccare il proprio *status* e rivelare falle nel proprio sistema.

Compito dell'ENISA è quello di promuovere un vero e proprio cambio di mentalità, che diffonda una nuova cultura della sicurezza delle reti e delle informazioni, basata sulla fiducia, la trasparenza e l'*information sharing*.

Compito dell'ENISA è anche quello di aumentare le competenze in campo tecnologico, attraverso l'organizzazione di esercitazioni che consentano di riunire tutto il *know how* dei maggiori esperti a livello europeo e non solo, così da accrescere le possibilità di fronteggiare ade-

guatamente i rischi dello spazio cibernetico. Fino ad oggi, l'ENISA ha organizzato due esercitazioni, denominate "Cyber Europe": una nel 2010 ed una nel 2012. La seconda ha coinvolto anche numerosi attori del settore privato, rimasti esclusi da quella del 2010.

L'esercitazione del 2010 si è basata sulla simulazione di un attacco rivolto contro gli *Internet Interconnected Site* (IIS), che si è caratterizzato per la graduale perdita dell'interconnettività internet tra tutti gli stati membri partecipanti. Lo scenario aveva come obiettivo quello di stimolare la cooperazione tra gli stati, al fine di ripristinare il corretto funzionamento di internet in tutta l'Europa.

L'esercitazione del 2012 ha presentato uno scenario più complesso, incentrato su una serie di incidenti informatici su larga scala, che hanno nuovamente coinvolto tutti i paesi partecipanti. Nello specifico, si è trattato di un attacco massiccio diretto soprattutto ai servizi di distribuzione di energia elettrica, avente lo scopo di interromperne le funzioni (DdoS, Distributed Denial of Service). I partecipanti hanno ricevuto informazioni sullo scenario tramite posta elettronica e hanno poi dovuto collaborare utilizzando procedure e strutture standard, per valutare la situazione e concordare le possibili linee d'azione. Come detto, oltre a 25 paesi e ad alcune istituzioni europee, nel 2012 hanno preso parte anche molti rappresentanti del mondo industriale e della sicurezza informatica, il cui coinvolgimento ha segnato un importante avanzamento dei risultati ottenuti, sia a livello di *know how* che a livello cooperativo.

Nel 2006 la Commissione ha elaborato la comunicazione relativa a una strategia per una "società dell'informazione sicura"[20], nella quale si è nuovamente sostenuta l'esigenza di portare avanti l'impegno europeo nella diffusione di una maggiore sicurezza delle reti e delle informazioni e di una cultura della cybersecurity.

Nello stesso anno è stata approvata anche la comunicazione della Commissione relativa ad un programma europeo per la protezione delle infrastrutture critiche[21]. Questo documento ha stabilito la creazione di un gruppo di contatto PIC (Protezione infrastrutture critiche) quale piattaforma di coordinamento e cooperazione per gli aspetti generali del programma. Presieduto dalla Commissione, il gruppo riunisce tutti

[20] Commissione europea, *Una strategia per una società dell'informazione sicura. "Dialogo, partenariato e responsabilizzazione"* (COM(2006)251), 31 maggio 2006.

[21] Commissione europea, *Comunicazione relativa a un programma europeo per la protezione delle infrastrutture critiche* (COM(2006)786), 12 dicembre 2006.

i punti di contatto PIC nazionali al fine di assistere gli stati membri nel processo di individuazione e designazione delle infrastrutture critiche nazionali, attraverso due criteri settoriali di base:

1) portata: perturbazione o distruzione di una particolare infrastruttura critica, misurata in base all'ampiezza dell'area geografica che potrebbe essere danneggiata, dalla sua perdita od indisponibilità;
2) gravità: conseguenze della perturbazione o distruzione di una particolare infrastruttura, valutate in base ai seguenti elementi:
   - conseguenze per i cittadini (numero di persone colpite);
   - conseguenze economiche (entità delle perdite economiche e/o del deterioramento di prodotti o servizi);
   - conseguenze ambientali;
   - conseguenze politiche;
   - conseguenze psicologiche;
   - conseguenze a livello di salute pubblica.

La comunicazione sull'EPCIP (European Programme for Critical Infrastructure Protection) resta significativa per aver predisposto un programma europeo dedicato alla protezione delle infrastrutture critiche europee e nazionali, che è stato ulteriormente sviluppato negli anni successivi.

Nel 2008 l'Unione ha presentato la *Relazione sull'attuazione della Strategia europea in materia di sicurezza*, già citata in precedenza, che nella sua versione in lingua inglese contiene il termine "cybersecurity". Nello specifico, la sicurezza informatica viene presentata come un aspetto rilevante delle questioni di terrorismo e criminalità organizzata[22]. Nel documento, quindi, viene fatto formalmente riferimento alla cybersecurity, considerando la possibilità che attacchi di natura cibernetica aventi come bersaglio sistemi informatici privati o governativi possano divenire una nuova potenziale arma economica, politica e militare. Sebbene la cybersecurity ricopra una parte ristretta del documento, la relazione è senza dubbio importante per quanto riguarda lo sviluppo della trattazione europea di questa materia.

Sempre nel 2008 è stata approvata la direttiva 2008/114/CE del Consiglio "relativa all'individuazione e alla designazione delle infrastrut-

[22] Consiglio dell'Unione europea, *Relazione sull'attuazione della strategia europea in materia di sicurezza*, cit., p. 5.

ture critiche europee e alla valutazione della necessità di migliorarne la protezione"[23]. La direttiva procede all'individuazione delle infrastrutture critiche per l'Europa, cosiddette ECI (European Critical Infrastructure), tramite l'utilizzo di alcuni criteri per valutarne il peso effettivo e l'importanza fondamentale. Viene definita ECI "un'infrastruttura critica ubicata negli Stati membri il cui danneggiamento o la cui distruzione avrebbe un significativo impatto su almeno due Stati membri"[24].

I primi settori presi in considerazione per l'attuazione della direttiva sono stati quelli dell'energia e dei trasporti, più alcuni relativi sottosettori (Tabella 1), ma viene affermata l'intenzione di procedere in un secondo momento alla revisione della direttiva stessa, "al fine di valutarne l'impatto e di esaminare la necessità di includere nel suo campo di applicazione altri settori, tra i quali anche quello delle tecnologie dell'informazione e della comunicazione (ICT)"[25].

Tabella 1 – Settori di ECI

Settore	Sottosettore	
I. Energia	1. Elettricità	Infrastrutture e impianti per la produzione e la trasmissione di energia elettrica per la fornitura di elettricità
	2. Petrolio	Produzione, raffinazione, trattamento, stoccaggio e trasporto di petrolio attraverso oleodotti
	3. Gas	Produzione, raffinazione, trattamento, stoccaggio e trasporto di gas attraverso oleodotti
		Terminali GNL
II. Trasporti	4. Trasporto stradale	
	5. Trasporto ferroviario	
	6. Trasporto aereo	
	7. Vie di navigazione interna	
	8. Trasporto oceanico, trasporto marittimo a corto raggio e porti	

Fonte: Direttiva 2008/114/CE dell'8 dicembre 2008, allegato 1.

Ad oggi, la direttiva non ha subito modifiche, continuando ad interessare i soli settori dell'energia e dei trasporti, anche se l'ICT è spesso dichiarato sempre più fondamentale per il funzionamento delle moderne società europee. La direttiva del 2008 offre, dunque, un contributo importante allo sviluppo della tematica cyber in Europa, sia per l'inclusione

[23] Direttiva 2008/114/CE dell'8 dicembre 2008 relativa all'individuazione e alla designazione delle infrastrutture critiche europee e alla valutazione della necessità di migliorarne la protezione.

[24] Ibidem, art. 2.b.

[25] Ibidem, preambolo, punto 5.

potenziale del settore ICT tra quelli coperti sia perché le infrastrutture critiche anche di altri settori sono largamente basate su infrastrutture ICT, così che attacchi/eventi cinetici e cibernetici devono essere considerati e gestiti per ridurre il rischio di compromissione di infrastrutture critiche europee.

Un documento della Commissione dell'agosto 2013[26] ha ribadito la necessità di estendere il campo di applicazione della direttiva del 2008 anche al settore ICT, in considerazione della forte interdipendenza tra quest'ultimo e i settori dell'energia e dei trasporti. Inoltre, il documento sembra suggerire che la proposta di direttiva che ha accompagnato l'approvazione della strategia europea per la cibersicurezza (si veda paragrafo 3.6) potrebbe offrire degna copertura al settore ICT[27].

Procedendo nella trattazione dei documenti maggiormente rilevanti, nel 2009 è stata approvata la direttiva 2009/140/CE, detta *framework* per le reti ed i servizi di comunicazione elettronica[28]. Tale direttiva obbliga gli stati membri a predisporre le misure interne atte a garantirne l'applicazione. In particolare occorre evidenziare l'importanza dell'articolo 13, recante misure concernenti la sicurezza delle reti, il quale invita alla creazione di "autorità nazionali di regolamentazione". Ad oggi, la direttiva non è stata ancora recepita nell'ordinamento italiano, soprattutto per quanto riguarda l'articolo 13.

Ancora nel 2009 la Commissione europea ha presentato la comunicazione relativa alla protezione delle infrastrutture critiche informatizzate[29]. La comunicazione mette in evidenza che le infrastrutture informatizzate si rivelano vitali per la crescita dell'economia e della società dell'Unione; pertanto, essa predispone un piano d'azione per rafforzare la sicurezza e la resilienza delle infrastrutture ICT e di quelle altre il cui funzionamento è retto dalle tecnologie dell'informazione e delle comunicazioni. In questo ambito, la comunicazione rafforza il ruolo dell'ENISA,

---

[26] European Commission, *Commission Staff Working Document on a new approach to the European Programme for Critical Infrastructure Protection. Making European Critical Infrastructures more secure* (SWD(2013)318), 28 August 2013.

[27] Ibidem, p. 8.

[28] Direttiva 2009/140/CE del 25 novembre 2009 recante modifica delle direttive 2002/21/CE, 2002/19/CE e 2002/20/CE.

[29] Commissione europea, *Proteggere le infrastrutture critiche informatizzate. "Rafforzare la preparazione, la sicurezza e la resilienza per proteggere l'Europa dai ciberattacchi e dalle ciberperturbazioni"* (COM(2009)149), 30 marzo 2009.

sul piano tattico ed operativo, incaricandola di implementare il già citato EPCIP.

Il piano d'azione illustrato nel documento è articolato in cinque punti:

1) preparazione e prevenzione, grazie al ruolo dell'ENISA e delle partnership pubblico-privato;
2) individuazione e risposta, grazie all'adozione di un sistema europeo di condivisione delle informazioni e di allarme (EISAS, European Information Sharing and Alert System);
3) mitigazione e recupero, tramite i piani d'emergenza, le esercitazioni nazionali e paneuropee e l'attività dei CERT nazionali;
4) cooperazione internazionale, tramite la cooperazione tra CERT nazionali;
5) criteri per le ECI nel settore ICT, per favorirne l'individuazione e la designazione.

La comunicazione del 2009 sulla protezione delle infrastrutture critiche ha contribuito ad accrescere il ruolo dell'ENISA a livello europeo, per il coordinamento delle politiche nazionali volte alla protezione delle infrastrutture critiche. L'impegno europeo in questo settore è stato riconfermato nel 2011, dalla comunicazione "relativa alla protezione delle infrastrutture critiche informatizzate" [30] e dalle seguenti conclusioni del Consiglio[31]. Entrambi questi documenti del 2011 hanno confermato il ruolo primario dell'ENISA in ambito PIC e invitato gli stati membri a procedere alla realizzazione di un proprio CERT nazionale.

Nel settembre 2010 la Commissione ha presentato una proposta di direttiva relativa agli attacchi contro i sistemi di informazione. Il documento si propone di introdurre "fattispecie di reato nel settore degli attacchi contro i sistemi di informazione e [...] norme minime per le relative sanzioni [... nonché] disposizioni comuni per impedire tali

[30] Commissione europea, *Comunicazione relativa alla protezione delle infrastrutture critiche informatizzate "Realizzazioni e prossime tappe: verso una sicurezza informatica mondiale"* (COM(2011)163, 31 marzo 2011.

[31] Consiglio dell'Unione europea, *Protezione delle infrastrutture critiche informatizzate "Realizzazioni e prossime tappe: verso una sicurezza informatica mondiale" (CIIP) - Adozione delle conclusioni del Consiglio* (10299/11), 19 maggio 2011.

attacchi e migliorare la cooperazione giudiziaria penale europea in questo campo"[32]. Gli articoli 3-6 definiscono i seguenti reati[33]:

1) accesso illecito a sistemi di informazione;
2) interferenza illecita per quanto riguarda i sistemi;
3) interferenza illecita per quanto riguarda i dati;
4) intercettazione illecita.

Negli ultimi anni, la proposta di direttiva sul cybercrime è stata più volte discussa dal Parlamento europeo. Nel luglio 2013 la proposta ed i relativi emendamenti presentati dalle varie commissioni coinvolte – in particolare dalla commissione Libertà civili, giustizia e affari interni – sono stati discussi in sessione plenaria, ma ad oggi la direttiva non è stata ancora approvata.

Nel 2010 sono stati pubblicati altri due importanti documenti: *Un'agenda digitale europea* e la strategia di sicurezza interna. L'agenda digitale si prefigge lo scopo di "ottenere vantaggi socioeconomici sostenibili grazie a un mercato digitale unico basato su internet veloce e superveloce e su applicazioni interoperabili"[34]. Nello specifico, l'agenda individua le linee d'azione da seguire nei due macro-settori del "mercato digitale unico e dinamico" e dell' "interoperabilità e standard".

La realizzazione di un mercato unico e sicuro, da una parte, incrementa la sicurezza dei cittadini europei e, dall'atra, attrae investimenti a beneficio di domanda ed offerta. L'obiettivo è, dunque, quello di conseguire dei vantaggi dal punto di vista sociale ed economico, a partire dall'attuale situazione di interconnessione costante e digitalizzazione crescente.

Il secondo documento, *La strategia di sicurezza interna dell'UE in azione*[35], cerca di delineare le attuali minacce alla tenuta del complesso europeo, così individuando cinque tappe verso un'Europa più sicura:

1) smantellare le reti criminali internazionali;

---

[32] Commissione europea, *Proposta di direttiva relativa agli attacchi contro i sistemi di informazione, e che abroga la decisione quadro 2005/222/GAI del Consiglio* (COM(2010)517), 30 settembre 2010, art. 1.

[33] L'articolo 9 stabilisce che i tali reati sono punibili con pene detentive non inferiori ai due anni.

[34] Commissione europea, *Un'agenda digitale europea* (COM (2010) 245 f/2), 26 agosto 2010, p. 3.

[35] Commissione europea, *La strategia di sicurezza interna dell'UE in azione: cinque tappe verso un'Europa più sicura* (COM(2010)673), 22 novembre 2010.

2) prevenire il terrorismo e contrastare la radicalizzazione e il reclutamento;
3) aumentare i livelli di sicurezza per i cittadini e le imprese nel ciberspazio;
4) rafforzare la sicurezza attraverso la gestione delle frontiere;
5) aumentare la resilienza dell'Europa alle crisi e alle calamità.

Dei cinque *step* sopra elencati, quello che rileva è il terzo. Accrescere la sicurezza dei cittadini, da un lato, e quella del settore industriale, dall'altro, costituisce una priorità assoluta per la cybersecurity e, quindi, per la sicurezza dell'Unione stessa. Relativamente a questo punto, la strategia riconosce l'importanza di proteggere tutti coloro che usufruiscono di internet e dei servizi online – cosiddetti "end user" (utenti finali) – dai rischi derivanti dal crimine informatico. In particolare, questo dovrebbe avvenire attraverso una maggiore europeizzazione delle procedure di perseguimento dei responsabili.

Inoltre, si sottolinea l'importanza di collaborare con il settore privato e di conseguire progressi in campo tecnologico, per garantire una risposta efficace ai cyber attack. Queste ultime due considerazioni rappresentano la vera ossatura del progetto volto ad aumentare il livello di sicurezza nel cyber spazio. Partnership pubblico-privata e *capability building* costituiscono due condizioni imprescindibili per la cybersecurity.

Per garantire la realizzazione di questa terza tappa verso un'Europa più sicura, la strategia stabilisce tre azioni da intraprendere, individuando per ciascuna di esse le autorità incaricate ed il termine di previsione per la messa in pratica. La prima azione riguarda l'istituzione di un Centro europeo per il cybercrime, realizzato nel 2012 e divenuto operativo dal 2013, in sostituzione del già esistente Hi-Tech Crime Centre presso l'Europol. La seconda azione mira alla creazione di un meccanismo di *incident reporting*, attraverso il quale cittadini e imprese possano fare rapporto sui crimini informatici subiti. La terza azione, infine, consiste nella messa in atto di un network di CERT nazionali e CERT-EU e di un sistema europeo di condivisione delle informazioni e di allarme (EISAS).

Nel marzo 2012 la Commissione ha chiesto ufficialmente all'Europol di creare uno European Cyber Crime Centre (EC3), per farne il punto focale della lotta europea contro il crimine informatico. Il centro è divenuto operativo dal gennaio 2013 ed attualmente svolge il ruolo di coordinamento delle investigazioni a livello europeo, agendo da punto di riferimento per il cybercrime in Europa. Il compito dell'EC3 è di offrire

supporto agli stati membri e alle istituzioni europee nello sviluppo delle capacità operative ed analitiche relative alle attività di investigazione e alla promozione della cooperazione con i partner internazionali.

Nel settembre dello stesso anno l'Unione ha deciso di creare anche il CERT-EU (Computer Emergency Response Team of the European Union), l'organo europeo deputato al monitoraggio delle minacce nel cyber spazio e alla risposta ad attacchi di natura cibernetica. Il CERT-EU è composto da esperti nel campo della sicurezza informatica provenienti da alcune delle maggiori istituzioni europee – quali la Commissione, il Segretariato generale del Consiglio, il Parlamento, il Comitato delle Regioni ed il Comitato economico e sociale – e collabora con i CERT nazionali degli stati membri e con alcune grandi compagnie di sicurezza ICT.

Dal 2012, quindi, l'Unione si è dotata di alcuni strumenti operativi necessari per affrontare i rischi provenienti dalla dimensione digitale e coordinare le attività dei singoli stati membri. A questo punto, diventa perciò cruciale che tutti gli stati si adeguino di conseguenza, realizzando strutture simili e consentendo un'efficiente attività di dialogo e scambio a livello UE. Tali attività dovrebbero beneficiare di strutture verticali ed orizzontali che siano in grado di realizzare la cooperazione sia tra i CERT nazionali e le istituzioni europee sia tra questi ed i vari *stakeholder* privati sia, infine, tra i CERT nazionali stessi.

Ad oggi sono 23 gli stati membri dell'Unione europea che si sono dotati di un proprio CERT nazionale[36]. Mancano all'appello Bulgaria, Cipro, Croazia, Grecia, Irlanda e l'Italia, la quale non ha ancora provveduto a realizzare il proprio CERT nazionale malgrado la disposizione del DPCM del 24 gennaio 2013 (si veda paragrafo 2.5). In Italia sono attivi un CERT-Difesa ed un CERT-PA, quest'ultimo inaugurato nel gennaio del 2014.

1.3 La strategia dell'Unione europea per la cibersicurezza

Nel 2013 si arriva all'approvazione della *Strategia dell'Unione europea per la cibersicurezza* (7 febbraio 2013). Il documento è frutto del lavoro congiunto della Commissione e dell'Alto Rappresentante per gli affari esteri e la politica di sicurezza ed illustra la visione dell'UE sul tema della

[36] Software Engineering Institute, *List of National CSIRTs*, http://www.cert.org/incident-management/national-csirts/national-csirts.cfm.

cybersecurity e le azioni necessarie da intraprendere, per garantire la sicurezza di tutti i cittadini e degli stati.

Nella sua parte iniziale, la strategia cerca di mettere in evidenza il peso del fattore ICT nell'era moderna, il quale costituisce ormai un aspetto fondamentale della vita sociale e della crescita economica dei paesi europei, nonché una risorsa critica sulla quale poggia gran parte del settore industriale. La dipendenza di quest'ultimo e di molte delle infrastrutture critiche nazionali dai sistemi digitalizzati e da internet in generale cresce sempre più; e così crescono anche i rischi. Pertanto, è dichiarato per l'Europa l'obiettivo di dotarsi degli strumenti necessari per poter prevenire ed eventualmente reagire a possibili attacchi di natura cibernetica, in grado di recare notevoli danni e di attentare alla sicurezza dei paesi.

Scopo principale della strategia, come indicato anche nel titolo, è quello di garantire uno spazio cibernetico "aperto e sicuro", che sia accessibile a tutti e, allo stesso tempo, dotato degli strumenti adeguati per assicurare la riservatezza dei dati e delle informazioni in esso contenuti. Compito dell'Unione è promuovere l'applicazione di principi, norme e valori che sono già validi nella dimensione fisica, anche in quella digitale. Diritti fondamentali, democrazia e stato di diritto dovrebbero essere tutelati anche nel cyber spazio. Questi principi sono elencati all'interno della strategia:

1) protezione dei diritti fondamentali, della libertà di espressione, dei dati personali e della privacy;
2) accesso alla rete garantito per tutti;
3) *multi-stakeholder governance* democratica ed efficiente;
4) responsabilità condivisa tra tutti gli attori coinvolti.

Il rispetto di questi "*core values*" si presenta indispensabile per la messa in atto delle azioni necessarie a raggiungere gli obiettivi che la strategia si prefigge. In particolare, il documento delinea cinque priorità fondamentali per poter fronteggiare le minacce provenienti dal cyber spazio:

1) raggiungere la ciberresilienza;
2) ridurre drasticamente il cibercrimine;
3) sviluppare una politica e capacità di ciberdifesa connesse alla Politica di sicurezza e di difesa comune (PSDC);
4) sviluppare le risorse industriali e tecnologiche per la cibersicurezza;

5) creare una politica internazionale coerente dell'Unione europea sul ciberspazio e promuovere i valori costitutivi dell'UE.

La prima priorità riguarda il concetto di resilienza, con il quale si intende la capacità di una rete o di un sistema di preservare le proprie capacità ed i propri servizi, in caso di attacco. L'operazione successiva, di ripristino delle funzioni allo stadio iniziale, è invece definita "*recovery*" ed è altrettanto importante per la cybersecurity. Una buona capacità di resilienza assicura il pronto intervento delle autorità competenti ed il contenimento dei danni provocati dall'attacco. Ad esempio, nei casi di DDoS la suddetta capacità si rivela essenziale per porre fine alla fase di disagio e disservizio ed impedire l'eccessivo danno economico associato.

La seconda priorità consiste nella lotta massiva al cybercrime, il quale rappresenta oggi la causa maggiore di perdite di tipo economico, soprattutto a danno del settore privato. Ridurre il cybercrime è probabilmente l'obiettivo più urgente in questo ambito, poiché è necessario per garantire la protezione dei cittadini, dal punto di vista economico e non solo. Frodi telematiche, violazione dei dati personali, furto della proprietà intellettuale e dell'identità digitale, spionaggio industriale: questi fenomeni sono all'ordine del giorno e causano danni economici estremamente rilevanti e probabilmente sotto-stimati. Nel 2012 il 40% della popolazione europea si dichiara preoccupato per una possile manipolazione dei propri dati personali e il 38% per la sicurezza dei pagamenti online[37].

La terza priorità apre all'ambizione di creare una politica di cyberdefence, che sia inquadrata all'interno della PSDC; mentre la quarta rammenta l'importanza di progredire dal lato tecnologico, per essere in grado di gestire le situazioni di crisi. La quinta priorità proietta la questione della cybersecurity sul piano internazionale, a testimonianza del fatto che solo una proficua collaborazione a livello globale può portare a risultati importanti, nella sfida contro le minacce asimmetriche provenienti dal cyber spazio.

Di seguito vengono illustrate nel dettaglio le cinque azioni prospettate dalla strategia per garantire la sicurezza dello spazio cibernetico, le quali vengono individuate sulla base delle cinque priorità precedente-

[37] European Commission, *Special Eurobarometer 390: Cyber Security Report*, July 2012, p. 25, http://ec.europa.eu/public_opinion/archives/ebs/ebs_390_en.pdf.

mente esposte. Queste azioni sono: resilienza, lotta al cybercrime, cyber-defence policy, risorse tecnologiche ed international cyberspace policy.

1.3.1 Resilienza

Per incrementare il livello di resilienza cibernetica è fondamentale investire sul fattore tecnologico, ma è altrettanto importante cercare di coordinare l'operato di tutti gli attori coinvolti, per evitare inutili duplicazioni dei costi e facilitare lo scambio di informazioni, così velocizzando i tempi di progresso. Tutto questo è complesso da realizzare, considerato che gli stati non solo sono molto restii a devolvere poteri in ambito di sicurezza nazionale, ma si dimostrano anche molto reticenti e poco collaborativi nell'attività di *information sharing*.

Come riportato, al fine di promuovere la cooperazione intra-europea, l'Unione ha creato l'Agenzia di sicurezza delle reti e dell'informazione (ENISA), che dal 2004 opera per migliorare le capacità nazionali di ciber-resilienza e favorire il dialogo tra gli stati membri (si veda paragrafo 1.2). Nella strategia per la cibersicurezza la Commissione chiede all'ENISA di continuare a svolgere un ruolo fondamentale nei processi nazionali di *cyber capability building*, "in particolare creando competenze in materie di sicurezza e resilienza dei sistemi industriali di controllo e delle infrastrutture dei trasporti e dell'energia" e di "continuare a dare supporto agli Stati membri e alle istituzioni dell'UE nella realizzazione periodica di esercitazioni paneuropee sui ciberincidenti, che costituiranno anche la base operativa per la partecipazione dell'UE a esercitazioni internazionali sugli incidenti informatici"[38] Inoltre, la Commissione chiede all'ENISA di promuovere una "patente di sicurezza delle reti e dell'informazione"[39], quale programma di certificazione delle competenze e qualifiche dei professionisti informatici.

Stimolare il dialogo tra gli stati europei è una priorità della strategia, insieme a quella di incentivare la creazione di partnership pubblico-privato all'interno degli stati stessi. La cooperazione tra settore pubblico e privato è importante tanto quanto quella internazionale, soprattutto perché la maggior parte degli incidenti informatici coinvolge e colpisce proprio i privati. Le grandi compagnie industriali hanno cominciato da tempo a dotarsi di sistemi di sicurezza informatica in grado di arginare

[38] Commissione europea, *Strategia dell'Unione europea per la cibersicurezza*, cit., p. 8.
[39] Ibidem, p. 9.

la possibilità di attacchi e questo le ha messe in condizione di fare progressi nel tempo, in maniera più rapida rispetto a molti stati europei. L'esigenza di proteggere le proprie reti ed informazioni e di garantire la cosiddetta *business continuity* ha presto spinto gli operatori privati a predisporre sistemi di sicurezza capaci di rilevare attacchi di natura cibernetica e preservare, o al più ripristinare, le funzioni del servizio eventualmente danneggiato.

Generalmente, questi sistemi di sicurezza si costituiscono di un SOC (Security Operations Center) e di un CSIRT (Computer Security Incident Response Team) o CERT aziendale. Mentre il SOC ha il compito di monitorare lo stato delle infrastrutture IT e di sicurezza e di rilevarne possibili malfunzionamenti, CSIRT e CERT aziendali hanno invece il compito più specifico di rispondere efficacemente agli attacchi e di tutelare la continuità del servizio erogato.

Data la relativa maggiore esperienza del settore privato in questo campo, una buona partnership pubblico-privato (PPP) consentirebbe di coordinare gli sforzi e ridurre i costi, conseguendo risultati migliori in tempi più brevi. Tale partnership si dimostrerebbe vantaggiosa per entrambi le parti: il *know how* del privato potrebbe così trarre beneficio dall'autorità regolativa ed impositiva del governo nazionale, conseguendo obiettivi altrimenti difficili da realizzare senza chiare obbligazioni. Infatti, se l'innovazione può facilmente provenire dal settore privato, le priorità, invece, vengono categoricamente definite dai decisori politici. Pertanto, l'obiettivo di PPP non può che dipendere dalle politiche dei singoli stati europei, che hanno il dovere di incentivare questo tipo di collaborazioni.

A questo scopo, la strategia propone una serie di misure legislative da adottare a livello nazionale, la più significativa delle quali prevede la fissazione di "requisiti minimi comuni" per la sicurezza delle reti e delle informazioni. Tali requisiti minimi comuni avrebbero il pregio di obbligare gli stati a designare le autorità competenti, costituire centri di risposta alle emergenze cibernetiche (CERT) ed adottare strategie e piani d'azione nazionali per la NIS.

In questo quadro, la costituzione dei CERT nazionali rappresenta un passo fondamentale nella prospettiva di implementare la strategia europea, anche perché questi organi dovrebbero coordinarsi con il CERT-EU, che, come riportato, è responsabile per la sicurezza dei sistemi ICT delle istituzioni europee.

In fondo alla lista degli attori coinvolti si trovano gli utenti finali, i quali giocano anch'essi un ruolo significativo nel garantire la sicurezza

del cyber spazio. La strategia afferma l'importanza di diffondere tra gli utenti la consapevolezza dei rischi associati alla navigazione su internet, così che la prevenzione si costruisca dal basso, attraverso piccoli e semplici passi che mettano i cittadini nelle condizioni di potersi difendere. In quest'ottica si inseriscono le varie campagne di informazione volte a sensibilizzare il pubblico e promuovere un dibattito sulla questione della cybersecurity, ancora poco nota in alcuni paesi dell'Unione, specialmente nella società civile. Infatti, mentre le istituzioni ed il settore della ricerca dimostrano un crescente interesse per questa tematica, le imprese - pur possedendo gran parte del *know how* e delle risorse tecnologiche - si dimostrano ancora poco disposte a collaborare, sia con le autorità di governo che con le altre imprese, e la maggior parte degli utenti finali non ha sufficiente consapevolezza dei rischi associati all'uso delle reti. La diffusione di una cultura della sicurezza informatica si rivela, quindi, importante per fare sì che tutti gli attori coinvolti giochino il proprio ruolo nella sfida della cybersecurity.

1.3.2 Lotta al cybercrime

Il crimine informatico rappresenta la piaga peggiore per la sicurezza delle reti e delle informazioni, in termini di portata e di danni economici. Secondo uno studio commissionato da McAfee nel 2013, costa all'economia mondiale dai 300 miliardi a 1 miliardo di miliardi di dollari all'anno[40]. Ciò che merita veramente attenzione, però, è l'analisi degli effetti di questi numeri sul commercio, la tecnologia ed il benessere globale. Un sondaggio di Eurobarometro, ad esempio, evidenzia come circa il 38% degli utenti di internet, temendo di poter essere coinvolto in problematiche inerenti pagamenti online, abbia modificato il proprio comportamento: il 18% ha diminuito i propri acquisti online, mentre il 15% ha ridotto le proprie transazioni di *home banking*[41].

Il cybercrime ha acquisito negli ultimi anni un peso significativo ed una notorietà sempre più diffusa all'interno della società civile: secondo lo stesso sondaggio di Eurobarometro, il 73% circa della popolazione dell'UE ha visto o sentito qualcosa riguardo il cybercrime negli ultimi 12 mesi e

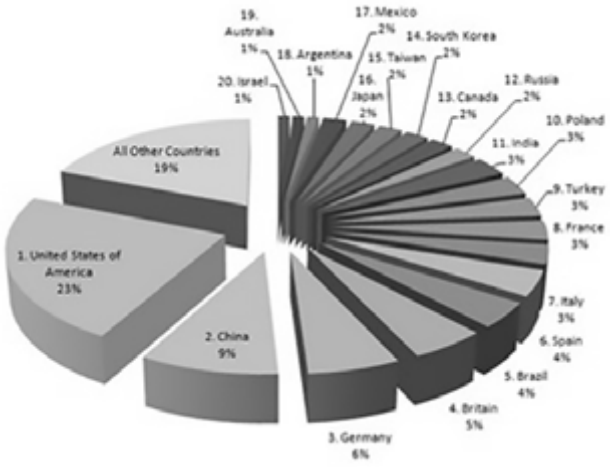
[40] James Andrew Lewis and Stewart Baker, *The Economic Impact of Cybercrime and Cyber Espionage*, Santa Clara, McAfee, July 2013, p. 5, http://csis.org/node/45446.

[41] European Commission, *Special Eurobarometer 390: Cyber Security Report*, cit., p. 28.

circa il 59% ne ha avuto notizia dalla televisione[42]. Questi dati costituiscono una media delle percentuali dei vari paesi membri, i quali presentano situazioni alquanto differenziate tra loro. In Italia, per esempio, si registra un tasso relativamente basso di informazione al riguardo: solo il 51% della popolazione nazionale ha sentito parlare di cybercrime dai mezzi di comunicazione od in sedi più informali, a fronte di un 40% che ne è totalmente all'oscuro. Infine, il 59% della popolazione europea si sente non adeguatamente o affatto informato sui rischi associati al cybercrime, mentre solo il 7% se ne dichiara ben consapevole[43]. Anche in questo caso, le percentuali variano a seconda dei contesti nazionali: paesi come Danimarca, Svezia e Finlandia registrano tassi di consapevolezza elevati, fino al 73%; mentre altri, come l'Italia, superano di poco il 20%.

Le differenziazioni sopra riportate dipendono in maniera significativa anche dalla diversa diffusione del crimine informatico nei vari contesti nazionali. Il grafico 1 illustra le percentuali di penetrazione del cybercrime nei venti paesi maggiormente colpiti. Come si può vedere, l'Italia ricopre la settima posizione, con una percentuale pari al 3%, dietro a Stati Uniti, Cina, Germania. Regno Unito, Brasile e Spagna.

Grafico 1 - I venti paesi maggiormente colpiti dal cybercrime



Fonte: BusinessWeek/Symantec 2009[44].

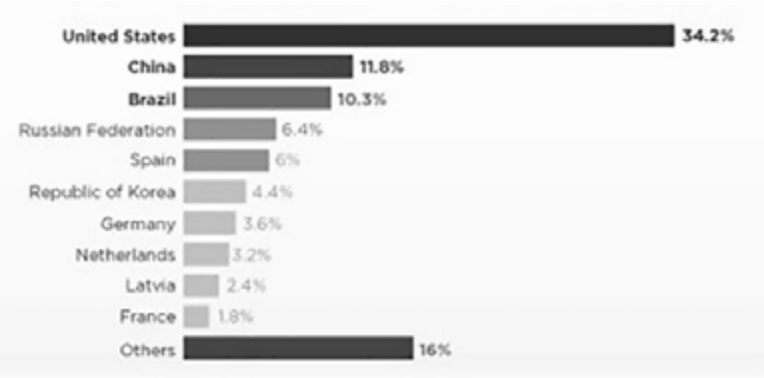
[42] Ibidem, p. 34-35.

[43] Ibidem, p. 37.

[44] Per i dati si veda Rachael King, "Malware Run Amok", in *BusinessWeek*, 7 July 2009, http://images.businessweek.com/ss/09/07/0707_ceo_guide_security/index.htm. Il

Nel grafico 2 è riportata la lista dei dieci paesi dai quali si origina il maggior numero di crimini informatici. Ancora una volta, Stati Uniti, Cina e Brasile compaiono in cima alla lista, allo stesso tempo bersaglio e luogo d'origine della maggior parte delle attività di cybercrime.

Grafico 2 - I dieci paesi in cui si origina il maggior numero di crimini informatici



Fonte: Websense, *2010 Threat Report*, November 2010, p. 9, https://it.websense.com/content/threat-report-2010-malware.aspx.

La lotta al cybercrime necessita di adeguati strumenti e, in particolare, di legislazioni forti ed efficaci, di meccanismi di *law enforcement* e di buone capacità tecnico-operative. In tutto questo, l'UE può coordinare l'attività dei singoli stati, facilitando un approccio collaborativo che metta insieme le autorità giudiziarie e gli *stakeholder*, ai vari livelli dell'Unione.

1.3.3 Cyberdefence policy

Per fronteggiare le minacce provenienti dal cyber spazio, l'Unione dovrebbe dar vita ad una politica di sicurezza cibernetica, inserita nell'ambito della Politica di sicurezza e difesa comune. Secondo quanto si legge nella strategia, lo sviluppo della cyberdefence dovrebbe concentrarsi sulle attività di "individuazione, risposta e recupero nei confronti di ciberminacce sofisticate" per "aumentare la resilienza dei sistemi

grafico è disponibile nell'eurosblog *l'Europa@Tor Vergata*, http://torvergata.eurosblog.eu/spip.php?article575.

informativi e di comunicazione che supportano gli interessi della difesa e della sicurezza nazionale degli Stati membri"[45].

La cyberdefence, quindi, si presenta rilevante al fine di tutelare la difesa e gli interessi di sicurezza nazionale degli stati membri. Per garantire un'adeguata cyberdefence, è necessario coinvolgere tutti gli aspetti del processo di *capability development*: "la dottrina, la leadership, l'organizzazione, il personale, la formazione, la tecnologia, l'infrastruttura, la logistica e l'interoperabilità"[46]. Questo processo è affidato all'Alto Rappresentante per gli affari esteri e la politica di sicurezza, agli stati membri e all'Agenzia europea di difesa (EDA), in collaborazione con l'ENISA e l'Europol.

Per incrementare le capacità di difesa europee in ambito cibernetico è opportuno predisporre di adeguati fondi e, per questo motivo, si rivelano cruciali i progetti di finanziamento in Europa, in particolare nell'ambito di "Horizon 2020", programma quadro di ricerca e innovazione che dispone di circa 80 miliardi di euro per il periodo 2014-2020.

Per quanto riguarda i finanziamenti alla cybersecurity, si deve fare riferimento ad almeno due aree distinte di tale programma: "Secure societies. Protecting freedom and security of Europe and its citizens" e "ICT Research & Innovation". Nella prima area vengono individuate le attività principali che l'Unione europea si impegna ad intraprendere per garantire la pace e la sicurezza dei suoi paesi membri. Tra queste attività compare anche l'avanzamento della cybersecurity. In questa sezione è presente il programma "Digital Security: Cybersecurity, Privacy and Trust", con a disposizione 47.040.000 euro per il 2014.

La seconda area riguarda lo sviluppo del settore ICT, che da solo rappresenta il 4,8% dell'economia europea[47]. La relativa sezione "Leadership in enabling and industrial technologies" contiene il programma "ICT 2014. Information and Communications Technology", con 125.000.000 euro per il 2014.

Nei giorni 19 e 20 dicembre 2013 il Consiglio europeo si è riunito per discutere, tra l'altro, della Politica di sicurezza e di difesa comune. Nelle conclusioni è affermata l'importanza di favorire lo sviluppo della PSDC, così superando la frammentazione dei mercati europei della difesa, che incide negativamente sulla sostenibilità e competitività dell'industria

[45] Commissione europea, *Strategia dell'Unione europea per la cibersicurezza*, cit., p. 12.
[46] Ibidem, p.13.
[47] http://ec.europa.eu/programmes/horizon2020/en/area/ict-research-innovation

europea della sicurezza e difesa.[48] Il rafforzamento della PSDC richiede l'azione decisa di tutti i paesi membri dell'Unione, in collaborazione con i suoi partner chiave: le Nazioni Unite e la NATO. Tale rafforzamento, si legge, deve avvenire "in piena complementarità con la NATO nel quadro concertato del partenariato strategico fra l'UE e la NATO e nel rispetto dell'autonomia e delle procedure decisionali di ciascuno"[49].

Inoltre, per incrementare la sicurezza interna ed esterna all'Unione, il Consiglio ha chiesto l'elaborazione di un "Quadro strategico UE in materia di ciberdifesa" per il 2014, coerentemente con gli sforzi della NATO, su proposta dell'Alto Rappresentante per gli affari esteri e la politica di sicurezza ed in collaborazione con la Commissione e l'EDA.

Nel prosieguo del documento, la ciberdifesa viene presentata come un'area in cui è opportuno favorire un miglioramento delle capacità. Il Consiglio europeo invita gli stati membri, coadiuvati dall'EDA, ad elaborare una tabella di marcia ed una serie di progetti incentrati sulla formazione e sulle esercitazioni; a migliorare la cooperazione civile/militare, sulla base della *Strategia dell'Unione europea per la cibersicurezza*; a proteggere i mezzi utilizzati nelle missioni ed operazioni dell'UE.

Inoltre, il documento fa riferimento al programma "Horizon 2020" per quanto riguarda l'attenzione che questo rivolge alle tecnologie cosiddette *dual-use*, che possono avere un duplice utilizzo, militare e civile. La dimensione cibernetica si presta evidentemente allo sviluppo di questo tipo di tecnologie.

Sulla base di ciò, il Consiglio europeo ha annunciato la prossima definizione di "un'azione preparatoria sulla ricerca connessa alla PSDC"[50].

1.3.4 Risorse tecnologiche

Il progetto presentato nella strategia dipende in modo cruciale anche dall'adeguamento delle risorse industriali e tecnologiche. Di notevole rilievo è il fatto che la maggior parte dei prodotti e servizi ICT utilizzati in Europa siano realizzati altrove. Preso atto dell'attuale assetto del mercato mondiale in questo settore, si rende opportuno lo sviluppo, ad opera della Commissione, di standard di sicurezza e regimi di cer-

[48] Consiglio europeo, *Conclusioni del Consiglio europeo 19 e 20 dicembre 2013 - Politica di sicurezza e di difesa comune*, 19 dicembre 2013.

[49] Ibidem, p. 2.

[50] Ibidem, p. 9.

tificazione volontaria a livello europeo per garantire la sicurezza della catena di approvvigionamento, in particolare nei settori economici critici (sistema industriale di controllo, infrastruttura dell'energia e dei trasporti)[51]. Affinché sia possibile garantire la sicurezza dei prodotti ICT usati in Europa, quindi, si rende necessario controllare ogni singola fase della catena produttiva, con tutte le problematiche connesse alla dislocazione di esse in diverse aree del mondo.

Questa necessità è stata affermata anche da David Francis, chief security officer della Huawei UK, che in un suo intervento dell'ottobre 2013[52] ha sottolineato l'importanza, anche per il settore industriale, di una continua attività di controllo della catena produttiva, così che ogni componente del prodotto rispetti determinati standard di sicurezza, stabiliti ed uniformemente applicati a livello europeo. Gli standard di sicurezza contribuirebbero ad accrescere il livello di fiducia nei prodotti ICT e, di conseguenza, il grado di protezione dei dati personali; ma perché questo avvenga è necessario investire nell'R&S e nell'innovazione.

1.3.5 International cyberspace policy

L'ultima priorità della strategia riguarda la cooperazione internazionale per la creazione di un dossier di raccordo per lo spazio cibernetico. La proiezione della questione cyber nelle relazioni esterne dell'Unione consentirebbe a quest'ultima di allacciare rapporti e stringere partenariati con attori internazionali, statali e non, attivi in questo settore. Tra le cooperazioni auspicate, la strategia include quelle con Consiglio d'Europa, OCSE, Nazioni Unite, OSCE, NATO, Unione africana, ASEAN e OSA. Una particolare attenzione viene poi rivolta alla cooperazione bilaterale con gli Stati Uniti, in special modo attraverso il Gruppo di lavoro UE-Stati Uniti su cybersecurity e cybercrime, istituito in occasione del vertice annuale UE-Stati Uniti del 2010. È significativo che nel corso di tale vertice, che dal 1990 costituisce un punto di forza della partnership transatlantica, le due potenze abbiano ritenuto importante creare un gruppo di lavoro specifico per la cybersecurity ed il cybercrime, il cui compito è

[51] Commissione europea, *Strategia dell'Unione europea per la cibersicurezza*, cit., p. 14.

[52] Intervento di David Francis al convegno "Cybersecurity & International Relations", organizzato a Roma il 14 ottobre 2013 nell'ambito del Festival della Diplomazia.

preparare il dialogo ed il confronto in sede di vertice ufficiale. Ciò prova che questi temi sono entrati nella lista delle loro priorità.

Per quanto riguarda, invece, l'elaborazione di un dossier di raccordo internazionale, la strategia non auspica l'elaborazione di nuovi strumenti di diritto internazionale riferiti al cyber, ma che siano estese portata ed campo di applicazione di tre documenti specifici già in essere: il Trattato internazionale sui diritti civili e politici, la Convenzione europea dei diritti dell'uomo e la Carta dei diritti fondamentali dell'uomo. L'impegno dell'Unione dovrebbe volgere verso l'attuazione delle disposizioni ivi contenute, anche nel cyber spazio.

Infine, la strategia segnala la rilevanza della Convenzione di Budapest sul cybercrime del 2001, promossa dal Consiglio d'Europa e firmata da 52 paesi. Ad oggi la Convenzione è stata ratificata da 41 stati, dei quali 23 sono membri dell'UE[53]. La strategia definisce la Convenzione un importante strumento aperto alla firma anche di paesi terzi; un modello per l'adozione di norme e regole nazionali ed un simbolo della volontà di cooperare a livello internazionale.

1.3.6 Ruoli e responsabilità

L'ultima parte della strategia riguarda la questione dei ruoli e delle responsabilità. In particolare, il documento cerca di individuare i principali organi di riferimento per la cybersecurity in Europa e di incentivare la creazione di organi nazionali *ad hoc* per la sicurezza delle reti, il *law enforcement* e la *defence*. Secondo quanto si legge, tutti gli organi competenti dovrebbero rimanere costantemente in contatto tra loro, instaurando anche delle collaborazioni esterne con l'industria e l'università, per garantire un continuo e proficuo scambio di informazioni.

Nella parte conclusiva del documento una nota tratta la questione del finanziamento della strategia, che dipenderà dai singoli bilanci stabiliti per ciascuna area di *policy* rilevante, secondo quanto stabilito dal Quadro finanziario pluriennale 2014-2020.

L'aspetto del finanziamento rimane uno dei più complessi e dibattuti, non solo a livello europeo, ma anche a livello nazionale. In generale, sono pochi gli stati che hanno deciso di stanziare somme cospicue per la

[53] I paesi UE che non hanno ancora ratificato la convenzione sono Grecia, Irlanda, Lussemburgo, Polonia e Svezia . Si veda: http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG.

cybersecurity e tra questi, in Europa, vi è il Regno Unito. Nel 2010 il paese ha destinato 650 milioni di sterline ad un programma quadriennale interamente dedicato ad incrementare le capacità nazionali di cyberscurity. Ulteriori 210 milioni di sterline sono stati confermati per il biennio 2015-2016.

Riguardo all'Italia, nel DPCM del 24 gennaio 2013 non viene invece fatto alcun riferimento alla questione del finanziamento nel disegnare l'architettura istituzionale della cybersecurity. L'articolo 13.1 stabilisce infatti che "dal presente decreto non derivano nuovi oneri a carico del bilancio dello Stato".

In generale, è ovvia la necessità di predisporre di fondi adeguati per la buona riuscita di una politica di sicurezza; e questo vale anche per la dimensione cibernetica. Pertanto, la questione dei finanziamenti necessiterebbe una maggiore definizione, sia a livello europeo sia a livello nazionale, considerata la sua vitale importanza.

Il testo della *Strategia dell'Unione europea per la cibersicurezza* si chiude con la previsione di un importante appuntamento per il 2014: l'organizzazione da parte della Commissione e dell'Alto Rappresentante di una conferenza che riunisca tutti i soggetti interessati, per monitorare ed assicurare la corretta implementazione della strategia a 12 mesi dalla sua approvazione. La conferenza si è svolta a Bruxelles il 28 febbraio 2014, ed ha visto la partecipazione di importanti attori istituzionali, quali Neelie Kroes, vice presidente della Commissione per l'Agenda digitale, e Paul Timmers, direttore della Direzione Sustainable & Secure Society della DG CONNECT della Commissione europea.

In questa occasione è stata presentata una tabella di valutazione del livello di implementazione della strategia[54], strutturata in due macro-obiettivi: il conseguimento della ciberresilienza e la drastica riduzione del cybercrime. Il primo macro-obiettivo ricomprende due sotto-obiettivi: l'incremento della sicurezza delle reti e dell'informazione e la diffusione di una relativa cultura generale. Il secondo macro-obiettivo ne ricomprende tre: la predisposizione di una legislazione forte ed efficace, il miglioramento delle capacità operative per il contrasto al crimine informatico e la promozione della cooperazione a livello europeo.

[54] European Commission, *Table on the Implementation of the "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace"* (JOIN(2013)1), 28 February 2014.

La tabella mette in evidenza i progressi conseguiti e le lacune da colmare, ma sopratutto testimonia l'impegno dell'Unione europea nel cominciare ad affrontare adeguatamente e sistematicamente la questione della cybersecurity, destinata a ricoprire un ruolo centrale nelle future politiche comunitarie di sicurezza.

La strategia cyber per l'Europa costituisce una svolta dal punto di vista normativo, poiché rappresenta il primo ed unico documento strategico europeo dedicato alla questione della cybersecurity e propone una serie di principi e valori chiave, necessari per la messa in atto delle azioni da intraprendere. In un panorama europeo nel quale non tutti gli stati membri si sono dotati di una propria strategia nazionale, l'Unione tenta di stimolare l'attenzione verso questa nuova sfida crescente ed aumentare le competenze generali, così da non trovarsi impreparata in caso di crisi. Perché questo avvenga, è necessario in primo luogo che tutti gli stati comincino a considerare il dominio cyber alla stregua di quello fisico, predisponendo e, conseguentemente, imponendo le adeguate misure di sicurezza. Infatti, considerare i due domini allo stesso livello significa anche ammettere un intervento coercitivo dello Stato, affinché questo possa imporre regole specifiche in materia.

Allo stato attuale, esistono svariate e considerevoli differenze a livello europeo, per cui la strategia si inserisce nell'attività più ampia dell'Unione di favorire un dialogo tra tutte le parti ed incoraggiare la diffusione delle buone pratiche. A stati particolarmente avanzati dal punto di vista cyber - come Regno Unito, Francia, Germania, Estonia e Paesi Bassi - si contrappongono stati in cui questa tematica risulta meno adeguatamente affrontata.

L'Italia non compare nella lista dei favoriti, ma il 2013 ha segnato una svolta con l'approvazione, il 24 gennaio, del DPCM *Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale* e, il 18 dicembre, del *Quadro strategico nazionale per la sicurezza dello spazio cibernetico* e del *Piano nazionale per la protezione cibernetica e la sicurezza informatica* (si veda paragrafo 2.5).

Questi documenti hanno inaugurato un impegno italiano sempre più importante nel settore, in linea con quanto auspicato/richiesto dall'UE. Unitamente alla *Strategia dell'Unione europea per la cibersicurezza*, l'UE ha approvato anche una proposta di direttiva "recante misure volte a garantire un livello comune elevato di sicurezza delle reti e dell'informazione nell'Unione". La proposta di direttiva costi-

tuisce la "misura principale"[55] della strategia ed ha come scopo quello di sostenere il funzionamento delle società e delle economie dei paesi membri, considerato il peso che la NIS ricopre nella creazione di un mercato mondiale dei servizi che sia affidabile.

Tutto sembra andare nella direzione di un progressivo rafforzamento degli strumenti finora posti in essere e di una parallela predisposizione di nuove misure a scopo integrativo. Anche il regolamento 526/2013 del maggio 2013, con il quale si è proceduto all'estensione e al rafforzamento del mandato dell'ENISA, costituisce un'ulteriore prova dell'intento dell'UE di farsi sempre più capace di fronteggiare le nuove minacce provenienti dallo spazio cibernetico, inserito ormai a pieno titolo nelle varie dimensioni del conflitto. Infatti, si parla di una "quinta" dimensione, dopo quelle della terra, del mare, dell'aria e dello spazio: il cyberspace rappresenta oggi l'evoluzione dei terreni d'azione dell'uomo ed in quanto tale si presta al crimine, al terrorismo e alla guerra. In quest'ambito, acceso è il dibattito sul cosiddetto "cyber warfare". Soprattutto dopo gli attacchi rivolti contro l'Estonia nel 2007 e la Georgia nel 2008, questo tema è divenuto un argomento saliente del dibattito internazionale: in particolare, si discute se far rientrare questo tipo di attacchi nella fattispecie dell'articolo 5 del Trattato istitutivo dell'Alleanza Atlantica, consentendo così alla NATO di intervenire in legittima difesa collettiva contro lo stato "aggressore" o contro lo stato che non vigila sull'operato lesivo di un proprio cittadino o comunque su un operato lesivo svolto dal proprio territorio. La questione è complessa ed esula dal presente studio, ma è importante sottolineare che, ad oggi, non si è proceduto ad un riconoscimento in tal senso, nonostante le forti pressioni esercitate da parte dell'Estonia e di alcuni altri paesi.

Forse vedremo comparire questo nuovo aspetto del cyber nei futuri documenti dell'Unione, ma al momento sembra più opportuno e realistico auspicare una maggiore definizione degli strumenti di cybersecurity, al fine di agire prontamente ed efficacemente per la messa in sicurezza delle reti e delle informazioni digitalizzate.

---

[55] Commissione europea, *Proposta di direttiva recante misure volte a garantire un livello comune elevato di sicurezza delle reti e dell'informazione nell'Unione* (COM(2013)48), 7 febbraio 2013, p. 2.

1.4 Organi rilevanti

L'Unione europea ha progressivamente incaricato determinati propri organi ed agenzie di occuparsi della questione della cybersecurity, procedendo all'assegnazione di compiti specifici in merito. Allo stato attuale i più rilevanti sono:

- Commissione europea;
- Alto Rappresentante per gli affari esteri e la politica di sicurezza;
- ENISA;
- EDA;
- EC3;
- CERT-EU.

La Commissione e, solo recentemente, anche l'Alto Rappresentante svolgono un ruolo importante nell'elaborazione di proposte e nella preparazione di documenti ufficiali riguardanti la cybersecurity: la strategia di sicurezza cibernetica del 2013 è, come riportato, un prodotto del loro lavoro congiunto.

La Commissione, in particolare, è stata protagonista dei primi documenti ufficiali dell'Unione in ambito cyber (si veda paragrafo 1.1), contribuendo in maniera significativa all'evoluzione di questa tematica. Inoltre una Direzione generale della Commissione – quella per le Reti di comunicazione, contenuti e tecnologia (CNET), detta DG CONNECT – è specificamente dedicata allo sviluppo delle tecnologie dell'informazione e delle comunicazioni, al fine di aumentare i posti di lavoro e favorire la crescita economica in Europa.

La DG CONNECT partecipa al finanziamento del progetto "Cybersecurity, privacy and trustworthy ICT: research and innovation", nell'ambito del programma "Horizon 2020", con un bilancio di circa 136 milioni di euro per il biennio 2014-2015, da confermare a fine 2014.

Una fondamentale agenzia europea per la cybersecurity è l'ENISA, di cui si è già detto in precedenza. Ricordiamo che l'ENISA rappresenta il punto di riferimento principale per il coordinamento delle politiche cyber nazionali, proponendosi come tramite europeo ed attivatore di dialogo. È rilevante mettere in evidenza l'impegno dell'Agenzia nel promuovere il progresso delle capacità tecnologiche, condizione essenziale per una risposta adeguata agli attacchi di natura cibernetica. Questo impegno si traduce nella costruzione di un rapporto solido con i vari Governi nazionali e nell'organizzazione di esercitazioni.

Si è già riportato che le esercitazioni costituiscono un modo molto importante di rafforzare la cooperazione, consentendo all'UE e alla comu-

nità internazionale di riunire i maggiori esperti in ambito cybersecurity, sottoponendo loro complicati esempi di attacchi cibernetici, così da testare il grado di competenze acquisite e stimolare l'apprendimento secondo la tecnica del *learn by doing*. Le esercitazioni di questo tipo rientrano nella categoria dei cosiddetti *serious game*, ideati per consentire al personale coinvolto di accrescere le proprie abilità ed affinare le proprie strategie, attraverso la simulazione di eventi di crisi potenzialmente realizzabili nella realtà. I *serious game* possono trovare applicazione sia in ambito civile sia in ambito militare; quelli cyber si collocano a metà strada tra questi due ambiti, in linea con il duplice scopo a cui possono essere destinati, a cui si accennato in precedenza.

Durante le esercitazioni non ha alcuna importanza la nazionalità degli esperti, poiché tutti lavorano egualmente all'interno di una piattaforma, utilizzando modelli comuni di conoscenza. Ciò significa che, dopo ogni esercizio, il metodo di risoluzione che si rivela migliore diventa automaticamente il modello base per affrontare problemi più complessi. Tale metodo viene messo immediatamente a completa disposizione di tutti gli altri partecipanti, i quali possono così sfruttare il *know how* altrui per apportare il proprio contributo nello *step* successivo. Il metodo consente di raggiungere in tempo reale la soluzione più efficace, attraverso la piena condivisione dell'*expertise* a disposizione.

A livello europeo due esercitazioni sono state organizzate dall'ENISA ed altre dal Cooperative Cyber Defence Centre of Excellence di Tallinn (CCD COE). Tale centro è stato inaugurato nel maggio 2008 e ha ottenuto pochi mesi dopo il patrocinio della NATO ed il riconoscimento dello *status* di organizzazione militare internazionale. È importante sottolineare che il CCD COE non è una struttura della NATO o dell'UE, ma un centro sorto per iniziativa dello stato estone, che dal 2003 ha esercitato molte pressioni per ottenerne il patrocinio da parte dell'Alleanza Atlantica.

Il centro svolge oggi un ruolo particolare per quanto riguarda la formazione e l'addestramento dei tecnici/analisti informatici in materia di cybersecurity. Dal 2012 le esercitazioni organizzate dal CCD COE prendono il nome di "*Locked Shields*" e si svolgono con cadenza pressoché annuale. L'ultima risale all'aprile del 2013 e, stando al relativo rapporto, ha messo in evidenza un sostanziale progresso delle squadre coinvolte rispetto alla precedente edizione del 2012[56].

[56] Cooperative Cyber Defence Centre Of Excellence (CCD COE), *Cyber Defence exercise Locked Shields 2013. After Action Report*, Tallinn, 2013, http://www.ccdcoe.org/locked-

Sempre secondo la logica dei *serious game*, più squadre hanno preso parte all'esercitazione, la quale è stata organizzata in modo tale che le "squadre blu" dovessero cooperare tra loro per rispondere a svariati attacchi da parte della "squadra rossa". Ogni squadra blu era composta da una serie di esperti IT e da due consulenti legali, aventi lo scopo di garantire il rispetto del diritto.

Lo scenario prevedeva il dispiegamento di un certo numero di squadre, dietro mandato delle Nazioni Unite, a sostegno del governo di uno stato fittizio (Boolea), il quale si trovava a dover fronteggiare un'aspra guerra civile ed aveva chiesto l'intervento della comunità internazionale. Compito delle squadre blu era rispondere agli attacchi di natura cibernetica rivolti contro i sistemi IT delle organizzazioni di aiuto locali e preservare l'integrità dei network militari. Le squadre avevano inoltre l'obbligo di tenere costantemente aggiornato il quartier generale, eseguire gli ordini da questo provenienti, e rispondere ai media. Paragonata all'esercitazione ENISA del 2012, la Locked Shield 2013 ha presentato problemi/esercizi più complessi e diversificati, soprattutto dal punto di vista dei *task*. L'introduzione di due elementi aggiuntivi, i consulenti legali per gli aspetti del diritto e i media per l'opinione pubblica, ha permesso di rendere lo scenario più completo e realistico.

Secondo il rapporto dell'esercitazione del 2013, le squadre hanno riportato notevoli successi nelle attività di "preventing", "detecting" e "mitigating" degli attacchi, in confronto ai precedenti eventi.

Numerose altre esercitazioni sono state organizzate negli ultimi anni da altri attori internazionali, quali la NATO e gli Stati Uniti; ma quello che preme mettere in rilievo è che questa pratica va via via consolidandosi da circa 3 anni. Prima del 2010, infatti, non si registrano molti eventi del genere, in ogni caso caratterizzati da un tasso relativamente basso di partecipazione.

La pratica delle esercitazioni si rivela molto significativa sia per la messa a fattor comune delle competenze informatiche sia perché costituisce l'occasione di una cooperazione internazionale. Eventi simili dovrebbero essere organizzati anche su scala nazionale, anche per permettere una più stretta collaborazione tra il settore pubblico e quello privato.

Dal 2012 l'Italia organizza annualmente un'esercitazione nazionale denominata "CybIt", la quale, nella sua ultima edizione, ha visto anche la

---

shields-2013.html.

partecipazione di attori privati operanti nel settore energetico (si veda paragrafo 2.1). Si auspica che questa pratica venga consolidata negli anni a venire, con un coinvolgimento più ampio del settore privato.

Inoltre, sempre in Italia, si sta pensando di creare una sorta di "Battle Lab", grazie all'operato del Comando C4 Difesa, delle Forze Armate e di altri rilevanti *stakeholder*, così da permettere l'esercizio continuativo del personale in questione[57]. Quest'attività è stata già realizzata in alcuni paesi, come Stati Uniti e Regno Unito, che hanno già inaugurato le proprie "*cyber unit*".

A partire da ottobre 2013, il Ministero della Difesa britannico ha lanciato una campagna di reclutamento per la costituzione di una futura "*Joint Cyber Reserve*", la quale avrà come obiettivo quello di garantire la sicurezza cibernetica entro i confini nazionali. Il personale invitato ad offrire la propria candidatura non deve necessariamente provenire dalle fila dell'apparato militare; anzi, le probabilità di coinvolgere esperti informatici al di fuori dell'ambiente militare sono più che elevate ed auspicate, dal momento che in ambito cyber una sinergia civile/militare si rende necessaria.

A livello europeo, la costituzione di queste capacità aggregate e strutturate in ambito cibernetico potrebbe rappresentare un buon anello di congiunzione tra gli stati membri e le istituzioni UE, tra le quali l'ENISA giocherebbe un ruolo primario.

L'Agenzia europea di difesa ha il compito di delineare la cyberdefence all'interno delle politiche di sicurezza europee. La stessa strategia di sicurezza cibernetica afferma che "le attività a favore della cibersicurezza nell'Unione europea coinvolgono anche la dimensione della ciberdifesa" e che, come già riportato, "lo sviluppo di capacità di ciberdifesa dovrebbe concentrarsi sulle attività di individuazione, risposta e recupero nei confronti di ciberminacce sofisticate"[58].

---

[57] Secondo Umberto Maria Castelli, comandante del Comando C4 Difesa del Ministero della Difesa, il "Battle Lab" dovrebbe svolgere la funzione di una vera e propria "palestra per addestrare un futuro esercito del cyber spazio". Dichiarazione rilasciata da Castelli in occasione del seminario "Cooperare per crescere nella sicurezza", organizzato a Roma il 25 ottobre 2013 dall'Istituto superiore delle comunicazioni e delle tecnologie (ISCOM).

[58] Commissione europea, *Strategia dell'Unione europea per la cibersicurezza*, cit., p. 12.

Nonostante, quindi, le problematiche associate a questo concetto, la *sicurezza* e la *difesa* del dominio cyber sono presentate nella strategia come due facce della stessa medaglia. L'EDA ha perciò il compito di promuovere lo sviluppo delle *capabilities* di cyberdefence a livello europeo, a cominciare dai singoli stati.

L'agenzia ha commissionato alla Rand Corporation un'analisi dello sviluppo delle suddette *capabilities* in 20 stati membri, 20 nello specifico, dal punto di vista. Lo studio, pubblicato nel marzo 2013, ha evidenziato "un quadro complesso e diversificato" sia a livello UE che all'interno dei 20 paesi presi in esame[59]. Il rapporto completo, con i profili dettagliati di questi paesi, è classificato ma dalla parte resa pubblica si evince che gli stati con maggiore familiarità con la cybersecurity sono anche quelli con *capabilities* più avanzate nel settore della difesa. Specificamente, gli aspetti di *leadership*, *personnel* e *interoperability* risultano abbastanza consolidati; mentre quelli di *doctrine*, *organisation* e *training* si trovano ancora ad un primo stadio di maturità. L'aspetto *facilities*, poi, appare indubbiamente quello più complesso e il suo sviluppo è stato definito pressoché inesistente. Lo studio propone infine l'elaborazione, nel breve-medio periodo, di una "Roadmap for strengthening Cyber Defence in CSDP"[60].

A tale proposito ricordiamo che il Consiglio europeo del dicembre 2013 ha richiesto l'elaborazione entro il 2014 di un "Quadro strategico UE in materia di ciberdifesa", da realizzare su proposta dell'Alto Rappresentante ed in collaborazione con la Commissione e l'EDA (si veda paragrafo 2.3).

Gli ultimi due organi rilevanti sono l'EC3 ed il CERT-EU, rispettivamente deputati alle risposte al cybercrime e ai cyber attack. Entrambi sono nati nel 2012 e sono divenuti operativi a partire dal 2013, per cui il loro reale apporto sarà valutabile solo quando avranno raggiunto maggiori livelli di operatività. Quello che è certo è che la loro realizzazione si è presentata come una componente necessaria, anche se non sufficiente, per la corretta gestione della cybersecurity. L'EC3 ed il CERT-EU rappre-

---

[59] Sophie-Charlotte Brune et al., *Stocktaking study of military cyber defence capabilities in the European Union (milCyberCAP. Unclassified Summary*, Santa Monica, Rand, 2013, p. 6, http://www.rand.org/pubs/research_reports/RR286.html.

[60] European Defence Agency (EDA), *Factsheet Cyber Defence*, 19 November 2013, http://www.eda.europa.eu/info-hub/publications/publication-details/pub/factsheet-cyber-defence.

sentano, infatti, gli organi tecnici operativi dell'Unione, con il compito di rispondere concretamente ed efficacemente alle crisi di natura cibernetica. Il loro operato è, inoltre, fondamentale per il raccordo e la collaborazione con i loro corrispettivi nazionali, ove esistenti.

Dell'EC3 segnaliamo uno studio redatto in collaborazione con l'International Cyber Security Protection Alliance (ICSPA) e pubblicato nel 2013 che offre una panoramica dei possibili sviluppi del crimine informatico negli anni a venire. L'obiettivo è anticipare il futuro del cybercrime, consentendo a governi, imprese e cittadini di prepararsi per le sfide e le opportunità del prossimo decennio[61]. Lo studio afferma che "cybercrimes in 2020 will be adaptations of existing crimes to the technological developments of the next seven to eight years. […] Evolved threats to critical infrastructure and human implants will increasingly blur the distinction between cyber and physical attack"[62].

Il documento considera inoltre la possibilità che nuovi crimini informatici possano, in futuro, causare danni psicologici alle vittime e prevede che la natura evoluta e maggiormente complessa del cybercrime richiederà una migliore definizione dei ruoli e delle responsabilità degli organi incaricati di indagare e combattere queste minacce. Lo studio propone quindi la messa in atto di procedimenti giudiziari o "quasi-giudiziari" nei confronti non solo degli autori degli attacchi, ma anche delle organizzazioni oggetto di attacchi, siano esse pubbliche o private. A queste spetterebbe infatti il dovere di ripristinare i servizi - pena il pagamento di sanzioni - e di applicare norme per la prevenzione del crimine. Oltre a offrire un ampliamento della categoria dei crimini informatici, lo studio ha il pregio di evidenziare l'importanza dello sviluppo di adeguati meccanismi di *law enforcement*, per assicurare una corretta gestione del rischio e del danno, da parte di tutte le organizzazioni interessate.

Le istituzioni e gli organi dell'Unione descritti in questo paragrafo sono, attualmente, quelli maggiormente rilevanti per quanto riguarda la cybersecurity in Europa, ma è prevedibile che il panorama possa mutare negli anni a venire.

---

[61] Europol and ICSPA, *Project 2020. Scenarios for the future of Cybercrime*, 25 September 2013, p. 3, https://www.europol.europa.eu/content/project-2020-scenarios-future-cybercrime.

[62] Ibidem, p. 7.

1.5 Elementi critici

È importante mettere in evidenza come la strategia europea di sicurezza cibernetica non arrivi a definire il lato più squisitamente tecnico/operativo della cybersecurity, ma ne stabilisca solo le linee essenziali, in linea con gli scopi ed obiettivi di ogni documento strategico. Il documento, infatti, enuncia i valori chiave alla base dell'approccio europeo e le buone pratiche da seguire per raggiungere dei risultati significativi. *Core values* e *good practices* rappresentano le priorità europee in materia ed il punto di partenza per agire.

Quanto ai valori chiave, la strategia stabilisce l'importanza di agire sempre secondo un sentimento di responsabilità condivisa, il quale consenta di trattare la cybersecurity come una questione di portata globale. Essenziale, infatti, è l'adozione di una prospettiva che valichi i confini nazionali e quelli europei, affinché la cooperazione internazionale possa essere efficace, in considerazione della natura tendenzialmente *borderless* delle problematiche cibernetiche. Proprio il concetto di cooperazione è alla base dell'intero documento. Tale cooperazione è intesa sia a livello nazionale, per ciò riguarda la creazione di partnership pubblico-private; sia a livello europeo, con riferimento all'importanza per gli stati e per le rilevanti istituzioni ed agenzie dell'UE di comunicare ed agire insieme nell'ambito dell'Unione; sia, infine, a livello internazionale, con altri attori statali e non. Questa priorità rappresenta il *landmark* della strategia cyber dell'UE.

Affinché la cooperazione sia realizzabile, è opportuno che tutte le parti coinvolte sostengano e promuovano la creazione di strumenti di *confidence building*, basati sulla trasparenza e sull'*information sharing*. Proprio quest'ultimo punto si rivela una condizione imprescindibile per la buona riuscita di una politica di cybersecurity, anche se, purtroppo, di non facile realizzazione.

Lo scambio delle informazioni resta un argomento piuttosto ostico, soprattutto in tema di sicurezza. La diffidenza che esiste non solo tra stati sovrani, ma anche tra singolo stato ed imprese private, spinge le parti a rifuggire dal dialogo aperto e ad optare per la non condivisione delle informazioni. Tale scelta viene sempre percepita come un vantaggio sugli altri, secondo una logica realistica in cui il conflitto caratterizza la vera natura dei rapporti, siano essi tra individui o tra stati. Appare dunque molto difficile favorire il diffondersi su vasta scala di comportamenti collaborativi, ma non bisogna dimenticare che a volte cooperare in

un ambito nuovo può apparire molto più semplice che cercare un'intesa in un ambito tradizionalmente complicato.

Il cyber ha dalla sua parte la relativa novità. In una situazione generale in cui tutti gli attori principali cominciano a rapportarsi con una problematica per la prima volta, ci sono buone probabilità che questi decidano di operare insieme, per trarne reciproco vantaggio. Ora, è vero che non tutti gli attori si trovano nella stessa situazione - anzi, molte e significative sono le differenze in questo senso - ma è anche vero che nessuno si trova in possesso dell' "arma nucleare" in grado di tenere tutti gli altri sotto scacco. La scelta cooperativa potrebbe rivelarsi non impossibile, come dimostrano le sempre più frequenti occasioni di incontro tra stati, organizzazioni internazionali e compagnie private.

Attualmente, in Europa, l'*information sharing* può essere definito unidirezionale: non esiste un obbligo per le autorità di fornire informazioni al settore privato, il quale, al contrario, ha il dovere di fare rapporto alle autorità. A questo proposito, Troels Oerting, direttore dell'EC3, ha affermato nel marzo 2013 che il meccanismo di *info sharing* in Europa dovrebbe assomigliare a quello statunitense, essere cioè una strada a doppio senso, in cui le informazioni fluiscono in ambedue le direzioni[63].

1.6 Elementi valutativi

Vi è un altro aspetto problematico della cooperazione: il dominio cyber è per sua natura difficilmente contenibile all'interno di confini precisi, anche se le opinioni al riguardo divergono. È piuttosto diffusa l'idea secondo la quale il cyber costituirebbe un "*global common*". I sostenitori di questa tesi considerano lo spazio cibernetico come un bene comune, in quanto tale sottoposto al regime di *res communis omnium*, che presuppone l'inappropriabilità del bene e la sua libertà d'uso[64].

---

[63] Intervento di Troels Oerting al dibattito "What next for European cyber-security?", organizzato a Bruxelles il 19 marzo 2013 dalla Security & Defence Agenda (SDA). SDA, *Cyber-security: Problems outpace solutions*, December 2013, p. 9, http://www.securitydefenceagenda.org/Contentnavigation/Library/Libraryoverview/tabid/1299/articleType/ArticleView/articleId/3620/categoryId/62/Cybersecurity-Problems-outpace-solutions.aspx.

[64] Roberta Pisa, "L'accesso ad internet: un nuovo diritto fondamentale?", in *Treccani Magazine*, 7 gennaio 2010, http://www.treccani.it/magazine/diritto/approfondimenti/diritto_internazionale_e_comparato/2_Pisa_internet.html.

Il dibattito sul tema è molto acceso ed alcuni non condividono questa impostazione, sopratutto in considerazione del fatto che il cyber spazio risulta in larghissima parte posseduto da privati. Gli aspetti regolativi di Internet, ad esempio, sono interamente appannaggio di un ente internazionale no-profit, l'ICANN (International Corporation for Assigned Names and Numbers). L'ICANN ha il compito di gestire l'assegnazione degli indirizzi IP, nell'ambito del sistema di nome di dominio (DNS). Da un lato l'assegnazione di un codice identificativo per ogni singolo dispositivo elettronico permette ai computer di rintracciarsi ed interagire tra di loro; dall'altro lato l'assegnazione dei domini "com", "net" oppure "org" consente agli utenti di individuare i siti web. Il DNS è quindi alla base del funzionamento di internet, e l'immenso potere di controllo e gestione di questo sistema è appartenuto fino ad oggi a questo ente internazionale, in seguito ad un contratto stipulato con il Dipartimento per il Commercio degli Stati Uniti.

Quanto detto sopra è in contrasto con la tesi del cyber spazio inteso come *global common* ed apre ad uno scenario più complesso, non esente dalle logiche di competizione per il "comando e controllo".

La questione della natura dello spazio cibernetico è tuttora molto discussa, mal prestandosi ad un suo inquadramento nei principi tradizionali di diritto internazionale. In particolare, l'apparente mancanza di fisicità del cyber space rende difficile l'applicazione di concetti tipici del diritto del mare e del diritto dello spazio (luna e corpi celesti), aprendo a nuove possibilità di definizione ancora non previste a livello giuridico.

Stefano Silvestri, past president dell'Istituto Affari Internazionali, in un intervento del febbraio 2012[65] ha precisato che un *global common* può essere dichiarato tale solo qualora sia regolato dal diritto internazionale generale. In caso contrario il bene rimane "globale", ma non può essere considerato comune. Secondo Silvestri un ciberspazio del tipo *global common* non è compatibile con le logiche nazionali di competizione per l'acquisizione di una superiorità strategica in questo campo. Tanto meno gli stati sembrano intenzionati a firmare una nuova Convenzione inter-

[65] Stefano Silvestri, *Speaking notes*, documento NIAG a Finmeccanica su Cyber security e cooperazione internazionale, 6 febbraio 2012 (mimeo). Il NIAG (NATO Industrial Advisory Group) è un gruppo consultivo per gli aspetti industriali della Conferenza dei direttori nazionali degli armamenti (CNAD) della NATO e dei principali gruppi di armamenti, a cui ha preso parte una delegazione italiana di rappresentanti delle principali aziende nazionali operanti in vari settori tecnologici della difesa.

nazionale in difesa della natura comune dello spazio cibernetico. Appare pertanto difficile sostenere la tesi che il dominio cyber costituisca un *global common*.

Una tesi diversa è sostenuta da James Andrew Lewis, direttore del programma Tecnologie strategiche del Center for Strategic and International Studies (CSIS). In un intervento del settembre 2011 Lewis ha sostenuto che lo spazio cibernetico non può essere considerato un *common*, ma piuttosto un "condominio", in cui tutti i proprietari condividono la stessa struttura, dotata di poche regole e di un debole organo di governo[66]. Secondo Lewis il cyber spazio possiede dei confini entro i quali gli stati si sentono, o si sentiranno tra breve, legittimati a rivendicare la propria sovranità. Alcuni governi hanno infatti paragonato il ciberspazio al mare territoriale, accessibile dall'esterno ma soggetto al proprio controllo. L'estensione della sovranità nazionale al dominio cibernetico avrebbe come conseguenza quella di ridefinirne l'architettura, con le sue regole e la sua *governance*. A parere di Lewis, questa prospettiva si rivela molto più probabile di quanto possa sembrare.

Kamlesh Bajaj, amministratore delegato del Data Security Council of India (DSCI), ha affermato in un articolo del giugno 2012 che lo spazio cibernetico è allo stesso tempo un *global common* ed una risorsa nazionale[67]. Secondo Bajaj, si tratterebbe, infatti, di un bene comune di nuovo tipo, ancora privo di un regime formale di regolamentazione, ma in grado di offrire una vasta gamma di servizi a cittadini. Ciò dovrebbe spingere i governi a concludere accordi internazionali in questo campo, che non necessariamente debbono assumere la forma di trattati, considerata la persistente generale difficoltà nel comprendere appieno le dinamiche del ciberspazio.

Il dibattito sulla natura dello spazio cibernetico è tutt'altro che teorico, essendo alla base della cooperazione internazionale. È quindi prioritario chiarire le intenzioni della comunità internazionale in riferimento alla gestione della *governance* della dimensione cibernetica: la cooperazione internazionale è possibile solo in un'ottica di approccio *multi-stakeholder*,

---

[66] James Andrews Lewis, *Rethinking Cybersecurity. A Comprehensive Approach*, Speech at the Sasakawa Peace Foundation, Tokyo, 12 September 2011, http://csis.org/node/32513.

[67] Kamlesh Bajaj, "Globar cyber commons. Addressing cyber security issues", in *Neurope*, 3 June 2012, http://www.neurope.eu/node/114509.

basato sulla partecipazione attiva di tutti gli attori interessati, pubblici e privati.

La strategia europea di sicurezza cibernetica ha gettato le basi per un'auspicata evoluzione verso una più articolata politica europea di cybersecurity, che stabilisca chiaramente le regole da rispettare ed istituisca precisi meccanismi di comunicazione tra le parti.

Si discute in particolare sull'eventualità di stabilire degli standard o *security label* a livello europeo, validi in tutti gli stati membri. Il testo della strategia afferma l'importanza di stabilire "norme di sicurezza promosse dall'industria"[68] in virtù del *know how* consolidato posseduto dal settore privato in questo campo. Tale atteggiamento potrebbe rivelarsi significativo se affiancato da un'efficace attività di regolamentazione da parte delle istituzioni politiche. Comincia a farsi strada l'idea che sia necessario un intervento pubblico più coercitivo, sia a livello nazionale che europeo. Secondo questa prospettiva, spetterebbe all'Unione stessa il compito di fissare degli standard obbligatori di sicurezza e di predisporre tutte le misure atte a garantire una costante collaborazione tra il settore pubblico e quello privato e tra i governi e le istituzioni europee. Le opinioni al riguardo, però, divergono: oltre alla suddetta impostazione, c'è chi sostiene che la cybersecurity sia essenzialmente un processo auto-generantesi appannaggio del solo settore privato e chi crede che gli standard di sicurezza debbano essere fissati a livello globale e non regionale[69].

Quale che sia il livello decisionale, la messa in pratica dei suddetti standard di sicurezza appare, oggi, una priorità per la cybersecurity in generale. In quest'ottica si inserisce anche la necessità di creare un meccanismo di *incident reporting* che sia obbligatorio e non volontario. La questione della resistenza operata dal settore privato potrebbe essere parzialmente risolta tramite l'istituzione dell'anonimato oppure la classificazione di certe informazioni, le quali sarebbero così note solo alle istituzioni governative e non anche al pubblico. Questo punto di vista è stato presentato anche dall'ex Ministro britannico per la sicurezza e la lotta al terrorismo Pauline Neville-Jones, la quale ha affermato: "I would

[68] Commissione europea, *Strategia dell'Unione europea per la cibersicurezza*, cit., p. 14.

[69] Security & Defence Agenda (SDA), *Cyber-security: Problems outpace solutions*, cit., p. 9.

very much like to see a mandatory reporting system with anonymisation and not leading to a criminal investigation in every case"[70].

Neville-Jones, che attualmente ricopre il ruolo di rappresentante speciale del Governo britannico presso il settore industriale per gli affari di cybersecurity, ha inoltre più volte sottolineato l'esigenza di un vero e proprio "mentality shift"[71]: l'obiettivo, afferma, è far sì che i singoli e le aziende vedano la cybersecurity come un "enabler of their business"[72], in considerazione del fatto che i maggiori danni prodotti dal cybercrime sono di natura economica. Affinché ciò sia possibile è importante pensare la cybersecurity al di là delle mere logiche di *business continuity*, in uno sforzo di rinnovata mentalità e atteggiamento costruttivo. Coinvolgere il settore privato significa anche promuovere il concetto di sicurezza funzionale, che si prefigge la continuazione delle funzioni chiave della società moderna. Per inserire la cybersecurity all'interno di questa visione è necessario allontanare il settore privato da un'impostazione individualista e renderlo consapevole dell'impatto del cyber sulla vita economica del paese intero.

Tenendo tutto questo bene a mente, è auspicabile che l'Unione compia presto i prossimi passi nella direzione di una maggiore definizione della politica di cybersecurity e di un potenziamento degli strumenti già posti in essere. In parallelo, è fondamentale che anche gli stati seguano lo stesso esempio, così che tutti i vari livelli di *governance* europea godano di una buona consapevolezza situazionale e di adeguate *capabilities* e procedure.

---

[70] Security & Defence Agenda (SDA), *Where cyber-security is heading*, October 2012, p. 65, http://www.securitydefenceagenda.org/Contentnavigation/Library/Libraryoverview/tabid/1299/articleType/ArticleView/articleId/3412/New-SDA-cyber-report.aspx.

[71] Ibidem, p. 67.

[72] Ibidem, p. 61.

2.
Italia

2.1 Le prime politiche italiane in ambito cyber

Le prime politiche italiane relative all'ICT si sono incentrate sul contrasto al crimine informatico. Nel corso degli anni novanta, l'Italia ha approvato due leggi volte al perseguimento di alcune azioni condotte in rete: la legge n. 547 del 23 dicembre 1993, *Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica* e la legge n. 269 del 3 agosto 1998, *Norme contro lo sfruttamento della prostituzione, della pedopornografia, del turismo sessuale in danno di minori*, la quale ha attribuito all'organo del Ministero dell'Interno deputato alla sicurezza e alla regolarità dei servizi di telecomunicazione – la Polizia postale e delle comunicazioni – il dovere di intraprendere tutte le attività necessarie a contrastare il cybercrime (articolo 14). Le due leggi di cui sopra hanno apportato importanti modifiche al Codice penale e a quello di procedura penale, introducendo in Italia una nuova fattispecie di criminalità: quella informatica.

Nel 2002 l'Italia ha cominciato ad occuparsi anche di protezione delle informazioni in formato digitale, quelle raccolte nei *database* delle pubbliche amministrazioni. Infatti la direttiva del 16 gennaio 2002 sulla *Sicurezza informatica e delle telecomunicazioni nelle pubbliche amministrazioni*, emanata dal Ministro per le Innovazioni e tecnologie di intesa con il Ministro delle Comunicazioni, ha stabilito che "le informazioni gestite dai sistemi informativi pubblici costituiscono una risorsa di valore strategico per il governo del paese"[1] e devono pertanto essere efficacemente protette e tutelate. La direttiva invita le PA ad effettuare un'autovalutazione del livello di sicurezza informatica dei sistemi da esse utilizzati e,

[1] Direttiva del Presidente del Consiglio dei ministri, Dipartimento per l'Innovazione e le Tecnologie, del 16 gennaio 2002 (G.U. n. 69 del 22 marzo 2002).

conseguentemente, ad attivare le iniziative necessarie per posizionarsi su una prestabilita "base minima di sicurezza"[2].

La direttiva del 2002 costituisce il primo documento italiano volto alla tutela dei dati e delle informazioni raccolti dalle PA, considerati strategici per il governo del paese. Essa ha posto le basi per i successivi progressi della Pubblica Amministrazione italiana in materia di sicurezza informatica.

L'anno seguente un decreto del Ministro delle Comunicazioni – emanato il 14 gennaio 2003 di concerto con il Ministro della Giustizia e il Ministro dell'Interno – ha istituito l'Osservatorio permanente per la sicurezza e la tutela delle reti e delle comunicazioni, che ha ereditato tutte le competenze precedentemente attribuite al Gruppo di lavoro sulla sicurezza delle reti e la protezione delle comunicazioni, istituito con il Decreto interministeriale del 21 settembre 1999.

L'osservatorio agisce nell'ambito del Ministero dello Sviluppo economico e, rispetto al precedente Gruppo di lavoro, risulta ampliato dalla partecipazione di alcuni rappresentanti del Ministero della Difesa, del Dipartimento per la Funzione pubblica, del Dipartimento per l'Innovazione e le Tecnologie e del Ministero delle Attività produttive.

L'osservatorio è stato istituito "con la finalità di promuovere interventi normativi, regolamentari ed amministrativi, anche in relazione alle esigenze investigative di competenza dei dicasteri dell'interno e della giustizia"[3].

Dal 2003 l'osservatorio si occupa prioritariamente di alcune attività, tra le quali la predisposizione degli atti in materia di NIS; il controllo sull'adempimento degli obblighi incombenti sugli organismi di telecomunicazione; la facilitazione del processo di attuazione nell'ordinamento italiano delle direttive europee in materia.

Nell'ambito del Ministero dello Sviluppo economico, un altro organo importante opera in materia di sicurezza informatica: l'Istituto superiore delle comunicazioni e delle tecnologie dell'informazione (ISCOM), l'organo tecnico-scientifico del Governo che si occupa di servizi alle imprese, normazione, sperimentazione, ricerca di base e applicata, formazione ed istruzione specializzata nel campo delle telecomunicazioni.

L'istituzione del nucleo originario dell'ISCOM risale ai primi anni del novecento, quando la legge n. 111 del 24 marzo 1907 relativa all'am-

[2] Ibidem, Allegato 2.

[3] Decreto interministeriale del 14 gennaio 2003, art. 1.1

pliamento e miglioramento dei servizi postali, telegrafici e telefonici, fu motivata dall'esigenza di impartire un'istruzione professionale superiore ai funzionari della carriera direttiva, di studiare le proposte per il conseguimento di miglioramenti tecnici nei servizi, di determinare le condizioni tecniche cui deve soddisfare il materiale elettrico e di provvedere al collaudo del materiale stesso[4].

Nello stesso anno, l'Istituto superiore postale e telegrafico, come veniva allora chiamato, fu posto alle dipendenze del Ministro delle Poste e telegrafi. Da allora esso ha subito una serie di trasformazioni organizzative allo scopo di adeguarsi alle costanti evoluzioni del settore delle telecomunicazioni e delle tecnologie dell'informazione.

Oggi l'ISCOM offre il proprio supporto alle imprese operanti nel settore ICT, alle Pubbliche Amministrazioni e all'utenza, svolgendo soprattutto attività di consulenza. Ricopre inoltre un ruolo molto importante per quanto riguarda il rapporto con l'ENISA, agendo da principale interlocutore. L'istituto partecipa alle esercitazioni paneuropee e congiunte UE-Stati Uniti, occupandosi di organizzare quelle nazionali. Il 5 dicembre 2013 si è svolta presso l'ISCOM la seconda esercitazione nazionale di cybersecurity, denominata "CybIt 2013", dopo una prima edizione del giugno 2012[5]. Lo scenario dell'esercitazione del 2013 si è basato sulla simulazione di un attacco cibernetico a più riprese diretto contro alcune imprese operanti nel settore energetico ed alcune altre istituzioni statali, coinvolgendo sia attori pubblici che privati, a differenza dell'edizione precedente. L'obiettivo della "CybIt 2013" è stato quello di valutare l'efficienza dello scambio di informazioni tra istituzioni pubbliche nazionali e settore privato, sulla base dell'architettura delineata per la protezione cibernetica e la sicurezza informatica nazionali, come da DPCM 24 gennaio 2013 (si veda paragrafo 2.5). All'esercitazione hanno partecipato le società ENEL e TERNA. L'aspettativa è che la prossima edizione del 2014

[4] ISCOM, *CybIt 2013: esercitazione nazionale sulla sicurezza informatica*, http://www.isticom.it/index.php/archivio-sicurezza-ict/8-articoli/317-cybit-2013.

[5] In data 19 giugno 2012 si è svolta la prima esercitazione nazionale di sicurezza informatica, denominata "CybIt 2012". Lo scenario prefigurato è stato articolato simulando una serie di attacchi, operati da un gruppo fittizio di cyber criminali, potenzialmente in grado di danneggiare il funzionamento di alcuni siti istituzionali e dei servizi da essi erogati. L'esercitazione ha visto la partecipazione di circa quaranta esperti ICT, provenienti esclusivamente da organismi pubblici. ISCOM, *Cyber Italy 2012: prima esercitazione nazionale sulla sicurezza informatica*, http://www.isticom.it/index.php/archivio-sicurezza-ict/8-articoli/263-cybit-2012.

riesca a coinvolgere un maggior numero di soggetti privati e non solo del settore luce e gas.

Ancora nel 2003 sono stati approvati due rilevanti documenti rispettivamente in tema di protezione dei dati personali e tutela delle comunicazioni elettroniche. Il decreto legislativo n. 196 del 30 giugno 2003, *Codice in materia di protezione dei dati personali*, ha predisposto la disciplina inerente il trattamento dei dati personali che deve essere osservata da chiunque sia stabilito nel territorio dello stato o in altro luogo comunque soggetto alla sua sovranità e da chiunque utilizzi, per il trattamento di tali dati, strumenti situati all'interno dello stesso stato. Il codice resta significativo soprattutto per gli obblighi che ne derivano per i soggetti pubblici, specificamente le Pubbliche Amministrazioni.

Qualche mese dopo il decreto legislativo n. 259 del 1° agosto 2003, *Codice delle comunicazioni elettroniche*, ha stabilito la normativa relativa alle comunicazioni tramite mezzi/apparecchi elettronici, definendone principi, obiettivi e obblighi incombenti su gestori e settore pubblico. Quanto ai principi generali, l'articolo 3 del codice garantisce i diritti inderogabili di libertà delle persone nell'utilizzo dei mezzi di comunicazione elettronica, il diritto di iniziativa economica e di esercizio in regime di concorrenza e la libera fornitura di reti e servizi, sotto la disciplina del codice. Lo stesso articolo, al terzo comma, stabilisce che le deroghe al codice devono derivare da esigenze "della difesa e della sicurezza dello stato, della protezione civile, della salute pubblica e della tutela dell'ambiente e della riservatezza e protezione dei dati personali, poste da specifiche disposizioni di legge o da disposizioni regolamentari di attuazione".

Il codice individua anche un'Autorità nazionale di regolamentazione (ANR) che, in collaborazione con il Ministero dello Sviluppo economico, è tenuta ad adottare tutte le misure previste dallo stesso codice per il conseguimento degli obiettivi sopra indicati e la promozione dello sviluppo del mercato e degli interessi dei cittadini.

L'istituzione di una ANR delle comunicazioni elettroniche per l'Italia deriva dall'attuazione della direttiva europea 2002/21/CE, che istituisce un Organismo dei regolatori europei delle comunicazioni elettroniche (BEREC, Body of European Regulators for Electronic Communications) ed invita gli stati membri a predisporre le relative autorità nazionali di regolamentazione. Autorità e Ministero restano responsabili della corretta implementazione del codice.

Infine, l'articolo 16-bis individua, presso il suddetto Ministero, un CERT nazionale "con compiti di assistenza tecnica in caso di segnala-

zioni da parte di utenti e di diffusione di informazioni anche riguardanti le contromisure adeguate per i tipi più comuni di incidente". Ad oggi il CERT nazionale italiano non è ancora entrato in funzione.

I due codici, quello in materia di protezione dei dati personali e quello delle comunicazioni elettroniche sono in vigore da più di dieci anni, dettando la disciplina nei rispettivi campi di interesse e applicazione.

Nel marzo 2003 il Ministero per l'Innovazione e le tecnologie ha posto in essere un Gruppo di lavoro sulla protezione delle infrastrutture critiche informatizzate, formato da alcuni rappresentanti dei Ministeri principalmente coinvolti in quest'attività (Interno, Infrastrutture, Comunicazioni, ecc.) e dai maggiori *provider* privati, tra cui Telecom Italia e Wind.

L'anno successivo questo gruppo di lavoro ha pubblicato il rapporto *Protezione delle infrastrutture critiche informatizzate. La realtà italiana*,[6] che è stato di grande riferimento per lo sviluppo della cybersecurity in Italia. Il rapporto mette infatti in evidenza la crescente necessità di tutelare le infrastrutture considerate critiche, per la sicurezza della nazione ed il benessere dei cittadini, sottolineando come tale necessità derivi dal carattere interdipendente delle infrastrutture informatizzate, le quali condividono uno spazio comune genericamente denominato cyber spazio. All'interno del cyber spazio, il danneggiamento di un'infrastruttura può avere importanti ripercussioni su altre infrastrutture interconnesse, in seguito ad effetti domino potenzialmente disastrosi.

Il documento offre una trattazione di alcuni casi di interruzione della fornitura di servizi critici[7] ed individua una serie di infrastrutture informatizzate – il cui funzionamento è basato su un sistema di reti informatiche – di rilevante impatto per l'Italia come sistema paese:

- infrastruttura elettrica;
- reti informatiche e reti di telecomunicazioni;
- infrastruttura per il trasporto del gas;

---

[6] Presidenza del Consiglio dei Ministri, Gruppo di lavoro sulla protezione delle infrastrutture critiche informatizzate, *Protezione delle infrastrutture critiche informatizzate. La realtà italiana*, 10 marzo 2004, http://www.vigilfuoco.it/aspx/ReturnDocument.aspx?IdDocumento=2832.

[7] In Italia il 28 settembre 2003, alle ore 3:28, si è verificato un black-out che ha interessato tutto il paese eccetto la Sardegna. La fascia notturna ed il fatto che fosse un giorno festivo hanno permesso di intervenire prontamente per ripristinare il servizio, senza causare danni rilevanti, ma l'evento resta emblematico della criticità di alcune infrastrutture nazionali per il regolare svolgimento della vita del paese.

- rete ferroviaria;
- rete viaria;
- circuiti bancari e finanziari;
- ospedali ed altre criticità infrastrutturali;
- impianti nucleari;
- navigazione satellitare;
- sistemi di monitoraggio e controllo (detti SCADA, Supervisory Control and Data Acquisition).

Il rapporto auspica la costituzione, ad opera del Comitato di cui al secondo punto, di un CERT-PA, in grado di operare da *early warning system* della Pubblica Amministrazione, attivo 24 ore su 24, tutti i giorni della settimana. Il CERT-PA è divenuto operativo solo nel 2014 (si veda oltre).

2.2 VERSO UNA MAGGIORE CONSAPEVOLEZZA DEI RISCHI NEL CYBER SPAZIO

Nel 2005 il decreto legislativo n. 82 del 7 marzo, *Codice dell'amministrazione digitale*, ha segnato un importante passo in avanti nel processo italiano di informatizzazione delle PA, gettando le basi per la crescente offerta di sevizi pubblici sulla rete. Con esso, i cittadini e le imprese hanno ottenuto il diritto di comunicare in via telematica con le Pubbliche Amministrazioni e con i gestori di pubblici servizi, potendo così accedere ai documenti amministrativi tramite le tecnologie dell'informazione e delle comunicazioni. Tra le novità più significative vi è stata l'introduzione della possibilità di effettuare pagamenti con modalità informatiche (articolo 5) e l'attivazione del servizio di posta elettronica certificata (articolo 6). È stata inoltre istituita la Conferenza permanente per l'innovazione tecnologica, tuttora esistente, allo scopo di consigliare il Presidente del Consiglio dei ministri in materia di sviluppo ed attuazione delle innovazioni tecnologiche all'interno delle amministrazioni dello stato (articolo 18).

L'articolo 51 dello stesso decreto, dedicato alla sicurezza dei dati, stabilisce inoltre che: "Le norme di sicurezza definite nelle regole tecniche [...] garantiscono l'esattezza, la disponibilità, l'accessibilità, l'integrità e la riservatezza dei dati" e che "I documenti informatici delle pubbliche amministrazioni devono essere custoditi e controllati con modalità tali

da ridurre al minimo i rischi di distruzione, perdita, accesso non autorizzato o non consentito o non conforme alle finalità della raccolta".

Il *Codice dell'amministrazione digitale* si propone quindi l'accelerazione del processo di digitalizzazione in Italia per quanta riguarda il settore pubblico, senza però tralasciare l'importanza della protezione dei dati e delle informazioni personali.

Il 31 luglio 2005 è stata, inoltre, approvata la legge n. 155 "recante misure urgenti per il contrasto del terrorismo internazionale". Di questa legge – cosiddetta legge Pisanu dal nome del ministro dell'Interno allora in carica – occorre mettere in evidenza l'articolo 7-bis sulla sicurezza telematica: "l'organo del Ministero dell'Interno per la sicurezza e per la regolarità dei servizi di telecomunicazione assicura i servizi di protezione informatica delle infrastrutture critiche informatizzate di interesse nazionale individuate con decreto del Ministro dell'Interno".

L'organo cui viene fatto riferimento è il Centro nazionale anticrimine informatico per la protezione delle infrastrutture critiche (CNAIPIC), che è stato successivamente istituito nel 2008 e posto sotto la direzione della Polizia postale (si veda oltre).

La legge Pisanu è importante perché attribuisce la responsabilità della protezione delle infrastrutture critiche informatizzate al Ministro dell'Interno ed assegna alla Polizia postale il dovere di attuare il *law enforcement* nei casi di attacco cibernetico contro le infrastrutture critiche nazionali (articolo 7-bis.2). La legge stabilisce inoltre l'istituzione di un centro nazionale esclusivamente dedicato alla CIIP (Critical Information Infrastructure Protection).

Dal 2001 il Nucleo speciale frodi telematiche della Guardia di Finanza (ex Gruppo anticrimine tecnologico, GAT) opera nel contrasto agli illeciti economico-finanziari commessi in rete e fornisce, ai reparti competenti, importanti informazioni suscettibili di sviluppo operativo. Collabora inoltre attivamente con l'Agenzia per l'Italia digitale[8].

L'obiettivo principale del Nucleo speciale della Guardia di Finanza è, dunque, quello di contrastare il crimine finanziario informatico ma, nonostante le differenze di mandato, si sono verificati casi in cui i compiti della Polizia postale e del Nucleo speciale frodi telematiche si sono parzialmente sovrapposti. La Polizia postale, dal 2009 a capo del CNAIPIC,

[8] Sito il sito web della Guardia di Finanza: *Reparti speciali*, http://www.gdf.gov.it/GdF/it/Chi_siamo/Organizzazione/Reparti/Reparti_Operativi/Reparti_speciali/index.html.

si è vista attribuire competenze in ambito di protezione delle infrastrutture critiche, oltre a quelle già possedute in settori quali cybercrime, cyber terrorismo e spionaggio industriale.

È importante segnalare come anche l'Arma dei Carabinieri contribuisca al mantenimento della sicurezza informatica in Italia tramite il Servizio investigazioni scientifiche, che è articolato in un Raggruppamento investigazioni scientifiche (Ra.C.I.S.), quattro Reparti investigazioni scientifiche e 29 Sezioni investigative scientifiche (SIS)[9].

Come si è detto, il tema della cybersecurity è stato spesso messo in relazione con la normativa di contrasto alla pedopornografia, poiché quest'ultima avviene prevalentemente attraverso la rete. La legge n. 38 del 6 febbraio 2006, *Disposizioni in materia di lotta contro lo sfruttamento sessuale dei bambini e la pedopornografia anche a mezzo Internet*, ha predisposto, al suo articolo 14-bis, la creazione di un Centro nazionale per il contrasto della pedopornografia sulla rete Internet (CNCPO), posto sotto il comando della Polizia postale, con lo scopo di raccogliere segnalazioni sui siti web che diffondono materiale concernente lo sfruttamento sessuale di minori. Il centro è divenuto operativo nel 2008 ed è oggi capofila della lotta nazionale allo sfruttamento sessuale minorile online, in stretta collaborazione con il Dipartimento per le Pari opportunità della Presidenza del Consiglio dei ministri e con la Polizia postale.

La realizzazione di un centro espressamente dedicato al contrasto dei crimini di pedopornografia in rete testimonia la diffusione su scala nazionale di tali comportamenti illeciti, che sfruttano il mezzo internet per facilitare il contatto con le vittime. Con il CNCPO, le autorità di governo italiane hanno deciso di dotarsi di uno strumento specifico per il contenimento di questa minaccia e la protezione dei cittadini.

Il tema della cybersecurity si interseca anche con quello della protezione delle infrastrutture critiche. Nel 2008 il Ministero dell'Interno ha approvato un documento che si prefigge di stabilire le procedure nazionali per la classificazione delle infrastrutture critiche dell'Italia. Il decreto del 9 gennaio 2008, *Individuazione delle infrastrutture critiche informatiche di interesse nazionale*, precede di circa undici mesi la direttiva europea 2008/114/CE sulle ECI (si veda il paragrafo 1.2), approvata nel dicembre dello stesso anno. Tale decreto definisce infrastrutture

[9] Si veda il sito web dei Carabinieri: *Indagini Scientifiche*, http://www.carabinieri.it/Internet/Arma/Oggi/RACIS.

critiche nazionali tutti i sistemi e servizi informatici di supporto alle seguenti funzioni istituzionali:

- ministeri, agenzie ed enti da essi vigilati, operanti nei settori dei rapporti internazionali, della sicurezza, della giustizia, della difesa, della finanza, delle comunicazioni, dei trasporti, dell'energia, dell'ambiente, della salute;
- Banca d'Italia ed autorità indipendenti;
- società partecipate dallo Stato, dalle Regioni e dai Comuni con più di 500.000 abitanti, nei settori delle comunicazioni, dei trasporti, dell'energia, della salute e delle acque;
- ogni altra istituzione, amministrazione, ente, persona giuridica pubblica o privata la cui attività sia riconosciuta di interesse nazionale.

In attuazione del citato articolo 7-bis della legge Pisanu del 2005, il decreto stabilisce inoltre, come già menzionato, la creazione di un nuovo organo incaricato di operare nel settore della CIIP: il Centro nazionale anticrimine informatico per la protezione delle infrastrutture critiche (CNAIPIC), quale unità organizzativa della Polizia postale, all'interno del Dipartimento della Pubblica Sicurezza.

Lo stesso anno viene approvata la legge n. 48 del 18 marzo 2008, *Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica*, che autorizza il Presidente della Repubblica a ratificare la Convenzione internazionale di Budapest sul cybercrime, firmata dall'Italia nel 2001. Come già riportato, dei 52 paesi firmatari, solo 41 hanno proceduto alla ratifica della Convenzione, di cui 23 stati membri UE. La ratifica della Convenzione di Budapest si inserisce all'interno del processo nazionale di definizione, perseguimento e punizione del crimine informatico, che non può prescindere dalla sua natura tendenzialmente transnazionale.

La modernizzazione del paese e, in particolare, della Pubblica Amministrazione attraverso l'informatizzazione delle attività aumenta tendenzialmente anche i problemi connessi con la cybersecurity. Nel 2009 il Ministero per la Pubblica Amministrazione e per l'innovazione ha lanciato il "Piano e-Gov 2012" con il quale il Governo si impegna a favorire l'innovazione, la diffusione di servizi di rete, l'accessibilità e la trasparenza della Pubblica Amministrazione, così da avvicinarla alle esigenze dei cittadini e delle imprese.

Il piano ha come obiettivo quello di innalzare il livello generale di digitalizzazione del paese, in linea con le tendenze che caratterizzano gli altri stati europei, migliorando la qualità di alcuni servizi, come la scuola, le università, la giustizia, la sanità, l'ambiente ed i beni culturali, la mobilità ed il sostegno alle imprese. Si prefigge inoltre la semplificazione dei rapporti tra cittadini e PA e l'elaborazione di regole e standard tecnici per le infrastrutture nazionali.

Nell'ambito del piano, sono state previste numerose iniziative per lo sviluppo nazionale del fattore ICT, volte al perseguimento di tre obiettivi:

1) digitalizzazione dei servizi;
2) informatizzazione delle PA;
3) adozione di tecnologie dell'informazione e delle comunicazioni nel settore delle infrastrutture.

Nel biennio 2011-2012 sono stati realizzati 539 progetti, per un costo di 2.580.445 euro. Per la realizzazione degli obiettivi posti dal piano sono stati inoltre siglati numerosi protocolli d'intesa tra enti pubblici e privati, tra cui quelli con Ericsson Telecomunicazioni, Vodafone e IBM[10].

Il "Piano e-Gov 2012" attesta la volontà del Governo italiano di ridurre lo scarto in termini di sviluppo del processo di digitalizzazione, cosiddetto "*digital divide*", esistente con gli altri paesi europei, a partire dall'informatizzazione della PA e dalla collaborazione con il settore privato.

Nel 2010 la Presidenza del Consiglio dei ministri ha approvato il DPCM (5 maggio 2010) *Organizzazione nazionale per la gestione di crisi*, con l'obiettivo di aggiornare il *Manuale nazionale per la gestione di crisi*, pubblicato nel 1994 e rimasto valido per i successivi sedici anni. Considerati gli sviluppi nella tipologia di scenari e di minacce, è sembrato opportuno rivedere il documento. La revisione del manuale si è basata sui principi del *NATO Crisis Response System Manual* e del *Manual on EU Emergency and Crisis Coordination*. L'Italia ha così adeguato le procedure nazionali per la prevenzione, gestione e risposta delle/alle crisi a quelle già elaborate in sede NATO ed Unione europea.

[10] Per una lista completa si veda il sito web del Ministro per la Semplificazione e la Pubblica Amministrazione: *Reti Amiche: I protocolli d'intesa*, http://www.funzionepubblica.gov.it/lazione-del-ministro/servizi-per-il-cittadino/reti-amiche/i-protocolli-dintesa-sottoscritti.aspx.

L'articolo 4 del decreto definisce la struttura e le competenze del Comitato politico-strategico (CoPS), organo già previsto dal manuale del 1994, che deve continuare a svolgere un ruolo di indirizzo e di guida nelle situazioni di crisi nazionale. Il CoPS valuta gli elementi di situazione, elabora i provvedimenti da sottoporre al Consiglio dei ministri e, se necessario, autorizza l'adozione di misure di contrasto. La novità introdotta dal decreto del 2010 è quella di includere nel CoPS rappresentanti del Ministero dell'Economia e Finanza, oltre a quelli già presenti dei Ministeri degli Affari esteri, dell'Interno e della Difesa. Questa scelta è emblematica della crescente dimensione economica della sicurezza nazionale.

L'articolo 5 predispone poi l'istituzione di un nuovo organo: il Nucleo interministeriale di situazione e pianificazione (NISP). Il NISP ha assorbito tutte le competenze del Nucleo politico militare (NPM), previsto dal manuale del 1994, per svolgere attività di consulenza al CoPS in condizioni di crisi, nonché di controllo e valutazione in condizioni di normalità.

Il NISP, come già l'NPM, ha assunto carattere permanente, ricevendo il compito di monitorare costantemente la situazione di sicurezza interna ed internazionale. Il NISP agisce inoltre di supporto al CoPS, promuove la programmazione e pianificazione interministeriale, acquisisce informazioni e coordina lo svolgimento delle esercitazioni interministeriali, che consistono nella simulazione di crisi (articolo 6).

Il decreto del 2010 ha aggiornato l'organizzazione delle procedure di gestione delle situazioni di crisi, ma è rilevante soprattutto per avere inserito il NISP all'interno del panorama degli organi deputati alla sicurezza nazionale. Dal 2013 questo organo svolge un ruolo fondamentale per la cybersecurity in Italia (si veda oltre).

2.3 La relazione del COPASIR

Il 15 luglio 2010 il Comitato parlamentare per la sicurezza della Repubblica (COPASIR) ha trasmesso alle Camere una *Relazione sulle possibili implicazioni e minacce per la sicurezza nazionale derivanti dall'utilizzo dello spazio cibernetico*. Le relazioni del COPASIR hanno solitamente lo scopo di fornire alle Camere indagini approfondite sulle questioni di sicurezza nazionale ed internazionale di maggior rilevanza nel prossimo futuro. Rappresentano pertanto un importante riferimento per l'elaborazione di successive politiche nazionali in materia.

Il gruppo di deputati e senatori[11] che si è occupato dell'elaborazione e stesura della relazione è stato supportato da alcuni consulenti esterni, tra i quali la Rand Corporation, con l'obiettivo di definire la minaccia cibernetica e coglierne gli aspetti più pericolosi per la sicurezza del sistema paese. Nel documento, tale minaccia viene distinta in quattro principali tipologie: a) cyber-crime; b) cyber terrorism; c) cyber espionage; D) cyber war.[12]

In base alla relazione, l'approccio migliore alla minaccia cibernetica risulterebbe essere quello sistemico, ossia quello in grado di coinvolgere tutti i settori della società, dalle grandi imprese ai singoli cittadini, così da diffondere un buon livello di educazione alla sicurezza informatica e da stimolare la cooperazione tra pubblico e privato.

Relativamente al cybercrime, la relazione riporta i dati Symantec del 2009[13], che posizionano l'Italia al decimo posto tra i paesi al mondo più esposti "in termini di produzione di *software* malevolo, di *spam* ovvero posta elettronica 'spazzatura', di siti di *phishing* per frodi finanziarie online e di attacchi verso altri paesi"[14]. Ai primi posti di questa *top ten* si collocano Stati Uniti, Brasile, Cina e Germania (si veda il capitolo 1.3, grafici 1-2).

La relazione del COPASIR mette in evidenza la necessità, per l'Europa e l'Italia, di dotarsi dei mezzi opportuni per combattere il cybercrime e garantire la sicurezza delle reti. Il cybercrime si rivela come la nuova frontiera di attività criminose che si rivolgono *in primis* contro i singoli individui ma anche contro le infrastrutture critiche nazionali, attentando così alla sicurezza del paese. Il COPASIR sottolinea come, a partire dai primi anni 2000, numerose convenzioni e partnership sono state stipulate tra soggetti pubblici e privati per fronteggiare il cybercrime. Tra le più significative menzionate nella relazione, segnaliamo di seguito

---

[11] Massimo D'Alema (presidente), Maria Piera Pastore (segretario), Carmelo Briguglio, Fabrizio Cicchitto, Ettore Rosato, Stefano Esposito, Giuseppe Caforio, Achille Passoni, Gaetano Quagliariello e Francesco Rutelli (relatore).

[12] COPASIR, *Relazione sulle possibili implicazioni e minacce per la sicurezza nazionale derivanti dall'utilizzo dello spazio cibernetico*, 7 luglio 2010, p. 17, http://www.senato.it/leg/16/BGT/Schede/docnonleg/19825.htm

[13] Symantec, *Symantec Intelligence Quarterly, July-September 2009*, October 2009, http://eval.symantec.com/mktginfo/enterprise/other_resources/b-symc_intelligence_quarterly_july-sept_2009_20666025.en-us.pdf.

[14] COPASIR, *Relazione sulle possibili implicazioni e minacce per la sicurezza nazionale …*, cit., p. 21.

quelle con Poste italiane (2002 e 2009) e con Rete ferroviaria italiana (2003).

Nel 2002 la società Poste italiane e la Polizia italiana hanno sottoscritto un accordo, volto a stabilire congiuntamente determinati servizi per prevenire e combattere il crimine informatico. Negli anni, la Polizia postale ha firmato con alcune università italiane dei protocolli d'intesa per la formazione specializzata del personale di polizia e degli studenti interessati ad intraprendere una carriera in questo settore. Anche Poste italiane ha intrapreso importanti collaborazioni con le università, tra cui emerge quella con l'Università statale di Milano, per realizzare un sistema di supporto alle vittime di *phishing*, tramite posta elettronica, denominato "Phishing Forensic Analyzer". Sempre Poste italiane ha avviato la costituzione di un Centro di eccellenza nazionale sulla cybersecurity (CENSec), sull'esempio del CCD COE di Tallinn.

Nel 2003 è stata stipulata la "Convenzione per la prevenzione dei crimini informatici sui sistemi di gestione della sicurezza della circolazione ferroviaria utilizzati dalla Rete Ferroviaria Italiana Spa", che dal 2009 consente una stretta collaborazione tra Rete ferroviaria italiana (RFI) e CNAIPIC per garantire la protezione dell'infrastruttura ferroviaria.

Nel 2009, infine, è stata realizzata la European Electronic Crime Task Force, grazie al contributo della Polizia postale, dell'agenzia statunitense di *law enforcement* Secret Service e di Poste italiane. La struttura ha l'obiettivo di porsi come centro di eccellenza europeo per la lotta al cybercrime e di costruire un'alleanza strategica per la condivisione di informazioni e l'aggregazione di competenze ed *expertise* a livello europeo, mediante il coinvolgimento di istituzioni pubbliche, forze di polizia, mondo accademico, magistratura e settore privato. La task force si riunisce periodicamente presso il quartier generale di Poste italiane e l'ultimo incontro si è svolto in data 23 aprile 2013 ed è stato dedicato al dibattito sulle necessità urgenti di realizzare un CERT nazionale e predisporre reti di cooperazione internazionale. Questi incontri hanno lo scopo di favorire la collaborazione e la fiducia reciproca tra tutti gli attori coinvolti nella lotta al cybercrime, a livello nazionale ed europeo.

Per il COPASIR la strategia italiana di lotta al crimine informatico si è articolata secondo cinque direttrici, una delle quali è basata sulle numerose iniziative intraprese dal Governo e dai principali attori nazionali della sicurezza informatica per promuovere la cooperazione pubblico-privato ed incoraggiare lo sviluppo in questo campo. Notiamo come, in particolare, il sistema delle convenzioni - basato sulla firma di accordi di

collaborazione e protocolli d'intesa tra istituzioni pubbliche ed imprese private - sembra caratterizzare l'approccio italiano alla questione della cybersecurity, fin dai primi anni del 2000. Il consolidamento di questo approccio, però, non è stato assistito da un parallelo adeguamento del quadro normativo, impedendo, ad esempio, l'elaborazione di standard obbligatori nazionali di sicurezza e la chiara individuazione delle strutture incaricate di gestire la cybersecurity.

La relazione sottolinea come un attore fondamentale per la cybersecurity in Italia sia il Sistema di informazione per la sicurezza della Repubblica, che svolge un ruolo decisivo per quanto riguarda l'attività di monitoraggio e controllo delle minacce informatiche che attentano alla sicurezza del sistema paese.

Dall'approvazione della legge n. 124 del 3 agosto 2007, *Sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto*, che ha riformato il comparto *intelligence* italiano[15], i servizi segreti operano in questo settore attraverso tre strutture:

1) Divisione INFOSEC dell'AISE (Agenzia informazioni e sicurezza esterna);
2) Sezione controingerenza telematica dell'AISI (Agenzia informazioni e sicurezza interna);
3) Ufficio centrale per la segretezza del DIS (Dipartimento informazioni per la sicurezza).

La relazione del COPASIR chiude con una raccomandazione importante per il Governo, affinché questo adotti "un impianto strategico-organizzativo che assicuri una *leadership* adeguata e predisponga chiare linee politiche per il contrasto alle minacce e il coordinamento tra gli attori interessati"[16]. Viene, quindi, suggerita l'individuazione di una struttura di coordinamento, da istituire presso la Presidenza del Consiglio dei ministri o l'autorità delegata, che si occupi di tutte le maggiori questioni di cybersecurity.

La relazione del COPASIR si è rivelata molto significativa per la presa di consapevolezza, da parte delle autorità di governo e delle agenzie ita-

[15] In seguito alla legge del 2007 la struttura dell'intelligence ha assunto una nuova organizzazione, con alla base il DIS, l'AISE e l'AISI, al livello intermedio l'autorità delegata e al vertice il CISR ed il Presidente del Consiglio dei ministri.

[16] COPASIR, *Relazione sulle possibili implicazioni e minacce per la sicurezza nazionale ...*, cit., p. 49.

liane, del significato crescente della minaccia cibernetica, che è in grado di impattare notevolmente sulla vita socio-economica e sulla sicurezza del paese. Il documento invita alla predisposizione di adeguate politiche nazionali di cybersecurity.

Il Sistema di informazione per la sicurezza della Repubblica sottopone ogni anno al Parlamento una relazione sulla politica dell'informazione per la sicurezza, finalizzata a delineare il panorama delle minacce in continua evoluzione che attentano alla sicurezza del sistema paese Italia. Quella del 2010 è la prima ad annoverare, tra le "sfide crescenti" degli "scenari di rischio", la cosiddetta *cyber threat*. Le successive relazioni hanno incluso la dimensione cibernetica nei tradizionali domini da mettere in sicurezza, per la salvaguardia degli interessi nazionali.

2.4 Sviluppi recenti

2.4.1 Il 2011

Nel 2011 il Presidente della Repubblica ha emanato il decreto legislativo n. 61 (11 aprile 2011), *Attuazione della direttiva 2008/114/CE recante l'individuazione e la designazione delle infrastrutture critiche europee e la valutazione della necessità di migliorarne la protezione* (si veda il paragrafo 1.2). Il decreto stabilisce le procedure per l'individuazione e la designazione delle cosiddette ECI, nei settori dell'energia e dei trasporti, come prescritto dalla direttiva europea, nonché le modalità di valutazione della sicurezza di tali infrastrutture e le relative prescrizioni minime di protezione dalle minacce di varia natura (articolo 1.1).

In base alla definizione contenuta nel decreto, improntata su quella fornita dalla direttiva europea, un'infrastruttura critica è quella "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" (articolo 2-bis).

L'articolo 4 del decreto assegna il compito di individuare e designare le ECI al NISP, coadiuvato da rappresentanti del Ministero dello Sviluppo economico per il settore dell'energia, e da rappresentanti del Ministero delle Infrastrutture e dei Trasporti e degli enti vigilati per il settore dei trasporti. Il NISP rappresenta anche il punto di contatto nazionale per

la protezione delle ECI con gli altri stati membri e con la Commissione europea (articolo 13.1).

I criteri di valutazione utilizzati per individuare e designare le ECI riguardano: a) le possibili vittime (numero di morti e di feriti); b) le possibili conseguenze economiche (perdite finanziarie, danni ambientali, deterioramento del servizio); c) le possibili conseguenze per la popolazione in generale (sofferenze fisiche, perdita di fiducia nelle istituzioni, perturbamento della normale vita quotidiana).

È da rilevare che il decreto del 2011 non prevede alcun fondo finanziario per la realizzazione degli obiettivi da esso posti.

Lo stesso anno il DPCM 12 ottobre 2011 ha istituito presso la Presidenza del Consiglio dei ministri un Gruppo di studio per la sicurezza dell'utilizzo dello spazio cibernetico che, sulla base delle indicazioni fornite dal COPASIR nella relazione del 2010, ha ricevuto il compito di porre in essere presso la Presidenza del Consiglio un Comitato interministeriale, principalmente preposto all'elaborazione di una "Strategia nazionale per la sicurezza cibernetica", senza indicare tempistiche al riguardo[17]. Al gruppo di studio è stato affidato l'incarico di effettuare una ricognizione delle strutture già esistenti in Italia, individuare gli assetti organizzativi posti in essere da altri paesi europei e formulare una proposta per mettere a sistema le strutture nazionali precedentemente individuate.

2.4.2 Il 2012

Nel 2012 l'Italia, con l'approvazione di due decreti legislativi, ha recepito due importanti direttive dell'Unione europea in tema di protezione dei dati personali e sicurezza delle reti e dei servizi di comunicazione elettronica. L'Italia si è adeguata al mutato contesto normativo europeo con un ritardo di circa un anno, ritardo che le ha inizialmente procurato, insieme ad altri paesi, la diffida di avvio della procedura di infrazione.

Con il decreto legislativo n. 69 del 28 maggio 2012 sono state trasposte nell'ordinamento interno le direttive 2009/136/CE e 2009/140/CE ed il regolamento (CE) 2006-2004 sulla cooperazione tra le autorità nazionali responsabili di tutelare i consumatori. A questo scopo, è stato modificato il già citato decreto legislativo n. 196 del 30 giugno 2003, recante codice in materia di protezione dei dati personali. Inoltre, con il decreto legisla-

[17] Agenda digitale italiana, *Strategia Cyber Security*, http://www.agenda-digitale.it/agenda_digitale/images/documenti/strategia_cyber_security.pdf.

tivo n. 70 del 28 maggio 2012 è stato modificato il decreto n. 259 del 1° agosto 2003, recante codice delle comunicazioni elettroniche.

L'obiettivo delle direttive europee di cui sopra è quello di armonizzare le varie disposizioni nazionali in materia di protezione dei diritti e delle libertà fondamentali in ambito informatico e telematico, con particolare attenzione alla tutela del diritto alla vita privata e alla riservatezza. I decreti italiani hanno contribuito a rendere più completo il quadro normativo nazionale in questa materia, in linea con quanto stabilito a livello europeo.

Sempre nel 2012 l'Italia ha istituito un'agenzia nazionale incaricata di operare a sostegno dello sviluppo del settore ICT nel territorio nazionale, in linea con quanto stabilito nell'Agenda digitale italiana e in quella europea.

Il decreto legge n. 83 del 15 giugno 2012 – cosiddetto decreto Sviluppo, convertito in legge n. 134 del 7 agosto 2012 – ha istituito l'Agenzia per l'Italia digitale (AgID), avente il compito di coordinare "le azioni in materia di innovazione per promuovere le tecnologie ICT a supporto delle pubbliche amministrazioni, garantendo la realizzazione degli obiettivi dell'Agenda digitale italiana, in coerenza con l'Agenda digitale europea"[18].

L'agenzia ha ereditato le competenze della preesistente DigitPA, ente nazionale per la digitalizzazione della pubblica amministrazione (ancora prima denominato CNIPA[19]), istituita con decreto legislativo n. 177 del 1° dicembre 2009, *Riorganizzazione del Centro nazionale per l'informatica nella pubblica amministrazione, a norma dell'articolo 24 della legge 18 giugno 2009, n. 69*.

L'agenzia ha assorbito anche le funzioni del Dipartimento per la digitalizzazione e l'innovazione della Presidenza del Consiglio, dell'Agenzia per la diffusione delle tecnologie per l'innovazione e dell'Istituto superiore delle comunicazioni e delle tecnologie dell'informazione – per le sole competenze sulla sicurezza delle reti.

Come riportato, l'AgID ha la primaria responsabilità di implementare l'Agenda digitale italiana (ADI), stabilita con decreto del Ministero dello Sviluppo economico in data 1° marzo 2012. Il successivo decreto legge n. 179 del 18 ottobre 2012, *Ulteriori misure urgenti per la crescita del paese*

[18] Si veda il sito dell' Agenzia per l'Italia digitale: http://www.agid.gov.it/agenzia.

[19] Il Centro nazionale per l'informatica nella pubblica amministrazione (CNIPA) è stato istituito con decreto legislativo n. 196 del 30 giugno 2003, recante codice in materia di protezione dei dati personali (si veda paragrafo 2.1).

– cosiddetto provvedimento Crescita 2.0 – ha predisposto le misure specifiche per la realizzazione concreta dell'agenda.

L'AgID ha ricevuto anche il compito di portare avanti il progetto di una cabina di regia[20] per l'elaborazione di una strategia nazionale per lo sviluppo del paese basato sull'economia digitale. Questo è avvenuto con decreto legge n. 69 del 21 giugno 2013, *Disposizioni urgenti per il rilancio dell'economia* – cosiddetto decreto del fare, convertito in legge n. 98 del 9 agosto 2013 – che ha anche istituito un tavolo permanente[21], composto da esperti, per redigere una seconda strategia.

La strategia per la realizzazione dell'Agenda digitale è stata presentata nel maggio 2013 dall'allora direttore dell'Agenzia per l'Italia digitale, Agostino Ragosa[22]. Questi sottolinea come il fattore economico della cybersecurity rivesta un'importanza cruciale per il benessere di uno stato, costituendo un'opportunità di crescita. In base ai dati AgID, nel 2010 l'economia digitale ha registrato un impatto positivo sul PIL italiano pari a circa l'1,7%, per un valore di circa 26 miliardi di euro. In altri paesi, come Regno Unito e Svezia, il contributo supera la soglia del 5%. Ragosa osserva come l'impatto dell'economia digitale in Italia sia anche molto inferiore a quello registrato in Corea, Giappone, Stati Uniti, Francia, Germania e Canada: colmando entro il 2015 anche solo la metà del *gap* esistente con questi paesi, l'Italia otterrebbe un incremento del PIL del 4%.

La necessità di incentivare il progresso digitale a livello nazionale, in particolar modo all'interno delle Pubbliche Amministrazioni, ha fatto sì che le principali azioni strategiche elaborate dall'AgID per il prossimo futuro riguardino:

- rete a banda larga del paese;
- infrastruttura ICT delle PA;
- interoperabilità e Open Data;
- e-government e sviluppo digitale.

---

[20] La Cabina di regia è un ente istituito con decreto legge n. 5 del 9 febbraio 2012, poi convertito in legge n. 35 del 4 aprile 2012, che ha ricevuto il compito di preparare una strategia nazionale per lo sviluppo del paese, sulla base dell'iniziativa "Digital Agenda" contenuta nella strategia europea EU2020.

[21] Agenzia per l'Italia digitale, *Agenda digitale italiana*, http://www.agid.gov.it/agenda-digitale/agenda-digitale-italiana.

[22] Agenzia per l'Italia digitale, *La strategia AgID per la realizzazione dell'Agenda digitale italiana*, Forum PA, Roma, 28 maggio 2013, http://archivio.digitpa.gov.it/sites/default/files/SlideRagosaMappaDigitalAgenda.pdf.

A partire dal gennaio 2014 è divenuto operativo il CERT-PA, struttura operante all'interno dell'AgID e preposta al trattamento degli incidenti di sicurezza informatica del dominio costituito dalle Pubbliche Amministrazioni. Il CERT-PA fornisce alle amministrazioni servizi di analisi e di indirizzamento; servizi proattivi, con lo scopo di raccogliere ed elaborare dati e segnalazioni ai fini della sicurezza; servizi reattivi, per la gestione degli allarmi e degli incidenti di sicurezza; servizi di formazione e comunicazione, per promuovere una cultura della sicurezza cibernetica.

La legge n. 133 del 7 agosto 2012, *Modifiche alla legge 3 agosto 2007, n. 124, concernente il Sistema di informazione per la sicurezza della Repubblica e la disciplina del segreto*, ha attribuito al DIS il ruolo di coordinamento delle attività di ricerca informativa finalizzate a rafforzare la protezione cibernetica e la sicurezza informatica nazionali (articolo 3.1). Spetta poi al COPASIR vigilare sulla condotta delle suddette attività da parte di altri organismi pubblici non appartenenti al Sistema di informazione per la sicurezza della Repubblica, affinché questi rispettino i principi contenuti nella presente legge. La legge del 2007 attribuisce dunque al DIS un ruolo fondamentale in ambito cybersecurity.

La *Relazione sulla politica dell'informazione per la sicurezza* relativa all'anno 2012, preparata dal Sistema di informazione per la sicurezza della Repubblica per il Parlamento, ha dedicato un intero capitolo all'impatto delle "nuove tecnologie" sulla sicurezza del sistema paese. La minaccia cibernetica, definita trasversale, asimmetrica ed a-territoriale, implica l'allargamento del tradizionale concetto di sicurezza, per realizzare il cosiddetto modello "partecipato"[23]. La "sicurezza partecipata" assume, nel contesto cibernetico, un rilievo fondamentale, in quanto coinvolge una serie di attori pubblici e privati, tutti necessari ad un'efficace gestione della minaccia.

Il direttore del DIS, Giampiero Massolo, ha dichiarato nel gennaio 2014 che la realizzazione della sicurezza partecipata rappresenta, oggi, la vera sfida alla sicurezza nazionale[24]. Secondo Massolo, il rapporto con

[23] Sistema di informazione per la sicurezza della Repubblica, *Relazione sulla politica dell'informazione per la sicurezza 2012*, 28 febbraio 2013, p. 37-38, http://www.sicurezzanazionale.gov.it/sisr.nsf/relazione-annuale/relazione-al-parlamento-2012.html.

[24] Intervento di Giampiero Massolo in occasione della conferenza "La sfida cyber: minaccia all'economia nazionale", organizzata a Roma il 27 gennaio 2014 dalla Società Italiana per l'Organizzazione Internazionale (SIOI).

il settore privato, soprattutto con quella parte di esso che gestisce le reti di infrastrutture critiche nazionali, si rivela cruciale affinché sia possibile consolidare buone partnership, in nome della sicurezza. In questo quadro, l'intelligence costituisce solo una delle molteplici leve della sicurezza nazionale: "il sistema delle convenzioni, che ha una certa tradizione in Italia, è alla base della protezione dalla minaccia cibernetica".

La relazione sul 2012 fa inoltre riferimento al DPCM 24 gennaio 2013, approvato un mese prima, quale strumento normativo volto a definire una prima strategia di risposta nazionale alla questione della cybersecurity. In particolare, vengono individuati tre diversi livelli di intervento: a) indirizzo politico e coordinamento strategico; b) supporto e raccordo tra gli enti competenti; c) gestione delle crisi.

Un'ultima parte della relazione, dedicata all' "uso del web a fini propagandistici: il messaggio qaidista", evidenzia l'aumento dell'utilizzo dei mezzi informatici da parte delle maggiori organizzazioni di terrorismo internazionale, soprattutto per la diffusione di materiale audio-visivo dottrinale e per l'attività di reclutamento.

La relazione, notando il pericoloso irrobustirsi della minaccia cibernetica, invita il Governo italiano alla prossima adozione di un quadro strategico e di un piano nazionale in tema di sicurezza cibernetica.

2.5 I passi avanti del 2013

2.5.1 Il DPCM 24 gennaio 2013

Il 24 gennaio 2013 il presidente del Consiglio dei ministri ha approvato il DPCM *Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale*. Il documento ha rappresentato una svolta per l'Italia poiché che in esso viene definita, per la prima volta, "l'architettura istituzionale deputata alla sicurezza nazionale relativamente alle infrastrutture critiche materiali e immateriali" (articolo 1.1).

Il decreto ha evidenziato la presa di consapevolezza da parte delle autorità di governo italiane della necessità di dotarsi di un quadro legale per lo spazio cibernetico, affinché fosse possibile iniziare a relazionarsi efficientemente con questa nuova minaccia alla sicurezza nazionale.

Non può essere considerato un documento strategico, tanto meno un piano d'azione, in quanto si limita ad individuare gli organi e gli enti nazionali incaricati di gestire le eventuali situazioni di emergenza, in corrispondenza di eventi malevoli e pericolosi originatisi nel cyber spazio.

È tuttavia significativo poiché delinea un modello "organizzativo-funzionale" per la sicurezza informatica in Italia (articolo 1.3), improntato sulla coerente integrazione delle attività intraprese dagli organi ed enti deputati alla cybersecurity e le attività già svolte dal Ministero dello Sviluppo economico, dall'Agenzia per l'Italia digitale, dal Ministero della Difesa e dal Ministero dell'Interno.

Il decreto fornisce inoltre una serie di definizioni utili a fare chiarezza sui significati condivisi dei principali elementi della sicurezza cibernetica:

- spazio cibernetico;
- sicurezza cibernetica;
- minaccia cibernetica;
- evento cibernetico;
- allarme;
- situazione di crisi.

Non è presente la definizione di "infrastruttura critica", che è però contenuta nel decreto legislativo n. 61/2011 avente lo scopo di attuare nell'ordinamento italiano la direttiva europea sull'individuazione e la designazione delle ECI (si veda paragrafo 4.1).

Lo spazio cibernetico viene definito come "l'insieme delle infrastrutture informatiche interconnesse, comprensivo di hardware, software, dati ed utenti, nonché delle relazioni logiche, comunque stabilite, tra di essi"; mentre per sicurezza cibernetica si intende una "condizione per la quale lo spazio cibernetico risulti protetto grazie all'adozione di idonee misure di sicurezza fisica, logica e procedurale rispetto ad eventi, di natura volontaria od accidentale, consistenti nell'acquisizione e nel trasferimento indebiti di dati, nella loro modifica o distruzione illegittima, ovvero nel danneggiamento, distruzione o blocco del regolare funzionamento delle reti e dei sistemi informativi o dei loro elementi costitutivi" (articolo 2.1).

La cybersecurity è quindi la messa in sicurezza del dominio cibernetico per proteggerlo da un evento cibernetico. La minaccia cibernetica viene descritta come il "complesso delle condotte che possono essere realizzate nello spazio cibernetico o tramite esso, ovvero in danno dello stesso e finalizzate all'acquisizione e al trasferimento indebiti di dati, alla loro modifica o distruzione illegittima, ovvero a danneggiare, distruggere o ostacolare il regolare funzionamento delle reti e dei sistemi informativi o dei loro elementi costitutivi" (articolo 2.1).

Infine, l'allarme risulta essere la comunicazione di avviso di un evento cibernetico; mentre la situazione di crisi è quella "in cui l'evento cibernetico assume dimensioni, intensità o natura tali da incidere sulla sicurezza nazionale o da non poter essere fronteggiato dalle singole amministrazioni competenti in via ordinaria ma con l'assunzione di decisioni coordinate in sede interministeriale" (articolo 2.1).

La rilevanza del documento è però nell'individuazione delle strutture pubbliche nazionali operanti nel settore della cybersecurity (articoli 3-10).

Il presidente del Consiglio dei ministri riceve il compito primario di elaborare un Quadro strategico nazionale per la sicurezza dello spazio cibernetico ed un Piano nazionale per la protezione cibernetica e la sicurezza informatica (si veda oltre), rispettivamente su proposta e deliberazione del Comitato interministeriale per la sicurezza della Repubblica (CISR). Inoltre il presidente, sentito il CISR, impartisce le direttive al DIS e alle due agenzie del Sistema di informazione per la sicurezza della Repubblica, AISE ed AISI.

Il CISR svolge anche altre mansioni: approvare le linee di indirizzo per favorire la collaborazione tra soggetti pubblici e privati interessati alla sicurezza cibernetica; promuove l'*information sharing* e l'adozione di *best practices*. Il CISR elabora poi gli indirizzi generali e gli obiettivi fondamentali in materia di sicurezza informatica ed incoraggia la realizzazione delle iniziative necessarie per garantire la partecipazione dell'Italia ai consessi di cooperazione internazionale, soprattutto in ambito UE e NATO. Formula inoltre le proposte di intervento normativo ed organizzativo, al fine di potenziare le misure di prevenzione e risposta alla minaccia cibernetica e quelle volte alla gestione delle crisi.

Viene poi costituito un organismo di supporto al CISR, quale organismo collegiale di coordinamento, presieduto dal direttore generale del DIS. Questo organismo ha il dovere di svolgere tutte le azioni necessarie al buon funzionamento delle attività intraprese dal CISR.

Presso la scuola di formazione istituita all'interno del Sistema di informazione per la sicurezza della Repubblica viene creato un Comitato scientifico di esperti di sicurezza cibernetica, provenienti dalle università, dagli enti di ricerca, dalle Pubbliche Amministrazioni e dal settore privato, con il compito di formulare ipotesi di intervento, per incrementare i livelli di sicurezza delle reti. Il comitato ha altresì il dovere di favorire la diffusione di una cultura della sicurezza nel settore cibernetico.

Come già riportato, il DIS e le due agenzie AISE e AISI svolgono un ruolo fondamentale nell'ambito del Sistema di informazione per la sicurezza

della Repubblica, avvalendosi di strumenti, modalità e procedure stabilite dalla già citata legge n. 124 del 3 agosto 2007. Le due agenzie conducono, nei loro rispettivi ambiti di attribuzione, tutte le attività di ricerca ed elaborazione informativa per la protezione cibernetica e la sicurezza informatica nazionali. Il DIS provvede alla trasmissione di informazioni rilevanti ai fini della cybersecurity alle Pubbliche Amministrazioni e agli altri soggetti interessati, anche privati, e ad un nuovo organismo, il Nucleo per la sicurezza cibernetica.

Il Nucleo per la sicurezza cibernetica viene istituito presso l'Ufficio del Consigliere militare del presidente del Consiglio dei ministri. È presieduto dal Consigliere militare e composto da un rappresentante per ciascuno dei seguenti:

- DIS;
- AISE;
- AISI;
- Ministero degli Affari esteri;
- Ministero dell'Interno;
- Ministero della Difesa;
- Ministero dello Sviluppo economico;
- Ministero dell'Economia e Finanza;
- Dipartimento della Protezione civile;
- Agenzia per l'Italia digitale.

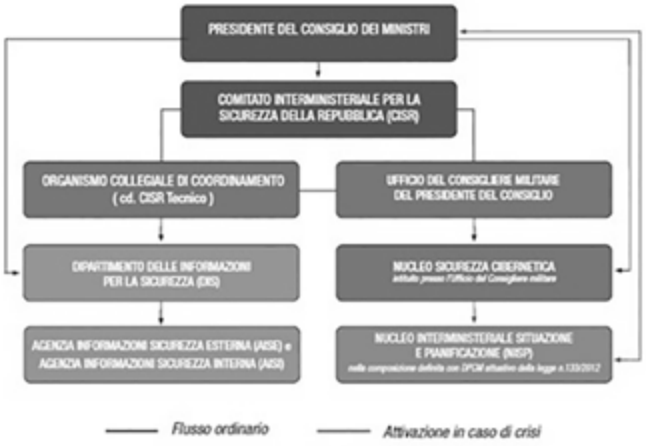
Il nucleo svolge una funzione di raccordo tra le diverse componenti dell'architettura istituzionale, promuove la programmazione e pianificazione operativa della risposta a situazioni di crisi cibernetica, mantiene attiva – 24 ore su 24, tutti i giorni della settimana – l'Unità per l'allertamento e la risposta alle crisi e costituisce il punto di riferimento nazionale per i rapporti con altri stati e con le organizzazioni internazionali, *in primis* Nazioni Unite, Nato e Unione europea[25]. Inoltre il Nucleo riceve le segnalazioni di evento cibernetico dall'estero, dirama gli allarmi all'interno del territorio nazionale, dichiara la situazione di crisi ed attiva il NISP quale "Tavolo interministeriale di crisi cibernetica".

L'Unità per l'allertamento è divenuta operativa dal novembre 2013. Ad essa è stata affiancata una Segreteria per la sicurezza cibernetica incaricata di organizzare le attività e coordinare gli impegni interministeriali.

[25] In questo caso, ereditando una funzione che prima spettava all'Iscom (si veda paragrafo 2.1).

Il NISP è anch'esso presieduto dal Consigliere militare ed ha il compito di monitorare sulla corretta gestione delle crisi cibernetiche, da parte di amministrazioni ed enti. Per quanto riguarda gli aspetti più tecnici, il Tavolo può avvalersi del CERT nazionale, istituito presso il Ministero dello Sviluppo economico, ma attualmente non ancora operativo.

Figura 1 - DPCM 24gennaio 2013: architettura nazionale deputata alla cybersecurity



Fonte: Relazione sulla politica dell'informazione per la sicurezza 2013.

Luisa Franchina, già direttore generale del Nucleo operativo per gli attentati NBCR (nucleari, biologici, chimici e radiologici) e direttore generale della Segreteria interministeriale di coordinamento delle infrastrutture critiche della Presidenza del Consiglio dei ministri, ha individuato nel giugno 2013[26] quattro azioni fondamentali per la cybersecurity in Italia, indicando quali tra gli organi elencati nel presente decreto ne sia responsabile:

1) strategia e pianificazione: presidente del Consiglio dei ministri e CISR;
2) prevenzione ed analisi dei rischi: DIS, AISE ed AISI;

[26] Intervento di Luisa Franchina alla IV Cyber Warfare Conference (CWC), organizzata a Roma il 19 giugno 2013 da Centro universitario di studi strategici ed internazionali dell'Università di Firenze (CSSII), Cyber Intelligence and Information Security Centre dell'Università "Sapienza" di Roma (CIS Sapienza) e Istituto per gli studi di previsione e le ricerche internazionali (ISPRI).

3) promozione e diffusione della conoscenza e della consapevolezza: DIS;
4) gestione delle crisi e allertamento: Nucleo per la sicurezza cibernetica, NISP e CERT nazionale.

Infine l'articolo 11 del decreto riporta compiti e doveri degli operatori privati coinvolti nella questione nazionale della cybersecurity, ovvero quelli che forniscono reti pubbliche di comunicazione o servizi di comunicazione elettronica e quelli che gestiscono infrastrutture critiche nazionali ed europee:

- comunicare al Nucleo per la sicurezza cibernetica ogni significativa violazione della sicurezza ed integrità dei propri sistemi informatici;
- adottare *best practices* e misure volte alla sicurezza cibernetica;
- fornire informazioni agli organismi di informazione per la sicurezza, consentendo loro l'accesso alle banche dati d'interesse;
- collaborare alla gestione delle crisi, soprattutto per quanto concerne il ripristino delle funzionalità dei sistemi, delle reti e dei servizi da essi gestiti.

Il decreto intende stabilire degli obblighi a carico del settore privato, affinché questo sia tenuto a collaborare con le istituzioni almeno per quanto riguarda la comunicazione degli eventi cibernetici. È da segnalare che le disposizioni finali del decreto (articolo 13) precisano che da esso non derivano nuovi oneri a carico dello Stato: non è quindi previsto alcun finanziamento a sostegno della realizzazione dell'architettura istituzionale deputata alla sicurezza cibernetica nazionale.

2.5.2 Il Quadro strategico e il Piano nazionale del dicembre 2013

Il 18 dicembre 2013 il Presidente del Consiglio ha adottato, su proposta unanime del CISR, il *Quadro strategico nazionale per la sicurezza dello spazio cibernetico* ed il *Piano nazionale per la protezione cibernetica e la sicurezza informatica*, come auspicato dal DPCM del 24 gennaio 2013[27].

[27] Presidenza del Consiglio dei ministri, *Sicurezza cibernetica: arrivano "Quadro strategico" e "Piano nazionale di protezione"*, Comunicato stampa, 18 dicembre 2013, http://www.governo.it/Notizie/Presidenza/dettaglio.asp?d=74182.

Entrambi i documenti sono stati elaborati dal Tavolo tecnico cyber (TTC) istituito in seno all'organismo collegiale permanente – cosiddetto CISR tecnico – presso il DIS, come da disposizione del DPCM del 24 gennaio 2013. Il TTC è composto dai rappresentanti cyber dei sei "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.

Quadro strategico nazionale (QSN) e Piano nazionale (PN) mirano a delineare un profilo accurato della minaccia cibernetica alla sicurezza delle reti di interesse nazionale, e a definire gli strumenti e le procedure per contrastarla. A questo fine, vengono individuati gli indirizzi strategici e quelli operativi, gli obiettivi specifici e le linee d'azione.

QSN e PN sono entrati in vigore il 27 gennaio 2014[28]. Resi pubblici circa un mese dopo, il 20 febbraio 2014, sul sito del Governo e su quello del Sistema di informazione per la sicurezza della Repubblica[29], sono stati successivamente menzionati in Gazzetta ufficiale ed hanno ricevuto l'approvazione della Corte dei Conti.

Il Quadro strategico nazionale costituisce un documento politico programmatico articolato in quattro anni (2014-2017), che mira ad accrescere le capacità di risposta del paese alle sfide riguardanti lo spazio cibernetico, indirizzando gli sforzi nazionali verso obiettivi comuni e soluzioni condivise. Il QSN "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"[30].

Il documento è articolato in due capitoli e due allegati. Il primo capitolo offre una panoramica delle principali minacce e vulnerabilità dello spazio cibernetico, definendone le tipologie e le caratteristiche fonda-

[28] Si veda il comunicato della Presidenza del Consiglio dei ministri, Dipartimento informazioni per la sicurezza (G.U. n. 41 del 19 febbraio 2014).

[29] Sistema di informazione per la sicurezza della Repubblica, *La cyber strategy italiana*, 20 febbraio 2014, http://www.sicurezzanazionale.gov.it/sisr.nsf/archivio-notizie/la-cyber-strategy-italiana.html.

[30] Presidenza del Consiglio dei ministri, *Quadro strategico nazionale per la sicurezza dello spazio cibernetico*, dicembre 2013, p. 7, http://www.agid.gov.it/sites/default/files/leggi_decreti_direttive/quadro-strategico-nazionale-cyber_0.pdf.

mentali. Secondo il QSN la cosiddetta *cyber threat* si caratterizza per la sua asimmetricità, dovuta al fatto che chi attacca è nella posizione di:

- colpire a distanza, da qualunque parte del mondo esista un accesso alla rete;
- attaccare sistemi altamente sofisticati, sfruttando anche una sola vulnerabilità;
- agire in tempi molto brevi, così da impedire un'efficace reazione difensiva;
- rimanere anonimo o comunque non facilmente individuabile.

Vengono poi indicate quattro macro-categorie di minaccia, che coincidono con quelle della già citata relazione del COPASIR del 2010 (si veda paragrafo 2.3):

1) criminalità cibernetica;
2) spionaggio cibernetico;
3) terrorismo cibernetico;
4) guerra cibernetica.

Quanto alla prima macro-categoria, viene messa in evidenza l'importanza dell'impatto economico del cybercrime, quale rischio di massima priorità, per il benessere e l'economia del sistema paese Italia. Lo spazio cibernetico viene infatti definito come "un dominio virtuale di importanza strategica per lo sviluppo economico, sociale e culturale"[31].

Per proteggere, sfruttare e garantire le opportunità che nascono dall'economia digitale, il Quadro specifica che gli stati devono assumersi la responsabilità primaria della protezione delle reti e delle infrastrutture collocate all'interno del proprio territorio, anche se in larga parte detenute e gestite dal settore privato.

Malgrado lo spazio cibernetico costituisca un dominio che, per sua natura, trascende i confini nazionali, lo stato continua ad essere l'attore principale nella protezione degli assetti critici nazionali. Anche l'elaborazione di un quadro normativo internazionale non può prescindere dall'azione concreta degli stati per attuarlo. "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

[31] Ibidem, p. 10.

tali, quindi, essi sono gli attori maggiormente in grado di sviluppare una robusta capacità operativa nello spazio cibernetico"[32].

Il QSN attribuisce quindi agli stati l'onere della sicurezza cibernetica nazionale, che è una condizione essenziale per la crescita economica e dipende largamente dal contrasto effettivo alle attività criminose condotte sulla rete, come quelle di sabotaggio, spionaggio e furto della proprietà intellettuale.

Riguardo al sabotaggio, l'informatizzazione delle infrastrutture critiche nazionali ha gradualmente consentito di facilitare e velocizzare la fornitura dei servizi, ma ha anche aumentato l'esposizione al rischio informatico. Attacchi di natura cibernetica a queste infrastrutture possono compromettere non solo la *business continuity* aziendale, ma anche l'erogazione di servizi essenziali, quali elettricità, gas, trasporti, ecc., che sono alla base della normale vita quotidiana dei cittadini. La messa in sicurezza delle infrastrutture critiche costituisce perciò un aspetto fondamentale della più ampia sicurezza cibernetica. Anche la protezione delle informazioni digitalizzate si rivela prioritaria dal punto di vista economico, in quanto spionaggio e furto dell'identità intellettuale sono in grado di infliggere ingenti perdite al settore privato che fa uso delle tecnologie dell'informazione e delle comunicazioni.

Il QSN individua le misure – fisiche, logiche e procedurali – alla base di un'adeguata politica di sicurezza delle informazioni:

1) misure fisiche: controllo degli accessi e tracciabilità degli spostamenti del personale autorizzato;
2) misure logiche: impiego di prodotti certificati, software antivirus aggiornati, sistemi di cifratura e di firma digitale, identificazione ed autenticazione degli utenti;
3) misure procedurali: elaborazione di norme e procedure volte a disciplinare gli aspetti organizzativi del processo di sicurezza, controllo sulla consistenza ed affidabilità degli apparati e definizione di ruoli, compiti e responsabilità.

Tali misure hanno lo scopo di arginare tutte le vulnerabilità organizzative, di processo e tecniche, che sono tipiche della rete e dei sistemi informatici, partendo da un approccio di analisi, gestione e mitigazione del rischio. A monte di tale politica di sicurezza si rivela comunque fon-

[32] Ibidem, p. 14.

damentale la promozione di efficaci attività di formazione, sensibilizzazione e responsabilizzazione degli utenti, nell'adozione ed osservanza delle suddette misure.

Il secondo capitolo del Quadro definisce gli strumenti e le procedure per potenziare le capacità cibernetiche dell'Italia, attraverso sei indirizzi strategici e 11 indirizzi operativi. Tutti gli organismi che il DPCM del 24 gennaio 2013 aveva classificato come attori primari dell'architettura nazionale deputata alla sicurezza informatica – presidente del Consiglio dei ministri, CISR, intelligence, Nucleo per la sicurezza cibernetica, NISP e CERT nazionale – sono chiamati a conseguire i seguenti "indirizzi strategici":

1) miglioramento, secondo un approccio integrato, delle capacità tecnologiche, operative e di analisi degli attori istituzionali interessati;
2) potenziamento delle capacità di difesa delle infrastrutture critiche nazionali e degli attori di rilevanza strategica per il sistema-paese;
3) incentivazione della cooperazione tra istituzioni e imprese nazionali;
4) promozione e diffusione della cultura della sicurezza cibernetica;
5) rafforzamento delle capacità di contrasto alla diffusione di attività e contenuti illegali online;
6) rafforzamento della cooperazione internazionale in materia di sicurezza cibernetica.

Gli indirizzi "strategici" sopra elencati sono connessi alla realizzazione di 11 indirizzi operativi:

1) sviluppo delle capacità del Sistema di informazione per la sicurezza della Repubblica, delle Forze Armate e delle autorità preposte alla Protezione e difesa civile;
2) identificazione di un'autorità nazionale per la NIS e potenziamento delle partnership pubblico-privato;
3) definizione di un linguaggio di riferimento unico, chiaro e condiviso;
4) rafforzamento dei rapporti di cooperazione e collaborazione con le organizzazioni internazionali, i paesi alleati e le nazioni amiche;
5) realizzazione della piena operatività del CERT nazionale;
6) adozione di efficaci misure di sicurezza cibernetica e adeguamento normativo;

7) elaborazione di standard, processi di certificazione di conformità e norme tecniche per la sicurezza delle informazioni;
8) cooperazione con il comparto industriale;
9) mantenimento di una stretta coerenza tra le comunicazioni strategiche e le attività condotte nell'ambiente cibernetico;
10) attribuzione ai settori strategici delle PA di adeguate risorse umane, finanziarie, tecnologiche e logistiche;
11) implementazione di un sistema integrato di *information risk management* nazionale.

Il primo obiettivo operativo riguarda l'incremento delle capacità tecniche delle autorità nazionali principalmente coinvolte nella cybersecurity, al fine di migliorare le attività di prevenzione, identificazione, repressione, reazione, contrasto, neutralizzazione e mitigazione degli eventi cibernetici e delle loro conseguenze.

Il secondo obiettivo auspica sia la realizzazione di un'autorità specifica per la NIS, che cooperi con le sue omologhe negli altri paesi dell'UE e con la Commissione europea, sia il rafforzamento delle partnership pubblico-privato, considerate centrali per l'avanzamento della cybersecurity in Italia. Le partnership devono essere agevolate da:

- creazione di tavoli istituzionali congiunti;
- organizzazione di periodiche esercitazioni a livello nazionale;
- obbligatorietà di segnalazione degli incidenti informatici da parte degli operatori privati;
- definizioni di procedure operative e *template* per lo scambio informativo.

Al fine di istituire un meccanismo di scambio reciproco delle informazioni, conoscenze ed esperienze, viene introdotta anche la possibilità di periodi formativi del personale interessato presso le strutture aziendali o le amministrazioni chiamate a tutelarne la sicurezza.

Il terzo obiettivo riguarda la diffusa ambiguità del linguaggio utilizzato nel campo della sicurezza informatica, che spesso complica l'attività di raccordo politico a livello nazionale e, ancor più, europeo. Per questo motivo si raccomanda la definizione di un linguaggio di riferimento unico, chiaro e soprattutto condiviso, in grado di facilitare l'interoperabilità interministeriale ed internazionale.

Il quarto obiettivo promuove la cooperazione con le organizzazioni internazionali, i paesi alleati e le nazioni amiche, nonché la par-

tecipazione attiva dell'Italia alle iniziative internazionali che trattino la materia. Questo obiettivo mira a definire un quadro di regole comuni e di legittimità internazionale; tutelare i flussi informatici legati al mercato unico europeo; favorire lo sviluppo di una politica di difesa cibernetica, in linea con la PSDC; garantire l'alleanza con la NATO e con quei paesi *like-minded* di interesse strategico.

Il quinto obiettivo affronta la questione della realizzazione del CERT nazionale italiano. Come già riportato, a partire dal novembre 2013 è attiva, presso il Nucleo per la sicurezza cibernetica, un'unità di allertamento destinata ad assumere il ruolo di CERT nazionale. Stando alle dichiarazioni del febbraio 2014 di Rita Forsi, direttore dell'ISCOM, e del consigliere militare del Presidente del Consiglio dei ministri, Giorgio Cornacchione, il CERT nazionale è attualmente attivo in fase pilota ed assumerà ufficialmente tutte le sue funzioni entro il 2014[33].

Il QSN propone un modello cooperativo pubblico-privato per la costituzione di un CERT nazionale in grado di agire da collegamento con gli altri CERT pubblici e privati nazionali e da interfaccia con il CERT-EU e quelli degli altri stati. Raccomanda inoltre la piena operatività del neonato CERT-PA e l'impiego efficiente del CERT-Difesa nell'ambito dei piani di operazione, in osservanza delle evoluzioni tecnico-funzionali e procedurali della CIRC (Computer Incident Response Capability) della NATO.

Il sesto obiettivo invita, in via generale, al continuo adeguamento normativo, in base all'evoluzione della tecnologia e dei suoi nuovi utilizzi, affinché sia sempre possibile garantire l'efficacia delle misure nazionali di sicurezza cibernetica.

Il settimo obiettivo concerne l'individuazione di standard specifici per la sicurezza dei prodotti ICT, durante tutta la fase di produzione; l'introduzione di relativi processi di certificazione di conformità a tali standard; l'elaborazione di norme tecniche per garantire la sicurezza delle informazioni (integrità, disponibilità e riservatezza). A tali fini, la previsione di alcuni incentivi di mercato potrebbe rivelarsi di grande impatto.

L'ottavo obiettivo sostiene la cooperazione con il comparto industriale, anche attraverso la predisposizione di servizi pubblici di assistenza e supporto, in particolare delle piccole e medie imprese.

---

[33] Interventi di Rita Forsi e Giorgio Cornacchione al convegno "Le applicazioni del Decreto contro la minaccia cibernetica", organizzato a Roma il 27 febbraio 2014 dal Centro studi difesa e sicurezza (CESTUDIS).

Il nono obiettivo riguarda la correlazione tra piano operativo e piano comunicativo-istituzionale, per garantire la coerenza tra le attività condotte nello spazio cibernetico e le comunicazioni strategiche ufficiali, queste ultime a supporto delle prime.

Il decimo obiettivo prevede il conferimento, a determinati settori delle PA considerati strategici, di tutte le risorse necessarie al conseguimento degli obiettivi indicati nel Quadro.

L'undicesimo ed ultimo obiettivo operativo incoraggia l'implementazione, a livello nazionale, di un sistema integrato di gestione del rischio delle informazioni, nel tentativo di realizzare una struttura efficace di prevenzione, identificazione e gestione della minaccia e di produrre importanti politiche di riferimento.

Il QSN ha anche due importanti allegati. Il primo individua i ruoli e le responsabilità dei soggetti pubblici deputati alla sicurezza cibernetica nazionale. In base al DPCM 24 gennaio 2013, gli attori coinvolti nella cybersecurity sono:

- presidente del Consiglio dei ministri;
- CISR;
- CISR tecnico (tavolo tecnico Cyber);
- comparto intelligence (DIS, AISE, AISI);
- Nucleo per la sicurezza cibernetica (Ufficio del Consigliere militare della PdCM);
- NISP (quale Tavolo interministeriale di crisi cibernetica);
- CERT nazionale.

Il Quadro amplia questa lista, introducendo:

- Agenzia per l'Italia digitale (CERT-PA);
- Ministero degli Affari esteri;
- Ministero dell'Interno;
- Ministero della Difesa (CERT-Difesa);
- Ministero dell'Economia e delle Finanze;
- Ministero dello Sviluppo economico (ISCOM).

Il secondo allegato offre infine un glossario dettagliato dei termini utilizzati nel campo ICT e della cybersecurity, con l'obiettivo di fare chiarezza sul significato di molti concetti, fornendone una definizione ufficiale.

Il *Piano nazionale per la protezione cibernetica e la sicurezza informatica* ha lo scopo fondamentale di dare concreta attuazione al QSN. Il docu-

mento declina tutti gli indirizzi operativi sopra riportati, delineando, per ciascuno, gli obiettivi da raggiungere e le linee d'azione da seguire.

Figura 2 - Relazione tra Quadro strategico e Piano nazionale

Fonte: Piano nazionale per la protezione cibernetica e la sicurezza informatica

Il Piano mira allo sviluppo dei sei indirizzi strategici nell'arco del biennio 2014-2015, stabilendo una "roadmap" per l'adozione delle misure prioritarie volte all'implementazione del Quadro, sulla base di un dialogo che veda la sicurezza informatica nazionale non solo come un obiettivo ma, soprattutto, un processo che coinvolge tutti gli attori interessati a vario titolo alla tematica *cyber*[34].

Per questo motivo il Piano "dovrà essere condiviso con *stakeholder* privati, che costituiscono attori rilevanti nell'ottica di una *partnership* pubblico-privato e, in quanto tali, rappresentano *conditio sine qua non* per lo sviluppo di un'efficiente capacità di sicurezza e difesa cibernetica nazionale"[35].

La centralità delle partnership è evidenziata dai propositi di coinvolgere attivamente gli operatori privati negli eventi di sicurezza cibernetica nazionali ed internazionali, a livello bilaterale e multilaterale, e di rafforzare gli specifici canali di dialogo e consultazione con le istituzioni, anche al fine di dare maggiore impulso all'attivazione del CERT nazio-

[34] Presidenza del Consiglio dei ministri, *Piano nazionale per la protezione cibernetica e la sicurezza informatica*, dicembre 2013, p. 7, http://www.agid.gov.it/sites/default/files/leggi_decreti_direttive/piano-nazionale-cyber_0.pdf.

[35] Ibidem, p. 8.

nale e alla costituzione di una "Computer Incident Response Capability" (CIRC) nazionale integrata.

Inoltre, all'ottavo obiettivo operativo – cooperazione con il comparto industriale – viene anche annunciata la prossima realizzazione di un laboratorio governativo di analisi comparativa dei sistemi ICT di interesse, delle amministrazioni e delle infrastrutture critiche nazionali.

L'istituzione di partnership pubblico-privato rappresenta una sfida importante per il futuro, dalla quale dipenderà il successo delle politiche adottate. A questo scopo l'organizzazione di Tavoli di condivisione e scambio delle informazioni tra istituzioni pubbliche e settore privato nonché università e istituti di ricerca dovrebbe rappresentare la prossima priorità del Governo italiano, sull'esempio delle iniziative in corso in altri paesi europei: ad esempio il Regno Unito ha realizzato numerosi *hub* (nodi) di settore, presso cui si riuniscono periodicamente le principali imprese di ciascun settore critico nazionale e le istituzioni pubbliche deputate alla sicurezza cibernetica.

L'obiettivo di questi Tavoli dovrebbe essere quello di facilitare la collaborazione attiva pubblico-privata, partendo proprio dal punto di vista delle imprese. Il coinvolgimento anche del mondo accademico si rivela necessario al fine di indirizzare la ricerca verso chiari progetti di utilità pratica per entrambi i settori di cui sopra.

Tra gli aspetti più rilevanti del Piano è interessante notare che il decimo obiettivo operativo – attribuzione di risorse adeguate – prevede la definizione delle priorità e dei costi associati alle misure di cybersecurity e cyberdefence per la protezione delle infrastrutture critiche e lo sviluppo delle capacità cibernetiche, nonché l'elaborazione di strumenti normativi e finanziari per l'ottimizzazione e l'eventuale condivisione delle spese tra settore pubblico e privato e tra paesi, in base a determinati programmi di cooperazione nazionale ed internazionale. Il Piano non stabilisce quindi un bilancio per la cybersecurity, ma pone le basi per successive e più che auspicate evoluzioni a livello normativo in questa direzione.

Paolo Lezzi, amministratore delegato della società Maglan che si occupa di *information defence technology*, in un'intervista rilasciata il 13 marzo 2014 ha dichiarato che una potenziale condivisione delle spese tra settore pubblico e privato per gli aspetti di cyberdefence potrebbe esplicarsi tramite la realizzazione di una *task force* nazionale per la sicurezza cibernetica, all'interno della quale strutturare una solida cooperazione tra le parti, incentrata sul ruolo fondamentale della cosiddetta

infrastruttura economica. Quest'ultima, secondo Lezzi, ricomprende l'insieme delle infrastrutture critiche nazionali dei settori energia, trasporti, telecomunicazioni e finanziario, costituendo la vera ossatura del sistema economico italiano.

L'istituzione di questa *task force* avrebbe il pregio di coordinare l'operato – ad oggi alquanto disaggregato – di tutti i soggetti interessati a livello nazionale e di organizzare la cooperazione con gli organi analoghi a livello europeo. Si ricorda che una proposta simile era già stata presentata nel 2003 ed affidata all'Osservatorio permanente per la sicurezza delle reti e delle comunicazioni (si veda paragrafo 1), ma non ha avuto alcun seguito. A parere di Lezzi l'eventuale condivisione delle spese per la cyberdefence – tra Stato ed imprese – dipende in modo cruciale dalla previa istituzionalizzazione della cooperazione pubblico-privata.

Infine, per garantire la piena efficacia del Piano, si legge che le linee d'azione ivi contenute dovranno essere sottoposte a misurazione, attraverso un'apposita matrice elaborata dall'organismo collegiale permanente (cosiddetto "CISR tecnico") per verificare l'attuazione degli interventi previsti dal DPCM del 24 gennaio 2013. Non viene però fornita alcuna indicazione circa i tempi di elaborazione della suddetta matrice e di valutazione del Piano.

Quadro strategico nazionale e Piano nazionale, insieme, costituiscono la strategia nazionale di cybersecurity dell'Italia. Sebbene con un certo ritardo rispetto alla media dei paesi europei più avanzati, nel 2014 anche l'Italia si è infine dotata di una strategia ufficiale per proteggere lo spazio cibernetico.

QSN e PN si propongono non solo di rimanere al passo con i tempi "ma anche di coglierne le 'anticipazioni', così da prevenire le future minacce atte a minare lo sviluppo economico, sociale, scientifico e industriale, nonché la stabilità politico-militare del nostro paese"[36].

Sarebbe auspicabile che, nel prossimo futuro, l'Italia provveda a dotarsi anche di una strategia nazionale di sicurezza. È ora in vigore una strategia specifica per la sicurezza informatica, ma in assenza di una più comprensiva strategia nazionale di sicurezza.

Nel marzo 2014 il Sistema di informazione per la sicurezza della Repubblica ha sottoposto all'attenzione del Parlamento la *Relazione sulla politica dell'informazione per la sicurezza* relativa all'anno 2013. Anche

[36] Ibidem, p. 5.

questa edizione dedica una sezione specifica alla *cyber threat*, quale tipologia principale di minaccia asimmetrica. Essa viene definita come "pervasiva, sofisticata, eseguibile con strumenti di facile accesso ed uso, rapida nelle evoluzioni e dotata di elevata capacità di rimodulazione rispetto agli strumenti posti di volta in volta a difesa di reti e sistemi"[37].

La relazione sottolinea come le attività di monitoraggio intraprese nel 2013 dal comparto intelligence abbiano messo in evidenza il fatto che la concentrazione degli eventi cibernetici maggiormente rilevanti si è tradotta in un significativo aumento delle azioni intrusive volte all'acquisizione di informazioni sensibili e alla sottrazione di *know how* pregiato, a danno di enti governativi e militari, ambasciate, centri di ricerca e società operanti nei settori della difesa e dell'energia.

Tale monitoraggio ha registrato anche numerosi episodi di sottrazione informativa, soprattutto di natura finanziaria, da parte della criminalità organizzata. Ancora una volta, emerge il notevole impatto economico del cybercrime sul sistema paese. In particolare, la relazione mette in guardia sulle molteplici implicazioni di un pericoloso consolidamento del mercato cyber *underground*, sviluppatosi nel *deep web* – dove è possibile acquistare servizi di ogni tipo, finalizzati alla conduzione di attività illecite sulla rete – e della moneta digitale denominata *bitcoin*, quale nuovo strumento di regolazione finanziaria, che permette di garantire l'anonimato e la non tracciabilità delle transazioni.

Una certa attenzione viene poi dedicata al cosiddetto *hacktivism* – principalmente riconducibile al movimento Anonymous – il quale ha registrato, negli ultimi anni, un crescendo in termini di motivazione politico-ideologica e potenziale offensivo. Questo fenomeno sta gradualmente acquisendo una marcata connotazione di antagonismo digitale, complementare ai tradizionali strumenti di protesta. Viene considerata la possibilità di sconfinamento della protesta digitale nell'organizzazione di attacchi dimostrativi di natura cibernetica che possano compromettere la sicurezza di reti e sistemi.

Inoltre, come assoluta novità, la relazione presenta un allegato finale, che riferisce sulle attività svolte in materia di protezione delle infrastrutture critiche materiali e immateriali, nonché di protezione cibernetica e sicurezza informatica nazionale. Nello specifico, vengono analiz-

[37] Sistema di informazione per la sicurezza della Repubblica, *Relazione sulla politica dell'informazione per la sicurezza 2013*, 6 marzo 2014, p. 21, http://www.sicurezzanazionale.gov.it/sisr.nsf/relazione-annuale/relazione-al-parlamento-2013.html.

zati il DPCM del 24 gennaio 2013 ed il Quadro strategico nazionale con il relativo Piano nazionale del dicembre 2013. A tal proposito, la relazione conferma che il Tavolo tecnico cyber (TTC) ha avviato l'esercizio finalizzato a consentire la verifica dell'attuazione delle linee d'azione definite nel Piano nazionale, attraverso l'apposita matrice di valutazione, attualmente al vaglio dei componenti del Tavolo. Ricorda inoltre che dal novembre 2013 è divenuta operativa l'Unità per l'allertamento e la risposta a situazioni di crisi cibernetica, nell'ambito del Nucleo per la sicurezza cibernetica, e che dal gennaio 2014 è entrato in funzione anche il CERT-PA.

Quanto al CERT nazionale, nessun riferimento viene fatto circa i tempi di realizzazione, ma si provvede a definirne chiaramente le attività, di tipo sia reattivo che preventivo, nell'ambito del Ministero dello Sviluppo economico. Le attività reattive saranno evidentemente connesse alle fasi di risposta agli incidenti cibernetici e di recupero delle funzioni da essi compromesse, mentre quelle preventive si caratterizzeranno nel seguente modo:

- mantenimento della continua consapevolezza situazionale;
- definizione e diffusione di linee guida e standard;
- promozione dell'istruzione e sensibilizzazione;
- sviluppo della cooperazione internazionale.

Riguardo alla cooperazione pubblico-privato, la relazione fa riferimento all'istituzione del cosiddetto "tavolo imprese", che si è riunito per la prima nel novembre 2013, con la partecipazione delle dieci imprese strategiche con le quali il DIS ha sottoscritto, in ragione della loro centralità nella *governance* nazionale cibernetica, apposite convenzione ex articolo 11 del DPCM del 24 gennaio 2013. La lista di queste dieci imprese non è stata resa pubblica, ma ne fanno sicuramente parte Telecom, ENEL, ENI e Finmeccanica.

La relazione si chiude ricordando l'importanza della partecipazione dell'Italia alle maggiori iniziative internazionali di settore, anche in previsione della presidenza italiana del Consiglio dell'Unione europea nel secondo semestre del 2014.

2.6 Lo stato di attuazione delle linee guida ENISA

Sulla base di quanto finora esposto, è possibile effettuare una valutazione dello stadio di sviluppo della cybersecurity in Italia, nel corso degli

ultimi venti anni. Durante gli anni novanta una nuova fattispecie di crimine, quello informatico, è stata introdotta al fine di rendere perseguibili i reati commessi sulla rete. Una branca specifica della Polizia di Stato, la Polizia postale, è stata inoltre incaricata di attuare tutte le misure necessarie per contrastare efficacemente il cybercrime. Gli anni duemila sono stati poi caratterizzati da una graduale presa di consapevolezza da parte delle autorità dei rischi derivanti dalla minaccia cibernetica e della necessità di dotarsi degli strumenti adeguati per fronteggiarla. In questi anni l'Italia ha adottato la prima legislazione in termini di tutela delle informazioni gestite dalle Pubbliche Amministrazioni e di protezione delle infrastrutture critiche informatizzate. Sono stati anche approvati il Codice in materia di protezione dei dati personali, il Codice delle comunicazioni elettroniche ed il Codice dell'amministrazione digitale, che hanno contribuito a definire la disciplina nazionale nei rispettivi campi di applicazione. Inoltre, sono stati posti in essere alcuni organi rilevanti ai fini della cybersecurity nazionale, quali l'Osservatorio permanente per la sicurezza e la tutela delle reti e delle comunicazioni, il Centro nazionale per l'informatica nella pubblica amministrazione (poi DigitPA e dopo ancora Agenzia per l'Italia digitale), il Centro nazionale per il contrasto della pedopornografia su Internet (CNCPO), il Centro nazionale anticrimine informatico per la protezione delle infrastrutture critiche (CNAIPIC) ed il NISP. La riforma dell'intelligence italiana del 2007 ha infine attribuito al DIS e alle due agenzie AISE e AISI un ruolo fondamentale nello sviluppo e mantenimento della sicurezza cibernetica.

A partire dal 2011, l'Italia ha cominciato a adeguare il quadro normativo nazionale alle nuove esigenze di cybersecurity, sempre più rilevanti al fine di proteggere la sicurezza e la crescita economica del paese. Sono state trasposte nell'ordinamento italiano importanti direttive europee volte a favorire l'armonizzazione delle legislazioni nazionali e contribuire allo sviluppo della cooperazione intra-europea. In questo quadro, nel 2012 è stata istituita l'Agenzia per l'Italia digitale, con il compito di incentivare lo sviluppo del fattore ICT nel paese e garantire l'applicazione dell'Agenda digitale europea e di quella italiana. L'agenzia svolge un ruolo importante per quanto riguarda l'informatizzazione delle PA e la diffusione di una cultura generale della sicurezza informatica.

Il 2013 ha segnato una svolta nella trattazione italiana della cybersecurity, introducendo importanti documenti nel quadro normativo nazionale. Il DPCM del 24 gennaio 2013 ha definito l'architettura istituzionale deputata alla sicurezza nazionale relativamente alle infrastrutture cri-

tiche informatizzate. Come già riportato, il decreto individua gli organi incaricati di gestire la sicurezza cibernetica in Italia, senza però definire alcuna strategia di contenimento della minaccia e tanto meno predisporre un fondo finanziario *ad hoc*. Il decreto inaugura un anno di crescente interesse per questa materia, che si è chiuso con l'approvazione di due nuovi importanti documenti: il Quadro strategico nazionale per la sicurezza dello spazio cibernetico e il Piano nazionale per la protezione cibernetica e la sicurezza informatica.

Per valutare lo stato dell'arte della cybersecurity in Italia, si è qui ritenuto di partire dall'analisi del già citato documento *National Cyber Security Strategies: Practical Guide on Development and Execution*, redatto dall'ENISA al fine di offrire supporto agli stati nel processo di elaborazione di una propria strategia nazionale di sicurezza cibernetica (si veda paragrafo 1.1). Come già riportato, il testo si caratterizza come un manuale/guida che propone un modello articolato in due fasi successive: una prima di sviluppo ed esecuzione, una seconda di valutazione ed aggiustamento.

Ai fini della presente valutazione, è necessario prendere in esame unicamente la prima fase, che è quella in cui sembra collocarsi attualmente l'Italia. All'interno della fase di sviluppo ed esecuzione di una strategia nazionale di cybersecurity, la guida dell'ENISA individua 18 tappe:

1) stabilire visione, scopo, obiettivi e priorità;
2) seguire un approccio di tipo *risk assessment*;
3) effettuare una ricognizione di politiche, regolamenti e capacità già esistenti;
4) sviluppare una chiara struttura di *governance*;
5) individuare e coinvolgere tutte le parti interessate;
6) stabilire efficaci meccanismi di *information sharing*;
7) elaborare piani nazionali di emergenza;
8) organizzare esercitazioni;
9) fissare dei requisiti base di sicurezza;
10) stabilire meccanismi di *incident reporting*;
11) contribuire alla diffusione della consapevolezza tra gli utenti;
12) incentivare la ricerca e lo sviluppo(R&S) ;
13) rafforzare i programmi di formazione ed educazione;
14) realizzare una capacità di risposta agli incidenti (CERT);
15) fronteggiare il cybercrime;
16) favorire la cooperazione internazionale;
17) creare partnership pubblico-privato;
18) bilanciare sicurezza e privacy.

I punti sopra elencati non hanno carattere esaustivo ma intendono offrire alcuni parametri di riferimento per la realizzazione di un percorso nazionale volto alla sicurezza cibernetica. Altri spunti importanti per la riflessione potrebbero essere l'elaborazione di una terminologia condivisa – questo anche e soprattutto a livello internazionale – e la predisposizione di meccanismi di verifica sistematica ai quali sottoporre, con cadenza regolare, gli sviluppi delle politiche e degli strumenti via via posti in essere.

Relativamente a ciascun punto, l'Italia ha conseguito risultati diversificati. L'analisi che segue prende in considerazione la situazione dell'Italia prima e dopo l'approvazione dei due documenti in ambito cybersecurity – QSN e PN – che hanno introdotto significative novità. La loro approvazione al termine del 2013 ha infatti notevolmente contribuito all'avanzamento della cybersecurity in Italia: in particolare, è stato individuato un chiaro percorso di sviluppo delle capacità cibernetiche nazionali.

Fino al 2013 l'Italia non disponeva di una strategia nazionale di sicurezza cibernetica, pertanto visione, scopo, obiettivi, priorità ed approccio non erano enunciati in alcun documento istituzionale (punti 1 e 2 del manuale ENISA). Era tuttavia evidente l'intenzione del Governo di muoversi in questa direzione, confermata dalla *ratio* della formazione del Gruppo di studio per la sicurezza dell'utilizzo dello spazio cibernetico, istituito con il DPCM del 12 ottobre 2011. Il gruppo era infatti incaricato di effettuare una ricognizione delle strutture esistenti in Italia (punto 3), al fine di porre in essere un Comitato interministeriale preposto all'elaborazione di una strategia nazionale. Sulla base delle politiche e strutture nazionali già disponibili in Italia, il DPCM del 24 gennaio 2013 ha poi indicato gli organi incaricati di gestire la cybersecurity, organizzati secondo una certa gerarchia di *governance* (punto 4).

Nel descrivere queste prime tappe del processo di preparazione di strategia nazionale di sicurezza cibernetica, la guida porta come esempio il Regno Unito, il quale non solo ha elaborato una propria visione nazionale della cybersecurity, ma ne ha anche definito lo scopo, gli obiettivi e le priorità fondamentali. Inoltre, esso ha adottato un approccio alla cybersecurity di tipo *risk assessment* ed ha stabilito una chiara struttura di *governance* nella sua gestione. Il caso britannico costituisce un buon esempio da seguire, per la messa a punto di questi primi obiettivi.

Per quanto riguarda il punto 1 (stabilire visione, scopo, obiettivi e priorità), Quadro strategico e Piano nazionale non enunciano chiaramente una visione italiana della cybersecurity, ma ne definiscono lo scopo, gli

obiettivi e le priorità. La visione è forse deducibile dal complesso dei due documenti, ma non risulta in essi esplicitata in maniera formale, diversamente da analoghi documenti di altri stati. Rispetto agli altri elementi di cui al punto 1, la visione dichiara il fine ultimo della sicurezza cibernetica, senza specificare le metodologie concrete per il suo raggiungimento. Nei documenti di fine 2013, scopo, obiettivi e priorità sono ben individuati attraverso gli indirizzi strategici ed operativi, gli obiettivi fondamentali e le linee d'azione.

Con i documenti del dicembre 2013, anche la metodologia di approccio (punto 2) è stata specificata: l'ultimo indirizzo operativo prevede infatti l'implementazione di un sistema di *information risk management* nazionale, sull'esempio europeo e di molti stati UE.

Il punto 3 (effettuare una ricognizione di politiche, regolamenti e capacità già esistenti) si è rivelato propedeutico all'elaborazione della strategia nazionale: come già riportato, il Gruppo di studio per la sicurezza dell'utilizzo dello spazio cibernetico ha ricevuto proprio questo compito.

QSN e PN hanno anche contribuito a fare maggiore chiarezza sull'architettura di *governance* deputata alla sicurezza informatica nazionale (punto 4), individuata nel DPCM del 24 gennaio 2013. Il primo allegato al QSN descrive infatti la struttura gerarchica di tutti i soggetti pubblici coinvolti nella cybersecurity, al cui vertice sono collocati, in ordine discendente, presidente del Consiglio dei ministri, CISR e Nucleo per la sicurezza cibernetica.

Per quanto concerne il punto 5, la guida suggerisce di individuare e coinvolgere tutte le parti interessate, sia pubbliche che private. Rimanda quindi al concetto di sicurezza partecipata, tutt'altro che semplice da realizzare. Includere il settore privato nel processo di elaborazione della strategia nazionale consentirebbe di definire ruoli e responsabilità di autorità governative, da un lato, ed imprese operanti nel settore, dall'altro lato. A questo proposito, la guida consiglia di attribuire compiti specifici ai proprietari/presidenti delle varie infrastrutture critiche nazionali, piuttosto che ai settori di volta in volta considerati. In base al DPCM del 24 gennaio 2013, le imprese operanti nel settore ICT o da esso dipendenti sono tenute a fornire informazioni circa gli eventi cibernetici subiti, mettendo a disposizione del Governo, ove necessario, le banche dati di interesse. Nessun compito specifico, però, viene loro attribuito nel processo nazionale di sviluppo e mantenimento della cybersecurity. È così istituito una sorta di meccanismo di *information sharing* tra

pubblico e privato, relativo soprattutto alle situazioni di violazioni della sicurezza o dell'integrità dei sistemi informatici aziendali. Tuttavia tale meccanismo risulta non regolamentato ed unidirezionale, nel senso che le informazioni scambiate fluiscono nel solo verso delle autorità di governo. Uno scambio reciproco di informazioni (punto 6) favorirebbe il coinvolgimento attivo delle imprese, agevolando la fiducia e la collaborazione tra le parti. A questo scopo, sarebbe anche utile fissare delle regole precise alla base del meccanismo di comunicazione, privilegiando un approccio settoriale, che istituisca una piattaforma comune per ciascun settore (*provider*, energia, trasporti, ecc.).

Individuare e coinvolgere tutte le parti interessate è un assunto fondamentale alla base del Quadro strategico e del Piano nazionale. Il concetto di sicurezza partecipata, soprattutto con il settore privato, viene presentato come essenziale per un'efficace politica di sicurezza informatica. In quest'ottica, come già riportato, è stato istituito il cosiddetto "tavolo imprese", che riunisce operatori pubblici e rappresentanti delle dieci imprese considerate strategiche per l'Italia, in ragione della loro centralità nella *governance* nazionale cibernetica. Il tavolo si è riunito una sola volta, nel novembre 2013, pertanto è ancora difficile valutarne l'operato. Tuttavia il coinvolgimento concreto di tutte le parti, secondo un approccio che può essere definito *multi-stakeholder*, si articola anche attraverso la messa in pratica di opportuni meccanismi di scambio reciproco delle informazioni che, a parte essere obbligatori in caso di incidenti informatici, mancano ancora di una chiara regolamentazione (si veda oltre).

Un'altra tappa significativa del processo di formulazione di una strategia nazionale di cybersecurity è rappresentata dall'elaborazione di piani nazionali di emergenza (punto 7), affinché sia possibile definire chiaramente cos'è una situazione di crisi e, di conseguenza, individuare le azioni necessarie per gestirla e gli organi incaricati di farlo. L'Italia non dispone ancora di questo tipo di piani, che sono alla base della realizzazione di una buona capacità nazionale di risposta agli incidenti, necessitando di un aggiornamento continuo, anche in considerazione dei risultati emersi durante le esercitazioni. Queste ultime si rivelano fondamentali per il conseguimento di progressi a livello tecnico-operativo.

Le esercitazioni (punto 8) – siano esse nazionali, europee o internazionali – contribuiscono ad innalzare il livello generale delle *capabilities* e delle procedure, incentivando al tempo stesso la cooperazione tra le parti coinvolte nella gestione delle crisi. L'Italia prende regolarmente parte

alle esercitazioni organizzate dall'ENISA, dalla NATO e dal CCD COE di Tallinn. Nel novembre 2013 ha partecipato alla "Cyber Coalition 2013" organizzata dall'Alleanza Atlantica, che ha simulato la difesa di una rete informatica da attacchi "malevoli" al fine di migliorare il coordinamento e la cooperazione e di perfezionare le procedure di scambio informativo tra la NATO ed i paesi partecipanti. Per l'Italia ha partecipato il personale dei CERT dello Stato Maggiore Difesa, dell'Esercito, della Marina, dell'Aeronautica, dell'Arma dei Carabinieri e della Scuola telecomunicazioni (STELMILIT) di Chiavari. Sono intervenuti inoltre esperti delle strutture di sicurezza ICT appartenenti ai ministeri Affari Esteri, Giustizia, Sviluppo economico ed Economia e Finanze, al DIS (Ufficio centrale per la segretezza) e all'Agenzia per l'Italia digitale[38]. La pratica delle esercitazioni è alla base del consolidamento del *know how* tecnico e del progresso tecnologico, nonché della cooperazione internazionale e di quella pubblico-privato. Infatti, come già riportato, in occasione dell'esercitazione "CybIt 2013"[39] sono stati chiamati a partecipare, per la prima volta in Italia, alcuni rappresentanti delle società ENEL e TERNA: questo fatto è emblematico dell'importanza di coinvolgere il settore privato negli aspetti più tecnici della sicurezza cibernetica.

Riguardo al punto 9 (fissazione di requisiti base di sicurezza), l'Italia sperimenta una certa difficoltà, in linea con gli altri stati europei. Si registra infatti una generale incapacità degli stati di elaborare standard tecnici per la sicurezza, siano essi validi all'interno dei propri confini o anche internazionalmente. Anche la *Strategia dell'Unione europea per la cibersicurezza* raccomanda l'adozione di requisiti minimi comuni, in grado di realizzare un mercato unico dei prodotti ICT, a vantaggio della sicurezza di tutta la catena produttiva. La fissazione di requisiti base di sicurezza costituisce un'importante criticità da affrontare, quindi, non solo a livello nazionale ma anche europeo ed internazionale.

Il settimo indirizzo operativo del Quadro strategico nazionale e del Piano nazionale indica la "*compliance* a standard e protocolli di sicurezza"

---

[38] Ministero della Difesa, *'Cyber Coalition 2013': conclusa l'Esercitazione NATO di Cyber Defence*, 29 novembre 2013, http://www.difesa.it/SMD_/Eventi/Pagine/CyberCoalition2013.aspx.

[39] Lo scenario dell'esercitazione "CybIt 2013" si è basato sulla simulazione di un attacco cibernetico a più riprese diretto contro alcune imprese operanti nel settore energetico e contro alcune istituzioni statali, coinvolgendo sia attori pubblici che privati, a differenza dell'edizione precedente del 2012.

come necessaria per garantire un livello elevato di sicurezza cibernetica. Prevede l'aggiornamento del quadro nazionale di riferimento sulla base delle normative NATO ed UE e la costituzione di un sistema per l'accreditamento e l'*auditing* degli enti responsabili dell'emissione di certificati digitali di autenticazione. Ad oggi non risulta ancora chiaro se tali standard e protocolli di sicurezza debbano essere elaborati a livello nazionale, europeo o internazionale. Prevale, in generale, la tendenza a lasciare aperta ogni possibilità, purché vengano conseguiti dei risultati. Attualmente lo standard internazionale più accreditato per la sicurezza informatica è quello ISO/IEC 27001, elaborato dall'Organizzazione internazionale per la standardizzazione (ISO), il quale fornisce i requisiti base di un Sistema di gestione della sicurezza delle informazioni (ISMS, Information Security Management System)[40]. In Italia l'Organismo di certificazione della sicurezza informatica (OCSI), che è attivo presso l'ISCOM e gestisce lo schema nazionale per la valutazione e certificazione della sicurezza dei sistemi e prodotti nel settore ICT, ha adottato lo standard *Common Criteria* ISO/IEC 15408. Ad oggi, però, non vi sono ancora standard obbligatori.

Tornando ai meccanismi di comunicazione, si è detto che il DPCM del 24 gennaio 2013 ha previsto alcuni obblighi in capo agli operatori privati che forniscono reti pubbliche di comunicazione o servizi di comunicazione elettronica accessibili al pubblico e a quelli che gestiscono infrastrutture critiche di rilievo nazionale ed europeo, il cui funzionamento è condizionato dall'operatività di sistemi informatici e telematici. Questi operatori sono tenuti a comunicare al Nucleo per la sicurezza cibernetica tutti gli incidenti informatici che colpiscono i loro sistemi. Il decreto, come già menzionato, non delinea però un chiaro meccanismo di *incident reporting* tra pubblico e privato, a livello nazionale, e tanto meno ne stabilisce regole e principi (punto 10). Un tale meccanismo esiste solo tra *internet service provider*, autorità nazionali competenti, ENISA e Commissione europea (si veda paragrafo 1.2). La messa in opera di efficaci meccanismi di scambio delle informazioni e comunicazione degli incidenti merita le dovute attenzioni delle autorità di governo, al fine di regolamentare la cooperazione pubblico-privato. Un procedimento formale per queste comunicazioni contribuirebbe ad istituzionalizzare

[40] Per maggiori informazioni, si veda *ISO/IEC 27001 - Information security management*, http://www.iso.org/iso/home/standards/management-standards/iso27001.htm.

questo tipo di collaborazione, evitando inutili duplicazioni di sforzi ed il rischio di segnalazioni non pervenute.

Il punto 11 del manuale ENISA riguarda la diffusione di un buon livello generale di consapevolezza dei rischi connessi alla navigazione in rete, affinché gli utenti siano in grado di adottare comportamenti responsabili ed eventuali misure di auto-protezione. Iniziative e campagne di informazione hanno il pregio di sensibilizzare i cittadini su queste problematiche. Ad esempio il mese della cybersecurity, fissato a ottobre, è un periodo in cui tutti gli stati europei si dedicano alla promozione e discussione pubblica delle questioni relative alla sicurezza informatica attraverso forum, *workshop*, conferenze ed eventi appositamente organizzati per i cittadini e le imprese.

I punti 12 e 13 sostengono, rispettivamente, la promozione delle attività di R&S ed il rafforzamento dei programmi nazionali di formazione e educazione: due requisiti fondamentali per l'avanzamento della cybersecurity. In questo ambito sarebbe utile organizzare un dibattito ed una collaborazione strutturata tra settore pubblico e privato, per determinare in maniera congiunta priorità nazionali di investimento in R&S nel settore della cybersecurity. Con riferimento al punto 13, inoltre, la programmazione di percorsi universitari e post-universitari altamente professionalizzanti consentirebbe di creare un gruppo di esperti IT per la cybersecurity.

Estonia e Regno Unito hanno già avviato specifici programmi universitari in questo settore, nell'interesse della salvaguardia nazionale. Negli ultimi anni anche in Italia si è cominciato ad attivare alcuni corsi universitari e post-universitari dedicati alla sicurezza cibernetica, sia dal punto di vista tecnico-informatico che da quello normativo-istituzionale. Ad esempio l'Università di Milano ha lanciato presso il Polo di Crema la prima laurea specialistica in Sicurezza informatica, volta alla formazione di esperti capaci di svolgere attività di ricerca, progettazione, realizzazione, verifica, coordinamento e gestione dei sistemi informatici, nell'ambito della protezione delle reti e delle infrastrutture informatiche nonché del trattamento sicuro e riservato dei dati e delle informazioni[41]. L'Università "La Sapienza" di Roma ha organizzato invece tre percorsi post-universitari dedicati alla cybersecurity: il master in Gestione della

[41] Per maggiori informazioni, si veda http://www.ccdinfcr.unimi.it/it/index.html.

sicurezza informatica, il master in Sicurezza dei sistemi e delle reti e il master in Governance e audit dei sistemi informativi[42].

Roberto Baldoni, direttore del centro di ricerca Sapienza in Cyber Intelligence and Information Security (CIS Sapienza), ha dichiarato nel febbraio 2014 che una delle maggiori difficoltà per l'Italia è il reperimento di esperti di sicurezza informatica che abbiano sostenuto studi specifici in materia: in Italia esiste, ad esempio, un solo programma universitario interamente dedicato al *reverse engineering*, una branca dell'ingegneria informatica che si occupa di ricostruzione delle architetture software danneggiate o compromesse[43]. È quindi importante che venga ampliata l'offerta formativa delle scuole di ingegneria informatica attraverso l'attivazione di corsi di laurea specificamente dedicati alla cybersecurity, al fine di andare incontro alle nuove esigenze delle imprese e della sicurezza nazionale.

La diffusione di una cultura generale della sicurezza, l'incentivazione delle attività di R&S ed il rafforzamento dei programmi formativi-educativi (punti 11, 12 e 13) costituiscono tutti aspetti fondamentali del processo di sviluppo della cybersecurity in Italia. Affinché questi obiettivi siano perseguibili è però indispensabile disporre di fondi finanziari *ad hoc*, attualmente non disponibili. Il mondo della ricerca, in particolare, è in grado di svolgere un ruolo importante nel conseguimento di progressi in materia. A questo proposito, è necessario avvicinare la ricerca alle esigenze di settore, tramite l'attivazione di programmi di diretto interesse del Governo e delle imprese.

I suddetti programmi educativi hanno lo scopo di formare la classe di analisti ed esperti informatici, capaci di operare all'interno dei CERT, ossia delle squadre di risposta alle emergenze cibernetiche. La realizzazione dei CERT nazionali è un elemento imprescindibile di una buona strategia nazionale di cybersecurity, poiché su di essa si basa la reale capacità di uno Stato di rispondere efficacemente agli attacchi e ripristinare prontamente i servizi danneggiati (punto 14). Come già riportato, l'Italia ha disposto l'istituzione di un proprio CERT nazionale il quale, però, non è ancora entrato in funzione. Attualmente sono operativi un CERT-Difesa ed un CERT-PA, quest'ultimo inaugurato nel 2014.

---

[42] Per maggiori informazioni, si veda http://mastersicurezza.uniroma1.it.

[43] Intervento di Roberto Baldoni al convegno "Le applicazioni del Decreto contro la minaccia cibernetica", organizzato a Roma il 27 febbraio 2014 dal Centro studi difesa e sicurezza (CESTUDIS).

Il quinto indirizzo operativo di QSN e PN, oltre a raccomandare l'avvio del CERT nazionale, incoraggia anche la costituzione di una "Computer Incident Response Capability" (CIRC) nazionale integrata e lo sviluppo del CERT-PA e dei CERT ministeriali "quali soggetti erogatori di servizi di assistenza tecnica, ricerca e sviluppo, formazione e informazione per i rispettivi utenti, pubblici e/o privati, operando sulla base di un approccio sia proattivo che reattivo"[44]. Questi obiettivi restano prioritari per un'adeguata gestione della minaccia informatica ed una pronta risposta agli attacchi/incidenti che si verificano nel cyber spazio.

Per quanto riguarda la lotta al cybercrime (punto 15), l'Italia ha dimostrato un notevole impegno fin dagli anni novanta. Si ricorda che le primissime politiche nazionali in ambito cyber hanno riguardato la modifica del Codice penale e del Codice di procedura penale, per comprendere la fattispecie dei reati informatici. Da allora, la Polizia postale resta incaricata di predisporre tutte le misure atte a contenere la minaccia cibernetica, comprese quelle di *law enforcement*. Sono state inoltre realizzate numerose collaborazioni tra soggetti pubblici e privati al fine di fronteggiare il crimine informatico (si veda paragrafo 2.3).

Dal punto di vista della cooperazione internazionale e della realizzazione di partnership pubblico-privato (punti 16 e 17), l'Italia non manca di apportare il proprio contributo, come attesta l'elevato numero di esercitazioni europee ed internazionali cui essa partecipa regolarmente, il costante dialogo tra autorità di governo nazionali ed istituzioni europee, tra cui in particolare l'ENISA, e le tante collaborazioni pubblico-privato instaurate per promuovere lo sviluppo del fattore ICT (si veda paragrafo 2).

Come già rilevato, un attivo coinvolgimento del settore privato nel processo di elaborazione di una strategia nazionale di cybersecurity contribuirebbe a rafforzare la cooperazione in questo ambito. Infatti, sebbene siano state realizzate svariate intese tra Governo ed imprese, queste ultime continuano a dimostrare una certa riluttanza nel comunicare alle autorità pubbliche gli incidenti cibernetici che interessano reti e sistemi aziendali, per motivi di reputazione e scarsa fiducia negli interventi governativi. Uno sforzo maggiore dovrebbe essere compiuto in questa direzione, per favorire il dialogo costruttivo tra i due settori. La creazione di partnership pubblico-privato (punto 17) costituisce il vero

[44] Presidenza del Consiglio dei ministri, *Piano nazionale per la protezione cibernetica* ..., cit., p. 19.

landmark del Quadro strategico e del Piano nazionale: la sua centralità viene messa più volte in evidenza, in osservanza di "un approccio olistico e di una forte unitarietà d'intenti"[45]. I due documenti del dicembre 2013 contribuiscono notevolmente a rafforzare il concetto di sicurezza partecipata, ritenuto alla base della strategia di cybersecurity.

L'ultimo punto (18) concerne il bilanciamento tra esigenze di sicurezza nazionale e diritto personale di privacy. Questo tema ha recentemente acquisito grande rilevanza, in seguito alle rivelazioni di Edward Snowden sulla massiccia attività di spionaggio indiscriminato condotta dalla National Security Agency statunitense. L'emergere del caso *Datagate* nel 2013 ha acceso il dibattito internazionale: fino a che punto le ragioni di sicurezza di uno stato lo autorizzano a violare il diritto di privacy dei propri cittadini e di quelli di altri stati?

L'Italia ha predisposto una legislazione in materia di tutela delle informazioni e dei dati personali già all'inizio degli anni duemila. Come riportato, nel 2002-2003 sono stati approvati importanti direttive e codici in materia, che da allora ne dettano la disciplina. Tuttavia il corretto bilanciamento tra esigenze di sicurezza nazionale e diritto di privacy dei cittadini non dipende unicamente dalla legislazione nazionale o internazionale, ma anche e soprattutto dall'utilizzo che i vari Governi decidono di fare degli strumenti tecnologici a loro disposizione.

I 18 punti della guida ENISA sono tutti singolarmente migliorabili nella loro realizzazione, e sopratutto suscettibili di verifica sistematica nel tempo, ma certamente non esauriscono la gamma dei possibili margini di avanzamento della cybersecurity. A questo proposito, il problema dell'ambiguità di linguaggio continua a rappresentare un ostacolo rilevante, non solo per l'attività di raccordo politico, ma anche per quella di ricerca scientifica. L'elaborazione di una terminologia condivisa a livello internazionale contribuirebbe in maniera significativa a facilitare il dialogo e la cooperazione tra le parti, che sarebbero così agevolate dall'utilizzo di definizioni e concetti comuni.

In conclusione, l'Italia ha iniziato ad occuparsi sistematicamente ed in maniera permanente di cybersecurity in tempi relativamente recenti e nel 2013 ha compiuto notevoli passi in avanti nell'adeguata trattazione della questione. Indubbiamente resta ancora molto da fare, ma negli ultimi anni sono stati approvati importanti documenti istituzionali in

[45] Presidenza del Consiglio dei ministri, *Quadro strategico nazionale per la sicurezza dello spazio cibernetico*, cit., p. 6.

materia e si è assistito alla diffusione in ambito governativo-imprenditoriale-accademico del dibattito sulla sicurezza informatica, quale minaccia crescente alla sicurezza degli stati. Questo interesse sembra destinato ad aumentare in futuro, in nome di un concetto di sicurezza nazionale che implichi la necessaria protezione della vita quotidiana dei cittadini per garantire la crescita economica del paese, leva fondamentale della sicurezza.

In base alla guida dell'ENISA la situazione italiana risulta alquanto modificata in seguito all'approvazione degli ultimi due documenti del dicembre 2013, che hanno introdotto importanti novità nel panorama italiano della sicurezza cibernetica: "Con questi due documenti l'Italia si dota di una strategia [...] 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"[46].

Il 2013 ha introdotto elementi nuovi nel contesto normativo italiano relativo alla sicurezza informatica, delineando una situazione di maggiore consapevolezza dei rischi e delle opportunità derivanti dalla dimensione cibernetica. È apprezzabile la celerità con la quale l'Italia, nell'arco di dodici mesi, ha approvato tre documenti di estrema rilevanza ai fini della cybersecurity nazionale.

Le priorità per il 2014 sono l'avvio del CERT nazionale e la piena operatività del CERT-PA, la costituzione di un'agenzia nazionale per la NIS e, auspicabilmente, l'elaborazione di una più comprensiva strategia nazionale di sicurezza. Sarà inoltre importante istituire tavoli di condivisione e scambio delle informazioni, sull'esempio del "tavolo imprese", che riuniscano settore pubblico, privato ed anche accademico, al fine di dare concreta attuazione alla tanto raccomandata cooperazione tra le parti.

[46] Ibidem, p. 7.

Conclusioni

Con il presente lavoro si è inteso tracciare una panoramica europea delle crescenti sfide che si originano nel dominio cibernetico il quale, pur generando molte opportunità di sviluppo, è causa di vulnerabilità alla sicurezza e all'economia degli stati nazionali. L'obiettivo di questo studio è stato quello di definire la posizione dell'Italia nello scenario europeo, soprattutto per quanto riguarda l'adeguamento normativo alle nuove esigenze di cybersecurity. Il contesto europeo resta fondamentale per la piena comprensione degli sviluppi italiani in materia, dal momento che le dinamiche nazionali degli stati membri sono in molti casi guidate dalle politiche comunitarie.

La cybersecurity in Europa rappresenta allo stato attuale un vero *work in progress*. L'approccio europeo alla sicurezza cibernetica ha proceduto in questi anni a passi relativamente lenti, soprattutto se paragonati a quelli di paesi come Stati Uniti o Regno Unito. Ciò è largamente dovuto all'assetto stesso dell'Unione che, ovviamente, deve mettere d'accordo molti e più diversi punti di vista nazionali. L'UE ha quindi registrato un ritardo nella formulazione di una propria strategia ma la sua approvazione nel 2013 è apprezzabile nella prospettiva di un'auspicabile evoluzione delle sue capacità di affrontare adeguatamente la questione della cybersecurity. La tematica necessita infatti di un'adeguata trattazione non solo a livello nazionale ma anche e soprattutto a livello UE, considerato che la cybersecurity è per definizione una questione che travalica i confini nazionali e necessita di una gestione multinazionale.

L'approvazione della *Strategia dell'Unione europea per la cibersicurezza* (7 febbraio 2013) è la base per la necessaria evoluzione verso l'elaborazione di strumenti più specifici dal punto di vista operativo, come il relativo Piano d'azione. La strategia infatti non arriva a definire il lato più squisitamente tecnico-operativo della cybersecurity, ma ne stabilisce le linee essenziali. Coerentemente con gli scopi ed obiettivi di ogni documento strategico enuncia i valori chiave alla base dell'approccio europeo e le buone pratiche da seguire per raggiungere risultati significativi.

La strategia europea ha contribuito a definire le priorità in ambito sicurezza cibernetica, le quali ruotano principalmente attorno a due capisaldi: la lotta al crimine informatico e la protezione delle infrastrutture

critiche informatizzate. Questi macro-aspetti della cybersecurity costituiscono il nocciolo duro della visione europea, che dal 2000 mantiene queste due priorità in cima alla *to do list* per la sicurezza cibernetica. La strategia ha anche contribuito a mettere in evidenza la necessità per gli stati membri di dotarsi di adeguati strumenti, normativi ed operativi, al fine di arginare le minacce provenienti dal cyber spazio, minacce che attentano non solo alla sicurezza nazionale ed europea ma, soprattutto, alla crescita economica. La grande maggioranza degli attacchi cibernetici mira infatti all'acquisizione di vantaggi economici: rispetto ai crimini informatici e allo spionaggio industriale tramite mezzi cyber i timori relativi al cyber terrorismo e la cyber war risultano spesso sovradimensionati. Attualmente la vera priorità è il contenimento del cybercrime, il cui impatto economico – spesso sottostimato – comporta ingenti danni al benessere dei cittadini e del sistema paese nel suo complesso.

Il secondo caposaldo delle politiche europee e nazionali in ambito cybersecurity è la protezione delle infrastrutture critiche informatizzate. Esse costituiscono l'ossatura del sistema di fornitura dei servizi essenziali, che sono alla base delle funzioni chiave delle società moderne e dei singoli che le compongono. La compromissione o l'interruzione di un servizio è causata generalmente da un incidente – ambientale o connesso all'errore umano – piuttosto che da un attacco deliberato, pertanto la distinzione tra attacchi volontari ed eventi accidentali si rivela meno importante che la pronta definizione delle attività di risposta e recupero del servizio. In particolare, minimizzare i tempi per la fase di ripristino costituisce un obiettivo importante per il contenimento dei danni associati ad eventi cibernetici. È fondamentale però non trascurare la possibilità che attacchi di natura cibernetica aventi come bersaglio sistemi informatici privati o governativi possano divenire una nuova arma di tipo economico, politico e militare.

La lotta al cybercrime e la protezione delle infrastrutture critiche informatizzate – gli aspetti più importanti della sicurezza cibernetica – richiedono un'adeguata trattazione, come già evidenziato, non solo a livello nazionale, ma anche europeo; e questo sia da un punto di vista normativo che operativo e procedurale.

Il coordinamento transfrontaliero appare tutt'altro che semplice da realizzare, considerata la generalizzata reticenza degli stati nel rivelare informazioni riservate riguardanti i propri assetti strategici. Eppure, per incrementare il livello di resilienza cibernetica è essenziale non solo investire sul fattore tecnologico ma anche cercare di coordinare tutti gli

attori coinvolti, onde evitare inutili duplicazioni dei costi, facilitare lo scambio di informazioni e velocizzare i tempi di realizzazione.

Al fine di promuovere la cooperazione intra-europea, l'Unione ha creato l'Agenzia di sicurezza delle reti e dell'informazione (ENISA), che dal 2004 opera per migliorare le capacità nazionali di ciberresilienza e favorire il dialogo tra stati membri, attraverso l'elaborazione di linee guida e l'individuazione di *best practices*.

Le attività di scambio internazionale delle informazioni dovrebbero risultare agevolate dall'istituzione di un chiaro meccanismo di *incident reporting*, volto ad incentivare i *provider* – ma anche le imprese – a rendere pubblici gli attacchi cibernetici subiti, coinvolgendo le autorità nazionali competenti e, di seguito, le istituzioni europee interessate e gli altri stati. Si rende quindi necessaria la creazione di un meccanismo di *reporting* che sia obbligatorio e non volontario. La questione della resistenza operata dal settore privato potrebbe essere parzialmente risolta tramite l'istituzione dell'anonimato o, meglio, la classificazione di certe informazioni che sarebbero così note solo alle istituzioni governative.

La pratica dell'*information sharing* a livello europeo e nazionale è alla base del consolidamento di un atteggiamento costruttivo finalizzato al coordinamento politico e al progresso tecnologico, fondamentale per la trattazione adeguata della sicurezza cibernetica. Lo scambio di informazioni ed esperienze dovrebbe coinvolgere le istituzioni europee e gli attori statali, ma anche le imprese e i singoli cittadini. Tuttavia la realtà dei fatti scoraggia questi propositi: solo in pochi casi gli incidenti informatici vengono comunicati a chi di dovere e, nella migliore delle ipotesi, questo avviene molti mesi dopo che si è verificato l'incidente. Esiste una forte riluttanza a rendere pubblici gli attacchi subiti, per ragioni di immagine e reputazione: molto spesso le imprese e gli stessi stati preferiscono tacere al riguardo per non intaccare il proprio *status* e rivelare falle nel proprio sistema. Lo sviluppo del dialogo tra le parti, anche attraverso l'istituzione di opportuni meccanismi obbligatori di comunicazione, costituisce quindi un obiettivo importante per il futuro.

Compito dell'ENISA è quello di promuovere un vero e proprio cambio di mentalità, che diffonda una nuova cultura della sicurezza delle reti e delle informazioni basata sulla fiducia, la trasparenza e l'*information sharing*. Attualmente in Europa quest'ultimo può essere definito unidirezionale, nel senso che non esiste un obbligo per le autorità pubbliche di fornire informazioni al settore privato, il quale, al contrario, ha il dovere di fare rapporto alle autorità. La predisposizione di un meccanismo bidi-

rezionale contribuirebbe ad incrementare la fiducia reciproca e ad istituzionalizzare la collaborazione pubblico-privato.

Perché questo sia realizzabile, è essenziale che gli stati sostengano la legislazione e le iniziative europee in questo campo, favorendone l'implementazione al livello nazionale e facilitando la cooperazione. A questo proposito è prioritario che tutti gli stati membri provvedano ad istituire un proprio CERT nazionale, al fine di monitorare le minacce che si originano nel cyber spazio ed attuare le misure di risposta ad eventi di natura cibernetica.

Nel settembre 2012 l'Unione ha deciso di creare il CERT-EU, il quale dovrebbe collaborare attivamente con i CERT nazionali degli stati membri e con alcune grandi compagnie di ICT per garantire la sicurezza dello spazio cibernetico europeo. A questo punto diventa perciò cruciale che tutti gli stati si adeguino, realizzando strutture simili e consentendo un'efficiente attività di raccordo a livello UE. Tali attività dovrebbero beneficiare di strutture verticali ed orizzontali, che siano in grado di realizzare la cooperazione sia tra i CERT nazionali e le istituzioni europee sia tra questi e i vari *stakeholder* privati sia, infine, tra i CERT nazionali stessi.

Ad oggi sono 23 gli stati membri dell'Unione europea che si sono dotati di un proprio CERT nazionale. Da questi restano esclusi Bulgaria, Cipro, Croazia, Grecia, Irlanda e Italia, la quale non ha ancora provveduto a realizzare il proprio CERT nazionale, come da disposizione del DPCM del 24 gennaio 2013. Attualmente in Italia sono attivi un CERT-Difesa ed un CERT-PA, quest'ultimo inaugurato nel 2014.

La cooperazione tra settore pubblico e privato, dentro e fuori gli stati, è importante tanto quanto quella internazionale, soprattutto perché la maggior parte degli incidenti informatici coinvolge e colpisce proprio i privati. Le grandi compagnie industriali hanno cominciato da tempo a dotarsi di sistemi di sicurezza informatica in grado di arginare la possibilità di attacchi e questo le ha messe in condizione di fare progressi in maniera più rapida rispetto a molti stati europei.

Data la relativa maggiore esperienza del settore privato in questo campo, la realizzazione di partnership pubblico-privato consentirebbe di coordinare gli sforzi e ridurre i costi, conseguendo risultati migliori in tempi più brevi. Tali partnership si dimostrerebbero vantaggiose per entrambe le parti: il *know how* del privato potrebbe trarre beneficio dall'autorità regolativa ed impositiva del Governo nazionale, conseguendo obiettivi altrimenti difficili da realizzare senza chiari obblighi.

Affinché ciò sia possibile, è importante pensare la cybersecurity al di là delle mere logiche di *business continuity*, in uno sforzo di rinnovata mentalità e costruttivo atteggiamento. Coinvolgere il settore privato significa anche promuovere il concetto di sicurezza funzionale, il quale si prefigge la continuazione delle funzioni chiave della società moderna.

Per inserire la cybersecurity all'interno di questa visione è necessario far sì che il settore privato aziendale abbandoni un'impostazione individualista e diventi consapevole dell'impatto che il cyber ha sulla vita economica dell'intero paese. Solo un pieno coinvolgimento delle imprese nel meccanismo istituzionale può creare le condizioni per un connubio tra settore pubblico e privato, in questo campo più essenziale che in altri.

Come già osservato, vi è un altro aspetto problematico della cooperazione nel dominio cibernetico: per sua natura esso è difficilmente contenibile all'interno di confini precisi, anche se le opinioni al riguardo divergono. È piuttosto diffusa l'idea secondo la quale il cyber costituirebbe un *global common*. I sostenitori di questa tesi considerano lo spazio cibernetico come un bene comune, in quanto tale sottoposto al regime di *res communis omnium*, che presuppone l'inappropriabilità del bene e la sua libertà d'uso.

Il dibattito su questo tema è aperto ed alcuni non condividono questa impostazione, soprattutto in considerazione del fatto che il cyber spazio risulta in larghissima parte posseduto da soggetti privati. Su questo tema, James Andrew Lewis, Senior Fellow del CSIS di Washington, ha sostenuto che lo spazio cibernetico non può essere considerato un *commons*, ma piuttosto un "condominio", in cui tutti i proprietari condividono la stessa struttura, dotata di poche regole e di una debole autorità di regolamentazione. Secondo Lewis, il cyber spazio possiede dei confini entro i quali gli stati si sentono, o si sentiranno tra breve, legittimati a rivendicare la propria sovranità. Alcuni governi hanno infatti paragonato il cyberspazio al mare territoriale, accessibile dall'esterno ma soggetto al proprio controllo. L'estensione della sovranità nazionale al dominio cibernetico avrebbe come conseguenza quella di ridefinirne l'architettura, con le sue regole e la sua *governance*. A parere di Lewis, questa prospettiva si rivela molto più probabile di quanto possa sembrare.

Il dibattito sulla natura dello spazio cibernetico è tutt'altro che teorico, essendo alla base della cooperazione internazionale. È quindi prioritario chiarire le intenzioni della comunità internazionale in riferimento alla gestione della *governance* della dimensione cibernetica: solo in un'ottica di approccio *multi-stakeholder*, basato sulla partecipazione

attiva di tutti gli attori interessati, pubblici e privati, la cooperazione può essere possibile.

Come evidenziato, tale cooperazione è intesa sia a livello nazionale, per quanto riguarda la creazione di partnership pubblico-privato; sia a livello europeo, con riferimento all'importanza, per gli stati e per le rilevanti istituzioni ed agenzie dell'UE, di comunicare ed agire insieme nell'ambito dell'Unione; sia, infine, a livello internazionale, con altri attori statali e non.

Il progetto europeo per la cybersecurity dipende in modo cruciale anche dall'adeguamento delle risorse industriali e tecnologiche. Di notevole rilievo è il fatto che la maggior parte dei prodotti e servizi ICT utilizzati in Europa siano realizzati altrove. Preso atto dell'attuale assetto del mercato mondiale in questo settore, si rende opportuno lo sviluppo, ad opera della Commissione europea, di standard di sicurezza e regimi di certificazione obbligatori, per garantire la sicurezza degli approvvigionamenti in particolare nei settori economici critici (sistema industriale di controllo, infrastruttura dell'energia e dei trasporti).

Per garantire la sicurezza dei prodotti ICT usati in Europa è quindi necessario controllare ogni singola fase della catena produttiva, con tutte le problematiche connesse alla dislocazione di esse in diverse aree del mondo. L'elaborazione di standard di sicurezza contribuirebbe ad accrescere il livello di fiducia nei prodotti ICT e, di conseguenza, anche il grado di protezione dei dati personali. La realizzazione di un mercato europeo digitale unico e sicuro avrebbe perciò il pregio di incrementare la sicurezza dei cittadini europei e, al tempo stesso, di attrarre investimenti a beneficio di domanda ed offerta.

Attualmente si discute sull'eventualità di stabilire degli standard o *security label* a livello europeo, validi in tutti gli stati membri. Comincia a farsi strada l'idea che sia necessario un intervento pubblico più coercitivo, a livello europeo ed anche nazionale. Secondo questa prospettiva spetterebbe all'Unione stessa il compito di fissare degli standard obbligatori di sicurezza e di predisporre tutte le misure atte a garantire una costante collaborazione tra il settore pubblico e quello privato e tra i Governi e le istituzioni europee.

A questo scopo la *Strategia dell'Unione europea per la cibersicurezza* del 2013 propone una serie di misure legislative da adottare a livello nazionale, la più significativa delle quali prevede la fissazione di "requisiti minimi comuni" per la sicurezza delle reti e delle informazioni. Tali requisiti obbligherebbero gli stati a designare le autorità competenti,

costituire i CERT e adottare le strategie e i piani d'azione nazionali per la NIS.

La fissazione di requisiti base di sicurezza costituisce un importante ostacolo da superare nel prossimo futuro, per la messa in sicurezza dei sistemi e delle reti. Non risulta chiaro se tali standard e protocolli di sicurezza debbano essere elaborati a livello nazionale, europeo od internazionale, in quanto generalmente prevale, a questo stadio, la tendenza a lasciare aperte queste diverse possibilità. Ad oggi, non esistono standard obbligatori.

La strategia europea di sicurezza cibernetica costituisce una svolta dal punto di vista normativo, poiché rappresenta il primo ed unico documento strategico europeo dedicato alla questione della cybersecurity e propone una serie di principi e valori chiave, necessari per la messa in atto delle azioni da intraprendere. In un panorama europeo nel quale non tutti gli stati membri si sono dotati di una propria strategia nazionale, l'Unione tenta di stimolare l'attenzione verso questa sfida crescente, così da non trovarsi impreparata in caso di crisi. Sono state così gettate le basi per importanti sviluppi futuri, che vedano l'elaborazione di regole precise da rispettare e l'istituzione di chiari meccanismi di comunicazione tra le parti.

È importante che l'Unione compia presto i prossimi passi nella direzione di una maggiore definizione di una politica di cybersecurity e di un potenziamento degli strumenti già posti in essere. In parallelo, è fondamentale che anche gli stati seguano lo stesso esempio, così che tutti i vari livelli di *governance* europea godano di una buona consapevolezza situazionale e di adeguate *capabilities* e procedure.

In futuro l'UE dovrà provvedere a colmare le lacune ancora esistenti nell'organizzazione del sistema europeo di cybersecurity. Ad esempio la questione dei finanziamenti necessita di una maggiore definizione, sia a livello europeo che nazionale, considerata la sua vitale importanza per la messa in atto di politiche e strumenti adeguati. Lo stanziamento di un fondo finanziario per la cybersecurity si rivelerebbe opportuno, sull'esempio di paesi come gli Stati Uniti ed il Regno Unito.

Significative novità dovrebbe provenire dalla prossima approvazione della direttiva europea sulla cybersecurity – la cui proposta è stata presentata congiuntamente alla strategia del 7 febbraio 2013. La direttiva potrebbe offrire degna copertura al settore ICT per quanto riguarda l'attuazione della direttiva 2008/114/CE "relativa all'individuazione e

alla designazione delle infrastrutture critiche europee e alla valutazione della necessità di migliorarne la protezione".

Importanti sviluppi sono inoltre attesi relativamente alla legislazione sul crimine informatico: negli ultimi anni, la Proposta di direttiva sul cybercrime è stata più volte discussa dal Parlamento europeo – da ultimo nel luglio 2013 – ma ad oggi non è stata ancora approvata.

La lotta al cybercrime necessita di adeguati strumenti e, in particolare, di legislazioni forti ed efficaci, di meccanismi di *law enforcement* e di buone capacità tecnico-operative. L'UE può coordinare l'attività dei singoli stati, facilitando un approccio collaborativo che metta insieme le autorità giudiziarie e gli *stakeholder*, ai vari livelli dell'Unione. L'approvazione della direttiva sul cybercrime potrebbe contribuire a definire gli strumenti, i ruoli e le responsabilità in questo campo.

È infine opportuno ricordare che, per incrementare la sicurezza interna ed esterna all'Unione, il Consiglio europeo del dicembre 2013 ha chiesto l'elaborazione entro il 2014 di un "Quadro strategico UE in materia di ciberdifesa", coerentemente con gli sforzi della NATO, su proposta dell'Alto Rappresentante per gli affari esteri e la politica di sicurezza e in collaborazione con la Commissione e l'Agenzia europea di difesa. Pertanto, è prevedibile che, nel prossimo futuro, anche la cyberdefence subisca un necessario avanzamento, a livello normativo e tecnico-operativo.

Rispetto alla media europea, l'Italia ha registrato un ritardo nella predisposizione delle adeguate politiche di cybersecurity, giungendo all'approvazione di una propria strategia nazionale solo nel dicembre 2013. Ad inaugurare questo anno di crescente interesse per la materia è stato il DPCM del 24 gennaio 2013 che ha definito l'architettura istituzionale deputata alla sicurezza nazionale relativamente alle infrastrutture critiche informatizzate. A dicembre 2013 il Quadro strategico nazionale ed il relativo Piano nazionale hanno stabilito gli indirizzi strategici ed operativi per la messa in sicurezza delle attività condotte nel cyber spazio.

Le sfide, immediate e future, lanciate dalla cybersecurity alla sicurezza e alla crescita economica dell'Italia richiedono un atteggiamento proattivo, che coinvolga non solo le istituzioni di governo, ma anche e soprattutto il settore privato e i singoli cittadini. Il concetto di "sicurezza partecipata" assume, nel contesto cibernetico, un rilievo fondamentale in quanto coinvolge un'ampia categoria di attori – pubblici e privati – tutti necessari per un'efficace gestione della minaccia. In questo quadro

l'intelligence costituisce solo una delle molteplici leve della sicurezza nazionale.

Nel corso del 2013 l'Italia sembra aver colto l'importanza di questo approccio multi-settoriale e *multi-stakeholder*, come si evince non solo dagli ultimi documenti approvati in materia ma anche dalle numerose iniziative intraprese a livello nazionale ed internazionale. La realizzazione della sicurezza cibernetica deve dispiegarsi su questi due livelli: quello interno, con la preparazione di un *framework* strategico nazionale, e quello internazionale, con una maggiore cooperazione e l'elaborazione di regole e pratiche comuni, ma anche di una terminologia condivisa.

I documenti normativi del 2013 hanno attribuito ruoli e competenze specifiche a determinati organi, incaricati di gestire la sicurezza cibernetica in Italia. Il Comitato interministeriale per la sicurezza della Repubblica (CISR) ha ricevuto il compito di elaborare – soprattutto attraverso il Tavolo tecnico Cyber (TTC) – gli indirizzi generali e gli obiettivi fondamentali in materia di sicurezza informatica e di incoraggiare la realizzazione delle iniziative necessarie per garantire la partecipazione dell'Italia ai consessi di cooperazione internazionale, soprattutto in ambito UE e NATO. Deve inoltre formulare proposte di intervento normativo ed organizzativo volte a potenziare le misure di prevenzione e risposta alla minaccia cibernetica e quelle per la gestione delle crisi.

Il DIS, coadiuvato dalle due agenzie AISE ed AISI, si occupa della prevenzione ed analisi del rischio, nonché della trasmissione di tutte le informazioni rilevanti ai fini della cybersecurity al Nucleo per la sicurezza cibernetica, alle Pubbliche Amministrazioni e agli altri soggetti interessati, anche privati. Le due agenzie conducono, nei loro rispettivi ambiti di attribuzione, tutte le attività di ricerca e di elaborazione informativa finalizzate alla protezione cibernetica e alla sicurezza informatica nazionali.

Il Nucleo per la sicurezza cibernetica svolge una funzione di raccordo tra le diverse componenti dell'architettura istituzionale, promuove la programmazione e pianificazione operativa della risposta a situazioni di crisi cibernetica, mantiene attiva – 24 ore su 24, tutti i giorni della settimana – l'Unità per l'allertamento e la risposta alle crisi e costituisce il punto di riferimento nazionale per i rapporti con altri stati e con le organizzazioni internazionali, *in primis* Nazioni Unite, Nato e Unione europea. Inoltre il Nucleo riceve le segnalazioni di evento cibernetico dall'estero, dirama gli allarmi all'interno del territorio nazionale, dichiara la situazione di crisi ed attiva il NISP.

È importante ricordare che l'Unità per allertamento è divenuta operativa dal novembre 2013 e che ad essa è stata affiancata una Segreteria per la sicurezza cibernetica incaricata di organizzare le attività e coordinare gli impegni interministeriali. Ad oggi questi sono gli organi principalmente deputati alla sicurezza cibernetica nazionale.

A conclusione della presente analisi delle politiche ed iniziative italiane maggiormente rilevanti in ambito cyber, si è valutato lo stato dell'arte della sicurezza cibernetica nazionale ricorrendo ad una comparazione punto per punto del caso italiano con le linee guida individuate dall'ENISA. Tale comparazione ha evidenziato i progressi e le lacune dell'Italia in questa materia, nonché i possibili margini di miglioramento. Tra questi emerge l'importanza di istituire un CERT nazionale, la cui operatività costituisce un obiettivo prioritario per il 2014.

Sembrerebbe inoltre raccomandabile l'attribuzione del coordinamento di tutte le attività relative alla cybersecurity ad un'unica agenzia governativa, che abbia lo scopo di rafforzare procedure, processi e collaborazione a livello nazionale e, contemporaneamente, agire da punto di riferimento in Europa e nel mondo. Il Quadro strategico nazionale fa riferimento alla prossima realizzazione di un'agenzia nazionale per la NIS, pertanto è auspicabile che questo processo non richieda un tempo eccessivo.

Anche l'istituzione di partnership pubblico-privato rappresenta una sfida importante per il futuro, dalla quale dipenderà il successo delle politiche nazionali adottate. Sebbene siano state realizzate diverse intese tra Governo ed imprese, queste ultime continuano a dimostrare una certa riluttanza nel comunicare alle autorità gli incidenti cibernetici che interessano reti e sistemi aziendali, per motivi di reputazione e scarsa fiducia negli interventi governativi. Uno sforzo maggiore dovrebbe essere compiuto in questa direzione, per favorire il dialogo costruttivo tra i due settori possibilmente in senso bidirezionale.

Il DPCM del 24 gennaio 2013 ha istituito una sorta di meccanismo di *incident reporting* tra pubblico e privato, relativo soprattutto alle situazioni di violazioni della sicurezza o dell'integrità dei sistemi informatici aziendali. Tuttavia tale meccanismo risulta non regolamentato ed unidirezionale, nel senso che le informazioni scambiate fluiscono solo verso le autorità. Uno scambio reciproco di informazioni favorirebbe il coinvolgimento attivo delle imprese, agevolando la fiducia e la collaborazione tra le parti. A questo scopo sarebbe anche utile fissare delle regole precise alla base del meccanismo di comunicazione, privilegiando un approccio

settoriale che istituisca una piattaforma comune per ciascun settore (*internet service provider*, energia, trasporti, etc.).

Un contributo notevole al progresso della cybersecurity in Italia potrebbe venire inoltre dall'organizzazione di Tavoli di condivisione e scambio delle informazioni tra istituzioni pubbliche e settore privato, nonché università e istituti di ricerca. L'obiettivo di questi Tavoli dovrebbe essere quello di facilitare la collaborazione attiva pubblico-privata, partendo proprio dal punto di vista delle imprese. In quest'ottica, è stato istituito un "tavolo imprese" che, in occasione della sua prima riunione nel novembre 2013, ha visto la partecipazione delle dieci imprese strategiche per l'Italia con le quali il Dipartimento informazioni per la sicurezza ha sottoscritto, in ragione della loro centralità nella *governance* nazionale cibernetica, apposite convenzione ex articolo 11 del DPCM 24 gennaio 2013.

Anche un coinvolgimento del mondo accademico e della ricerca si rivelerebbe utile, al fine di completare il quadro degli attori coinvolti nella sicurezza cibernetica. Il mondo della ricerca, in particolare, è in grado di svolgere un ruolo importante nel conseguimento di progressi in materia. Sarebbe pertanto opportuno avvicinare quest'ultimo alle esigenze di settore tramite l'attivazione di programmi di diretto interesse del Governo e delle imprese.

Per favorire l'avanzamento della cybersecurity è anche importante promuovere la diffusione di una cultura generale in materia, cosicché tutti i soggetti interessati possano svolgere il proprio ruolo e coordinarsi tra loro. Mentre le istituzioni e il settore della ricerca dimostrano un crescente interesse per questa tematica, le imprese – pur possedendo gran parte del *know how* e delle risorse tecnologiche – si dimostrano ancora poco propense a collaborare, sia con le autorità di governo che con le altre imprese. La maggior parte degli utenti finali non presenta sufficiente consapevolezza dei rischi associati all'uso delle reti. La diffusione di una cultura della sicurezza informatica si rivela quindi prioritaria affinché sia conseguibile un progresso a livello di sistema paese.

Si ribadisce infine come sia auspicabile che l'Italia, nel prossimo futuro, provveda a dotarsi anche di una strategia nazionale di sicurezza. È ora in vigore una strategia specifica per la sicurezza informatica, ma in assenza di una più comprensiva strategia nazionale di sicurezza.

Indubbiamente molto resta ancora da fare, ma negli ultimi anni – e segnatamente il 2013 - sono stati approvati importanti documenti istituzionali in materia e si è assistito alla diffusione in ambito governativo-im-

prenditoriale-accademico del dibattito sulla sicurezza informatica, quale minaccia crescente alla sicurezza e al benessere economico degli stati.

È importante che questo interesse aumenti in futuro, in nome di un concetto di sicurezza nazionale che implichi la necessaria protezione della vita quotidiana dei cittadini per garantire la crescita economica del paese, leva fondamentale della sicurezza.

Bibliografia

Saggi e articoli

Kamlesh Bajaj, "Globar cyber commons. Addressing cyber security issues", in *Neurope*, 3 June 2012, http://www.neurope.eu/node/114509

Ivanka Barzashka, "Are Cyber-Weapons Effective? Assessing Stuxnet's Impact on the Iranian Enrichment Programme", in *RUSI Journal*, Vol. 158, No. 2 (28 April 2013), http://dx.doi.org/10.1080/03071847.2013.787735

Scott Borg, "Logica della guerra cibernetica", in *LiMes. Quaderni Speciali* (Media come armi), aprile 2012, p. 47-53

Sophie-Charlotte Brune et al., *Stocktaking study of military cyber defence capabilities in the European Union (milCyberCAP. Unclassified Summary*, Santa Monica, Rand, 2013, http://www.rand.org/pubs/research_reports/RR286.html

Cooperative Cyber Defence Centre Of Excellence (CCD COE), *Cyber Defence exercise Locked Shields 2013. After Action Report*, Tallinn, 2013, http://www.ccdcoe.org/locked-shields-2013.html

Paul Cornish, Rex Hughes and David Livingstone, *Cyberspace and the National Security of the United Kingdom. Threats and Responses*, London, Chatham House, 2009, http://www.chathamhouse.org/node/5852

Cyber Intelligence and Information Security Center (CIS Sapienza), *2013 Italian Cyber Security Report. Critical Infrastructure and Other Sensitive Sectors Readiness*, Roma, Università La Sapienza, 2013, http://www.dis.uniroma1.it/~midlab/articoli/13CIS-Report.pdf

Olivier De France, "A cyberstrategy for Europe. Now what about a strategy?", in *ECFR's Blog*, 15 February 2013, http://www.ecfr.eu/blog/entry/a_cyberstrategy_for_europe._now_what_about_a_strategy

Dimitrios Delibasis, "State Use of Force in Cyberspace for Self-Defence: A New Challenge for a New Century", in *Peace Conflict and Development*, No. 8 (February 2006), http://www.bradford.ac.uk/

ssis/peace-conflict-and-development/issue-8/State-use-of-force.pdf

Alessio Di Angelantonio, *La Matrice GE McKinsey. Applicazione pratica con Excel*, ottobre 2007, http://download.microsoft.com/download/5/6/0/560adcbd-fd07-48d8-bfb1-86a64ac8d6cd/matricemckinseyconexcel.pdf

Federica Di Camillo e Lucia Marta, "Una Strategia di Sicurezza nazionale per l'Italia. Elementi di analisi", in *IAI Quaderni*, n. 34 (dicembre 2009), http://www.iai.it/content.asp?langid=1&contentid=126

Federica Di Camillo and Valérie Miranda, "Ambiguous Definitions in the Cyber Domain: Costs, Risks and the Way Forward", in *IAI Working Papers*, No 11|26 (September 2011), http://www.iai.it/pdf/DocIAI/iaiwp1126.pdf

Federica Di Camillo and Valérie Miranda, "Cyber Security: Toward EU-U.S. cooperation?" in *EU-U.S. Security Strategies. Comparative scenarios and recommendations,* Washington, Center for Strategic and International Studies, April 2011, p. 55-67, http://www.iai.it/content.asp?langid=1&contentid=599

Federica Di Camillo, Valérie Vicky Miranda e Stefano Felician, "Cybersecurity: Europa e Italia", in *Approfondimenti dell'Osservatorio di politica internazionale*, n. 32 (maggio 2011), http://www.iai.it/pdf/Oss_Polinternazionale/pi_a_0032.pdf

Carlo Disma, "Approccio dottrinale alla Cyber Warfare", in *Rivista Italiana Difesa (RID)*, a. 31., n. 12 (dicembre 2012), p. 55-57

Umberto Gori e Luigi Sergio Germani (a cura di), *Information Warfare. Le nuove minacce provenienti dal cyberspazio alla sicurezza nazionale italiana*, Milano, Franco Angeli, 2011

Umberto Gori e Luigi Sergio Germani (a cura di), *Information Warfare 2011. La sfida della Cyber Intelligence al sistema Italia: dalla sicurezza delle imprese alla sicurezza nazionale*, Milano, Franco Angeli, 2012

Umberto Gori e Serena Lisi (a cura di), *Information Warfare 2012. Armi cibernetiche e processo decisionale*, Milano, Franco Angeli, 2013

Luke Gribbon et al., *Cyber-security threat characterisation. A rapid comparative analysis*, Santa Monica, Rand, 2013, http://www.rand.org/pubs/research_reports/RR235.html

Danny Hakim, "Europe Aims to Regulate the Cloud", in *The New York Times*, 6 October 2013, http://nyti.ms/17aIsCv

Rex Hughes, "A treaty for cyberspace", in *International Affairs*, Vol. 86, No. 2 (March 2010), p. 523-541, http://21stcenturywiener.org/

wp-content/uploads/2013/11/A-Treaty-for-Cyberspace-by-Hughes.pdf

IBM, *IBM X-Force 2013 - Mid-Year Trend and Risk Report*, September 2013, http://public.dhe.ibm.com/common/ssi/ecm/en/wge03021usen/WGE03021USEN.PDF

Timothy J. Junio, "How Probable is Cyber War? Bringing IR Theory Back In To The Cyber Conflict Debate", in *Journal of Strategic Studies*, Vol. 36, No. 1 (March 2013), p. 125-133

Terrence K. Kelly, James P. Peeremboom and Steven M. Rinaldi, "Identifying, Understanding, and Analyzinig Critical Infrastructure Interdependencies", *in IEEE Control Systems Magazine*, Vol. 21, No. 6 (December 2011)

James Andrews Lewis, *Rethinking Cybersecurity. A Comprehensive Approach*, Speech at the Sasakawa Peace Foundation, Tokyo, 12 September 2011, http://csis.org/node/32513

James Andrew Lewis and Stewart Baker, *The Economic Impact of Cybercrime and Cyber Espionage*, Santa Clara, McAfee, July 2013, http://csis.org/node/45446

Adam P. Liff, "Cyberwar: 'A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War", in *Journal of Strategic Studies*, Vol. 35, No. 3 (2012), p. 401-428

Alessandro Longo, "Cybersecurity, L'Italia mette a punto una sua strategia", in *Il Sole 24 ore*, 23 gennaio 2013, http://24o.it/X0NNP

Alessandro Marrone, "Il bicchiere mezzo vuoto della difesa", in *AffarInternazionali*, 27 dicembre 2013, http://www.affarinternazionali.it/articolo.asp?ID=2489

Alessandro Marrone, "La Nato guarda al futuro ", in *AffarInternazionali*, 28 ottobre 2010, http://www.affarinternazionali.it/articolo.asp?ID=1580

Alessandro Marrone, "Sulla difesa l'UE rischia la retromarcia", in *AffarInternazionali*, 4 dicembre 2013, http://www.affarinternazionali.it/articolo.asp?ID=2474

Stefano Mele, "I principi strategici delle politiche di cybersecurity", in *Approfondimenti del Sistema di informazione per la sicurezza della Repubblica*, 5 dicembre 2013,

http://www.sicurezzanazionale.gov.it/sisr.nsf/il-mondo-intelligence/principi-strategici-delle-politiche-di-cyber-security.html

Federica Meta, "Cybersecurity, l'Italia avrà la sua task force", in *Corriere delle Comunicazioni*, 20 marzo 2013, http://www.corrierecomuni-

cazioni.it/it-world/20297_cybersecurity-l-italia-avra-la-sua-task-force.htm

Steven Lee Myers, "Cyberattack on Estonia stirs fear of 'virtual war'", in *The New York Times*, 18 May 2007, http://nyti.ms/1nGqZsq

Michele Nones, "La difesa delle attività strategiche", in *AffarInternazionali*, 23 agosto 2012,
http://www.affarinternazionali.it/articolo.asp?ID=2111

David Omand, "The steps needed to protect the EU's critical infrastructure against cyber-attack", in *Europe's World*, No. 25 (Autumn 2013), p. 112-118, http://europesworld.org/?p=176

Roberta Pisa, "L'accesso ad internet: un nuovo diritto fondamentale?", in *Treccani Magazine*, 7 gennaio 2010, http://www.treccani.it/magazine/diritto/approfondimenti/diritto_internazionale_e_comparato/2_Pisa_internet.html

Daniel Pitcairn, "A Missed Chance for NATO's Cybersecurity future", in *Defense One*, 23 October 2013, http://www.defenseone.com/ideas/2013/10/missed-chance-natos-cybersecurity-future/72542

Andrea Rigoni, "Cybersecurity, Rigoni: 'Serve una strategia nazionale'", in *Corriere delle Comunicazioni*, 6 aprile 2013, http://www.corrierecomunicazioni.it/it-world/20603_cybersercurity-rigoni-serve-una-strategia-nazionale.htm

Marco Roscini, *Cyber Operations and the Use of Force in International Law*, Oxford, Oxford University Press, 2014

Carlo Sarzana di S.Ippolito, "Dolenti note in tema di protezione delle infrastrutture critiche informatizzate...", in *Diritto & Diritti,* 22 maggio 2008,
http://www.diritto.it/docs/26027

Michael N. Schmitt (ed.), *Tallinn Manual on the International Law applicable to Cyber Warfare*, Cambridge, Cambridge University Press, 2013

Bruce Schneier, "There's No Real Difference Between Online Espionage and Online Attack", in *The Atlantic*, 6 March 2014, https://www.schneier.com/essay-475.html

Security & Defence Agenda (SDA), *Cyber-protection of critical infrastructure*, October 2012, http://www.securitydefenceagenda.org/Contentnavigation/Library/Libraryoverview/tabid/1299/articleType/ArticleView/articleId/3282/categoryId/58/Cyberprotection-of-critical-infrastructure.aspx

Security & Defence Agenda (SDA), *Cyber-security: Problems outpace solutions*, December 2013, http://www.securitydefenceagenda.org/Contentnavigation/Library/Libraryoverview/tabid/1299/articleType/ArticleView/articleId/3620/categoryId/62/Cybersecurity-Problems-outpace-solutions.aspx

Security & Defence Agenda (SDA), *Europe's defence: What the December 2013 European Council should yeld*, December 2013, http://www.securitydefenceagenda.org/Contentnavigation/Library/Libraryoverview/tabid/1299/articleType/ArticleView/articleId/3603/New-discussion-paper-Europes-defence-What-the-December-2013-European-Council-should-yield.aspx

Security & Defence Agenda (SDA), *What next for Euoropean cyber-security?*, April 2013, http://www.securitydefenceagenda.org/Contentnavigation/Library/Libraryoverview/tabid/1299/articleType/ArticleView/articleId/3436/What-next-for-European-cybersecurity.aspx

Security & Defence Agenda (SDA), *Where cyber-security is heading*, October 2012, http://www.securitydefenceagenda.org/Contentnavigation/Library/Libraryoverview/tabid/1299/articleType/ArticleView/articleId/3412/New-SDA-cyber-report.aspx

Symantec, *Symantec Intelligence Quarterly, July-September 2009*, October 2009, http://eval.symantec.com/mktginfo/enterprise/other_resources/b-symc_intelligence_quarterly_july-sept_2009_20666025.en-us.pdf

Emmet Tuohy, *Toward an EU Cybersecurity Strategy: The role of Estonia*, Tallinn, International Centre for Defence Studies, December 2012, http://icds.ee/index.php?id=73&L=1&tx_ttnews[tt_news]=1228&tx_ttnews[backPid]=211&cHash=d8a40b64ca

Documenti: Unione europea

Commissione europea, *Un'agenda digitale europea* (COM(2010)245 f/2), 26 agosto 2010, http://eur-lex.europa.eu/legal-content/it/TXT/?uri=celex:52010DC0245R(01)

Commissione europea, *Comunicazione relativa a un programma europeo per la protezione delle infrastrutture critiche* (COM(2006)786), 12 dicembre 2006, http://eur-lex.europa.eu/legal-content/it/TXT/?uri=celex:52006DC0786

Commissione europea, *Comunicazione relativa alla protezione delle infrastrutture critiche informatizzate "Realizzazioni e prossime tappe: verso una sicurezza informatica mondiale"* (COM(2011)163, 31 marzo 2011, http://eur-lex.europa.eu/legal-content/it/TXT/?uri=celex:52011DC0163

Commissione europea, *Creare una società dell'informazione sicura migliorando la sicurezza delle infrastrutture dell'informazione e mediante la lotta alla criminalità informatica. eEurope 2002* (COM(2000)890), 26 gennaio 2001, http://eur-lex.europa.eu/legal-content/it/TXT/?uri=celex:52000DC0890

Commissione europea, *eEurope. Una società dell'informazione per tutti* (COM(2000)130), 8 marzo 2000, http://eur-lex.europa.eu/legal-content/it/TXT/?uri=celex:52000DC0130

Commissione europea, *eEurope 2005: una società dell'informazione per tutti* (COM(2002)263), 28 maggio 2002, http://eur-lex.europa.eu/legal-content/it/TXT/?uri=celex:52002DC0263

Commissione europea, *Proposta di direttiva recante misure volte a garantire un livello comune elevato di sicurezza delle reti e dell'informazione nell'Unione* (COM(2013)48), 7 febbraio 2013, http://eur-lex.europa.eu/legal-content/it/TXT/?uri=celex:52013PC0048

Commissione europea, *Proposta di direttiva relativa agli attacchi contro i sistemi di informazione, e che abroga la decisione quadro 2005/222/GAI del Consiglio* (COM(2010)517), 30 settembre 2010, http://eur-lex.europa.eu/legal-content/it/TXT/?uri=celex:52010PC0517

Commissione europea, *Proteggere le infrastrutture critiche informatizzate. "Rafforzare la preparazione, la sicurezza e la resilienza per proteggere l'Europa dai ciberattacchi e dalle ciberperturbazioni"* (COM(2009)149), 30 marzo 2009, http://eur-lex.europa.eu/legal-content/it/TXT/?uri=celex:52009DC0149

Commissione europea, *Sicurezza delle reti e sicurezza dell'informazione: proposta di un approccio strategico europeo* (COM(2001)298), 6 giugno 2001, http://eur-lex.europa.eu/legal-content/it/TXT/?uri=celex:52001DC0298

Commissione europea, *Strategia dell'Unione europea per la cibersicurezza: un ciberspazio aperto e sicuro* (JOIN(2013)1), 7 febbraio 2013, http://www.ipex.eu/IPEXL-WEB/dossier/document/JOIN20130001.do?appLng=IT

Commissione europea, *La strategia di sicurezza interna dell'UE in azione: cinque tappe verso un'Europa più sicura* (COM(2010)673),

22 novembre 2010, http://eur-lex.europa.eu/legal-content/it/TXT/?uri=celex:52010DC0673

Commissione europea, *Una strategia per una società dell'informazione sicura. "Dialogo, partenariato e responsabilizzazione"* (COM(2006)251), 31 maggio 2006, http://eur-lex.europa.eu/legal-content/it/TXT/?uri=celex:52006DC0251

Consiglio dell'Unione europea, *Decisione che istituisce per il periodo 2007-2013 il programma specifico "Prevenzione, preparazione e gestione delle conseguenze in materia di terrorismo e di altri rischi correlati alla sicurezza", quale parte del programma generale sulla sicurezza e la tutela delle libertà* (2007/124/CE, Euratom), 12 febbraio 2007, http://eur-lex.europa.eu/legal-content/it/TXT/?uri=celex:32007D0124

Consiglio dell'Unione europea, *Un'Europa sicura in un mondo migliore. Strategia europea in materia di sicurezza*, 12 dicembre 2003, http://www.consilium.europa.eu/uedocs/cmsUpload/031208ESSIIIT.pdf

Consiglio dell'Unione europea, *Protezione delle infrastrutture critiche informatizzate "Realizzazioni e prossime tappe: verso una sicurezza informatica mondiale" (CIIP) - Adozione delle conclusioni del Consiglio* (10299/11), 19 maggio 2011, http://register.consilium.europa.eu/doc/srv?l=IT&f=ST%2010299%202011%20INIT

Consiglio dell'Unione europea, *Relazione sull'attuazione della strategia europea in materia di sicurezza. Garantire sicurezza in un mondo in piena evoluzione* (S407/08), 11 dicembre 2008, http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressdata/IT/reports/104641.pdf

Consiglio europeo, *Conclusioni del Consiglio europeo 19 e 20 dicembre 2013 - Politica di sicurezza e di difesa comune*, 19 dicembre 2013, http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/it/ec/140221.pdf

Direttiva 2002/19/CE del 7 marzo 2002, relativa all'accesso alle reti di comunicazione elettronica e alle risorse correlate, e all'interconnessione delle medesime, http://eur-lex.europa.eu/legal-content/it/TXT/?uri=celex:32002L0019

Direttiva 2002/20/CE del 7 marzo 2002, relativa alle autorizzazioni per le reti e i servizi di comunicazione elettronica, http://eur-lex.europa.eu/legal-content/it/TXT/?uri=celex:32002L0020

Direttiva 2002/21/CE del 7 marzo 2002, che istituisce un quadro normativo comune per le reti ed i servizi di comunicazione elettronica, http://eur-lex.europa.eu/legal-content/it/TXT/?uri=celex:32002L0021

Direttiva 2008/114/CE dell'8 dicembre 2008 *relativa all'individuazione e alla designazione delle infrastrutture critiche europee e alla valutazione della necessità di migliorarne la protezione*, http://eur-lex.europa.eu/legal-content/it/TXT/?uri=celex:32008L0114

Direttiva 2009/140/CE del 25 novembre 2009 *recante modifica delle direttive 2002/21/CE che istituisce un quadro normativo comune per le reti ed i servizi di comunicazione elettronica, 2002/19/CE relativa all'accesso alle reti di comunicazione elettronica e alle risorse correlate, e all'interconnessione delle medesime e 2002/20/CE relativa alle autorizzazioni per le reti e i servizi di comunicazione elettronica*, http://eur-lex.europa.eu/legal-content/it/TXT/?uri=celex:02009L0140-20091219

ENISA, *Annual Incident Reports 2012*, August 2013, http://europa.eu/!wp66cv

ENISA, *CERT cooperation and its further facilitation by relevant stakeholders*, 1 December 2006, http://europa.eu/!gb64dk

ENISA, *Critical Cloud Computing - A CIIP perspective on cloud computing services - Version 1.0*, December 2012, http://europa.eu/!cT64Hr

ENISA, *Cyber Europe 2010 Report,* 18 April 2011, http://europa.eu/!Cp89QX

ENISA, *Cyber Europe 2012. Risultanze fondamentali e raccomandazioni*, dicembre 2012, https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cce/cyber-europe/cyber-europe-2012/ENISA_2012_00490000_IT_TRA.pdf

ENISA, *Cyber Incident Reporting in the EU*, August 2012, http://europa.eu/!MD44td

ENISA, *Cybersecurity cooperation. Defending the digital frontline*, October 2013, http://europa.eu/!mt73gq

ENISA, *ENISA Threat Landscape mid year 2013*, 19 September 2012, http://europa.eu/!VG93kc

ENISA, *ENISA Threat Landscape 2013. Overview of current and emerging cyber-threats*, 11 December 2013, http://europa.eu/!cU87Cr

ENISA, *Italy Country Report,* January 2010, http://www.epractice.eu/files/Italy%20Country%20Report.pdf

ENISA, *National and International Cyber Security Exercises: Survey, Analysis & Recommendations*, October 2012, http://europa.eu/!wu37PJ

ENISA, *National Cyber Security Strategies. Practical Guide on Development and Execution*, December 2012, http://europa.eu/!gC63Tk

ENISA, *National Cyber Security Strategies. Setting the course of national efforts to strengthen security in cyberspace*, May 2012, http://www.gns.gov.pt/media/1238/ENISANationalCyberSecurityStrategies.pdf

European Commission, *Commission Staff Working Document on a new approach to the European Programme for Critical Infrastructure Protection. Making European Critical Infrastructures more secure* (SWD(2013)318), 28 August 2013, http://register.consilium.europa.eu/pdf/en/13/st13/st13280.en13.pdf

European Commission, *eGovernment in the European Union*, eGovernment Factsheets, Edition 4.0, December 2011, http://www.epractice.eu/files/eGovernmentEuropeanCommission.pdf

European Commission, *Horizon 2020 official standard presentation*, December 2013, http://ec.europa.eu/research/horizon2020/pdf/press/horizon2020-presentation.pdf

European Commission, *Special Eurobarometer 390: Cyber Security Report*, July 2012, http://ec.europa.eu/public_opinion/archives/ebs/ebs_390_en.pdf

European Commission, *Table on the Implementation of the "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace"(JOIN(2013)1)*, 28 February 2014, http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=4623

European Commission DG CONNECT, *Digital Agenda for Europe - Scoreboard 2012*, October 2012, http://ec.europa.eu/digital-agenda/download-scoreboard-reports

European Defence Agency (EDA), *Factsheet Cyber Defence*, 19 November 2013, http://www.eda.europa.eu/info-hub/publications/publication-details/pub/factsheet-cyber-defence

Europol, *European cybercrime centre to be established at the Europol*, 28 March 2012, https://www.europol.europa.eu/content/press/european-cybercrime-centre-be-established-europol-1417

Europol, *Threat Assessment (abridged) - Internet facilitated organised crime - iOCTA*, 7 January 2011, https://www.europol.europa.eu/sites/default/files/publications/iocta.pdf

Europol and ICSPA, *Project 2020. Scenarios for the future of Cybercrime*, 25 September 2013, https://www.europol.europa.eu/content/project-2020-scenarios-future-cybercrime

European External Action Service (EEAS), *Preparing the December 2013 European Council on Security and Defence. Final Report by the High Representative/Head of the EDA on the Common Security and Defence Policy*, 15 October 2013, http://eeas.europa.eu/statements/docs/2013/131015_02_en.pdf

Regolamento (CE) n. 460/2004 del 10 marzo 2004 che istituisce l'Agenzia europea per la sicurezza delle reti e dell'informazione,
http://eur-lex.europa.eu/legal-content/it/TXT/?uri=celex:02004R0460-20081101

Regolamento UE 526/2013 del 21 maggio 2013 *relativo all'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (ENISA) e che abroga il regolamento (CE) n. 460/2004*, 2013, http://eur-lex.europa.eu/legal-content/it/TXT/?uri=celex:32013R0526

Documenti: Italia

Agenzia per l'Italia digitale, *Linee guida per il disaster recovery delle Pubbliche Amministrazioni*, novembre 2013, http://www.agid.gov.it/sites/default/files/linee_guida/linee-guida-dr.pdf

Agenzia per l'Italia digitale, *La strategia AgID per la realizzazione dell'Agenda digitale italiana*, Forum PA, Roma, 28 maggio 2013, http://archivio.digitpa.gov.it/sites/default/files/SlideRagosaMappaDigitalAgenda.pdf

Camera dei Deputati, Commissione Trasporti, poste e telecomunicazioni, *Indagine conoscitiva sulla sicurezza informatica delle reti*, 28 febbraio 2012-22 gennaio 2013, http://leg16.camera.it/459?eleindag=/_dati/leg16/lavori/stencomm/09/indag/informatica

Comitato parlamentare per la sicurezza della Repubblica (COPASIR), *Relazione sulle possibili implicazioni e minacce per la sicurezza nazionale derivanti dall'utilizzo dello spazio cibernetico*, 7 luglio 2010, http://www.senato.it/leg/16/BGT/Schede/docnonleg/19825.htm

Presidenza del Consiglio dei ministri, *Agenda digitale italiana. e-Government - innovazione digitale nelle PA*, ottobre 2012, http://www.funzionepubblica.gov.it/media/1009447/agenda_digitale.pdf

Presidenza del Consiglio dei ministri, *Organizzazione nazionale per la gestione di crisi*, settembre 2012, http://www.difesa.it/SMD_/CASD/IM/CeMiSS/Pubblicazioni/OSN/Documents/05_Capponi.pdf

Presidenza del Consiglio dei ministri, *Piano e-Gov 2012: Report di avanzamento attività*, 11 novembre 2011, http://www.funzionepubblica.gov.it/media/872560/aggiornamento%20piano%20e-gov.pdf

Presidenza del Consiglio dei ministri, *Piano nazionale per la protezione cibernetica e la sicurezza informatica*, dicembre 2013, http://www.agid.gov.it/sites/default/files/leggi_decreti_direttive/piano-nazionale-cyber_0.pdf

Presidenza del Consiglio dei ministri, *Quadro strategico nazionale per la sicurezza dello spazio cibernetico*, dicembre 2013, http://www.agid.gov.it/sites/default/files/leggi_decreti_direttive/quadro-strategico-nazionale-cyber_0.pdf

Presidenza del Consiglio dei ministri, Gruppo di lavoro sulla protezione delle infrastrutture critiche informatizzate, *Protezione delle infrastrutture critiche informatizzate. La realtà italiana*, 10 marzo 2004, http://www.vigilfuoco.it/aspx/ReturnDocument.aspx?IdDocumento=2832

Sistema di informazione per la sicurezza della Repubblica, *Relazione sulla politica dell'informazione per la sicurezza 2010*, 28 febbraio 2011, http://www.sicurezzanazionale.gov.it/sisr.nsf/relazione-annuale/relazione-al-parlament-2010.html

Sistema di informazione per la sicurezza della Repubblica, *Relazione sulla politica dell'informazione per la sicurezza 2011*, 28 febbraio 2012, http://www.sicurezzanazionale.gov.it/sisr.nsf/relazione-annuale/relazione-al-parlamento-2011.html

Sistema di informazione per la sicurezza della Repubblica, *Relazione sulla politica dell'informazione per la sicurezza 2012*, 28 febbraio 2013, http://www.sicurezzanazionale.gov.it/sisr.nsf/relazione-annuale/relazione-al-parlamento-2012.html

Sistema di informazione per la sicurezza della Repubblica, *Relazione sulla politica dell'informazione per la sicurezza 2013*, 6 marzo 2014, http://www.sicurezzanazionale.gov.it/sisr.nsf/relazione-annuale/relazione-al-parlamento-2013.html

Fonti normative: Italia (in ordine cronologico)

Legge n. 547 del 23 dicembre 1993 - *Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica*, G.U. n. 305 del 30 dicembre 1993, http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:1993;547

Legge n. 269 del 3 agosto 1998 - *Norme contro lo sfruttamento della prostituzione, della pedopornografia, del turismo sessuale in danno di minori, quali nuove forme di riduzione in schiavitù,* G.U.

n. 185 del 10 agosto 1998, http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:1998;269

Direttiva del Presidente del Consiglio dei ministri, Dipartimento per l'Innovazione e le Tecnologie, del 16 gennaio 2002 - *Sicurezza informatica e delle telecomunicazioni nelle pubbliche amministrazioni*, G.U. n. 69 del 22 marzo 2002, http://www.gazzettaufficiale.it/eli/id/2002/03/22/02A03219

Decreto interministeriale del 14 gennaio 2003 - *Istituzione Osservatorio permanente per la sicurezza e la tutela delle reti e delle telecomunicazioni*, http://www.mise.gov.it/index.php?option=com_content&view=article& id=2017545

Decreto legislativo n. 196 del 30 giugno 2003 - *Codice in materia di protezione dei dati personali*, G.U. n. 174 del 29 luglio 2003, suppl. ordinario n. 123, http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2003;196

Decreto legislativo n. 259 del 1 agosto 2003 - *Codice delle comunicazioni elettroniche*, G.U. n. 214 del 15 settembre 2003, http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2003;259

Decreto legislativo n. 82 del 7 marzo 2005 - *Codice dell'amministrazione digitale*, G.U. n. 112 del 16 maggio 2005, suppl. ordinario n. 93, http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2005;82

Decreto legge n. 144 del 27 luglio 2005 - *Misure urgenti per il contrasto del terrorismo internazionale*, G.U. n. 173 del 27 luglio 2005, http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:2005;144

Legge n. 155 del 31 luglio 2005 - *Conversione in legge, con modificazioni, del decreto-legge 27 luglio 2005, n.144, recante misure urgenti per il contrasto del terrorismo internazionale*, G.U. n. 177 del 1 agosto 2005, http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:2005;155

Legge n. 38 del 6 febbraio 2006 - *Disposizioni in materia di lotta contro lo sfruttamento sessuale dei bambini e la pedopornografia anche a mezzo Internet,* G.U. n. 38 del 15 febbraio 2006, http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:2006;38

Legge n. 124 del 3 agosto 2007 - *Sistema di informazione per la sicurezza della Repubblica e la disciplina del segreto*, G.U. n. 187 del 13 agosto 2007, http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:2007;124

Decreto del Ministero dell'Interno del 9 gennaio 2008 - *Individuazione delle infrastrutture critiche informatiche di interesse nazionale*, G.U. n. 101 del 30 aprile 2008, http://www.gazzettaufficiale.it/eli/id/2008/04/30/08A02684

Legge n. 48 del 18 marzo 2008 - *Ratifica ed esecuzione della convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno*, G.U. n. 80 del 4 aprile 2008, suppl. ordinario n. 79, http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:2008;48

Decreto legislativo n. 177 del 1° dicembre 2009 - *Riorganizzazione del Centro nazionale per l'informatica nella pubblica amministrazione, a norma dell'articolo 24 della legge 18 giugno 2009, n. 69*, G.U. n. 290 del 14 dicembre 2009, http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2009;177

Decreto del Presidente del Consiglio dei ministri del 5 maggio 2010 - *Organizzazione nazionale per la gestione di crisi*, G.U. n. 139 del 17 giugno 2010,

http://www.gazzettaufficiale.it/eli/id/2010/06/17/10A07594

Decreto legislativo n. 61 dell'11 aprile 2011 - *Attuazione della Direttiva 2008/114/CE recante l'individuazione e la designazione delle infrastrutture critiche europee e la valutazione della necessità di migliorarne la protezione*, G.U. n. 102 del 4 maggio 2011, http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2011;061

Decreto del Presidente del Consiglio dei ministri del 12 ottobre 2011 - *Individuazione delle strutture e dei posti di funzione di livello dirigenziale non generale del Ministero dell'interno ...*, G.U. n. 286 del 9 dicembre 2011, http://www.gazzettaufficiale.it/eli/id/2011/12/09/11A15878

Decreto legge n. 5 del 9 febbraio 2012 - *Disposizioni urgenti in materia di semplificazione e di sviluppo*, G.U. n. 33 del 9 febbraio 2012, http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legge:2012;5

Legge n. 35 del 4 aprile 2012 - *Conversione in legge, con modificazioni, del decreto-legge 9 febbraio 2012, n.5, recante disposizioni urgenti in materia di semplificazione e di sviluppo*, G.U. n. 82 del 6 aprile 2012, suppl. ordinario n. 69, http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:2012;35

Decreto legislativo n. 69 del 28 maggio 2012 - *Modifiche al decreto legislativo 30 giugno 2003, n. 196, recante codice in materia di protezione dei dati personali in attuazione delle direttive 2009/136/CE ...*, G.U. n. 126 del 31 maggio 2012, http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2012;69

Decreto legislativo n. 70 del 28 maggio 2012 - *Modifiche al decreto legislativo 1° agosto 2003, n. 259, recante codice delle comunicazioni elettroniche in attuazione delle direttive 2009/140/CE ...*, G.U. n. 126 del 31 maggio 2012, http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2012;70

Legge n. 133 del 7 agosto 2012 - *Modifiche alla legge 3 agosto 2007, n. 124, concernente il Sistema di informazione per la sicurezza della Repubblica e la disciplina del segreto*, G.U. n. 186 del 10 agosto 2012, http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:2012;133

Decreto legge n. 179 del 18 ottobre 2012 - *Ulteriori misure urgenti per la crescita del paese*, G.U. n. 245 del 19 ottobre 2012, suppl. ordinario n. 194, http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legge:2012;179

Decreto del Presidente del Consiglio dei ministri del 24 gennaio 2013 - *Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale*, G.U. n. 66 del 19 marzo 2013, http://www.gazzettaufficiale.it/eli/id/2013/03/19/13A02504

Decreto legge n. 69 del 21 giugno 2013 - *Disposizioni urgenti per il rilancio dell'economia*, G.U. n. 144 del 21 giugno 2013, suppl. ordinario n. 50, http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legge:2013;069

Finito di stampare nel mese di agosto 2014
con tecnologia *print on demand*
presso il Centro Stampa "Nuova Cultura"
p.le Aldo Moro n. 5, 00185 Roma
www.nuovacultura.it
per ordini: ordini@nuovacultura.it

[Int_9788868123642_17x24bn_MP03]