La sicurezza delle reti e dei sistemi informativi: il ruolo degli ingegneri dell'informazione

Centro Studi Consiglio Nazionale Ingegneri

CONSIGLIO NAZIONALE DEGLI INGEGNERI

PRESSO IL MINISTERO DELLA GIUSTIZIA - 00186 ROMA - VIA ARENULA, 71

Ing. Giovanni Rolando	*Presidente*
Ing. Pietro Ernesto De Felice	*Vice Presidente*
Ing. Alessandro Biddau	*Consigliere Segretario*
Ing. Carlo De Vuono	*Tesoriere*
Ing. Giovanni Bosi	Consigliere
Ing. Roberto Brandi	Consigliere
Ing. Ugo Gaia	Consigliere
Ing. Romeo La Pietra	Consigliere
Ing. Giovanni Montresor	Consigliere
Ing. civ.amb.iun. Antonio Picardi	Consigliere
Ing. Sergio Polese	Consigliere
Ing. Alberto Speroni	Consigliere
Ing. Paolo Stefanelli	Consigliere
Ing. Silvio Stricchi	Consigliere
Ing. Giuseppe Zia	Consigliere

Presidenza e Segreteria 00187 Roma – Via IV Novembre, 114
Tel. 06.6976701 Fax 06.69767048
www.tuttoingegnere.it

Centro Studi Consiglio Nazionale Ingegneri

Sede: Via Dora, 1 - 00198 Roma - Tel. 06.85354739, fax 06 84241800
www.centrostudicni.it

ISBN 978-88-6014-057-9

Il presente testo è stato redatto ed elaborato da Antonello Pili e Mauro Di Giacomo.

Sommario

Premessa e sintesi

Il tema della sicurezza e della qualità delle reti e dei sistemi informativi ha assunto una rilevanza assoluta in Europa ed in Italia, in relazione al ruolo centrale che le tecnologie dell'informazione e della comunicazione hanno via via acquisto rispetto ad un numero ormai sempre più ampio di attività quotidiane e per effetto della contemporanea crescita delle minacce e degli attacchi portati ai sistemi ICT[1] da vere e proprie organizzazioni criminali.

Quando si affronta il tema della sicurezza ICT non si tratta, tuttavia, solo di fronteggiare i rischi peraltro sempre più elevati connessi alle frodi perpetrate su Internet (secondo la polizia postale nel 2010 in Italia sono state presentate 5.051 denunce da parte di utenti truffati on line, portando all'arresto di 285 persone e alla denuncia di 3.965 persone[2]), ma anche di prevenire default tecnologici nei sistemi ICT causati da eventi incidentali o dolosi capaci a loro volta di innescare il collasso delle infrastrutture critiche ormi tutte informatizzate, con la conseguenza, quindi, di mettere a repentaglio il benessere sociale e la stessa qualità della vita dei cittadini.

La percezione di rischi incombenti sui sistemi di rete e sui sistemi

1. Acronimo inglese del termine Information and Communication Technology (Tecnologie dell'Informazione e della Comunicazione).

2. Negli Usa l'Internet Crime Complaint Center (IC3) dell'Fbi solo nel corso 2010 ha raccolto invece oltre 300 mila denunce.

informatici ed i costi potenziali di eventi incidentali e attacchi, sta, così, spingendo l'Unione Europea ad accelerare i processi che portano ad un rafforzamento complessivo di tutto il sistema di *governance* e protezione della sicurezza ICT in senso lato, nonché a sollecitare gli Stati membri a costruire un sistema di regole e sanzioni comuni e più stringenti in modo particolare per individuare e proteggere le infrastrutture critiche informatizzate, così come già previsto per le altre infrastrutture critiche tradizionali (trasporti, energia, ecc.).

A fronte della crescente attenzione e consapevolezza circa i rischi di default tecnologici da eventi incidentali o dolosi, gli ingegneri e gli ingegneri dell'informazione in particolare si candidano ad acquisire un ruolo di primo piano rispetto ai processi di cambiamento nello sviluppo e gestione dei sistemi ICT orientati alla sicurezza.

In primo luogo è evidente che l'innalzamento dello status delle infrastrutture ICT di moltissimi enti pubblici e privati a "*infrastrutture critiche informatiche*", necessariamente impone un innalzamento anche del ruolo e del contributo dei professionisti chiamati a presiedere o ad intervenire su questi sistemi, considerati sempre più strategici e critici.

Le nuove e sempre più stringenti istanze di sicurezza prodotte dai nuovi indirizzi europei impongono a chi gestisce sistemi e infrastrutture di abbandonare la logica del ricorso a professionalità generiche e indistinte cui affidare queste funzioni e di mettere al centro figure professionali altamente specializzate. In questo senso gli ingegneri dell'informazione, le cui capacità e competenze tecnico professionali nella progettazione e nei modelli di sviluppo sono tutte orientate alla qualità, rappresentano una risorsa fondamentale da valorizzare.

Alte capacità e competenze tecnico professionali nella progettazione e realizzazione di sistemi ICT, deontologia ben codificata, integrazione con le altre discipline ingegneristiche, rappresentano un valore strategi-

co degli *ingegneri dell'informazione* per far fronte alla necessaria prospettiva sistemica che occorre perseguire per affrontare le problematiche connesse alla sicurezza dei sistemi ICT. La sicurezza delle reti e dei sistemi informativi comprende, infatti, ambiti diversi anche se profondamente interrelati che vanno dall'*ICT security*, che riguarda la protezione dei sistemi ICT al fine di salvaguardare i dati, le infrastrutture e gli applicativi, alla *Information security* che riguarda la protezione dei beni intangibili (informazioni, know how, brevetti, licenze ecc) aziendali e si estende sino alla *Operation security* che riguarda la protezione dei beni, delle sedi, degli impianti e delle stesse persone.

L'ingegnere ed in particolare l'ingegnere dell'informazione può giocare, in questa nuova ed ampia prospettiva di gestione della sicurezza dentro aziende, amministrazioni pubbliche ed organizzazioni che progettano, realizzano o gestiscono infrastrutture ICT, un ruolo centrale potendo inserirsi sia nelle attività di pianificazione, progettazione, sviluppo dei sistemi software e sistemi di rete, sia nelle attività di identificazione dei requisiti di sicurezza dei sistemi ICT e in quelle di definizione delle soluzioni, favorendo l'integrazione di tecnologie per la sicurezza all'interno dell'infrastruttura ICT, nonché preoccupandosi di far si che il sistema informativo sia in grado di resistere ad eventi imprevisti o ad atti dolosi (come i cyber-attacchi), che possano compromettere la disponibilità, l'autenticità, l'integrità e la riservatezza dei dati conservati o trasmessi e la fruizione stessa dei servizi offerti o resi accessibili tramite la rete o lo stesso sistema informatico.

Il nuovo orientamento alla sicurezza dei sistemi ICT apre spazi per gli ingeneri dell'informazione in nuove attività libero professionali comprendenti le verifiche di sicurezza dell'intero sistema, da affidare necessariamente a terze parti rispetto ai produttori e fornitori, allo scopo di testare dall'esterno la validità delle misure adottate e la impenetrabilità

del sistema informatici e di rete, evidenziando le eventuali "falle" e suggerendo, al bisogno, gli eventuali rimedi.

Ulteriori e potenzialmente davvero ampie occasioni professionali per gli ingegneri dell'informazione scaturiscono, inoltre, dalla emergente necessità di dare enfasi all'attività di **collaudo** di grandi e meno grandi infrastrutture informatiche a tutela degli interessi collettivi di sicurezza. Da questo punto di vista, diviene non più procrastinabile l'intervento del legislatore che attribuisca a professionisti qualificati e indipendenti quali gli *ingegneri dell'informazione*, lo svolgimento in via esclusiva dei servizi di collaudo delle reti e dei sistemi informativi. Queste attività, oggi, sono quasi sempre appaltate alle stesse società fornitrici di servizi software e di servizi di rete, col risultato di assistere spesso a collaudi incrociati tra grandi gruppi che si dividono il mercato nella fornitura di servizi ICT e che assumono di volta in volta la veste verificatori gli uni degli altri, in un evidente, insana ed inefficace condizione di conflitto di interessi.

I troppi "tilt" informatici cui stiamo assistendo negli ultimi mesi (dalle Poste italiane alla Servizio sanitario, dalla Borsa al sistema della posta certificata, per arrivare alle biglietterie ferroviarie) – sui quali potrebbe essere utilmente avviata una attività di osservatorio indipendente – evidenziano un deficit di capacità di collaudo e verifica degli stessi sistemi, proprio per la mancanza di vere "terze parti" cui affidare questa tipologia di incarichi.

Nell'affrontare dunque il tema emergente della sicurezza ICT, non si deve neppure trascurare l'ambito della produzione di software e sistemi informativi per la sicurezza, il cui valore non è affatto marginale e potrebbe offrire spazi occupazionali e di mercato per gli ingegneri dell'informazione. Si tratta di un segmento di mercato che in Italia ha un valore non trascurabile, essendo possibile stimarlo attorno al miliardo di euro (a fronte dei 15,5 miliardi di euro a livello europeo). Anche in questo caso,

occorre promuovere strumenti legislativi, finanziari e incentivi per far crescere il sistema produttivo nazionale dello sviluppo dell'industria del software e dei sistemi di rete orientati alla sicurezza.

Troppo spesso, oggi, gli ingegneri dell'informazione che si occupano di sicurezza ICT sono impiegati nei profili di vendita, sacrificando competenze anche molto avanzate in ragione di modelli di organizzazione del lavoro delle grandi imprese ICT, quasi sempre estere, che considerano il nostro paese solo come un mercato di sbocco ma non un'area avanzata da cui attingere risorse qualificate per fare ricerca e sviluppo.

Va anche detto che se è vero che tutti i corsi di ingegneria informatica prevedono un corso sulla sicurezza ICT è altrettanto vero che mancano i fondi pubblici per finanziare progetti di ricerca teorica ed applicata sul tema della sicurezza dei sistemi ICT. Anche laddove si riescono a formare alte professionalità in questo campo la strada per proseguire nella ricerca è quella dell'estero: Germania, Francia e Regno Unito continuano ad assorbire alte qualifiche, anche dall'Italia, potendo disporre di ingenti fondi per la ricerca.

Una generale presa di consapevolezza sul tema della sicurezza nell'ICT dovrebbe necessariamente preoccuparsi anche di sostenere la ricerca più avanzata nazionale, anche perché fare leva sul tema della sicurezza offrirebbe la possibilità di estendere e valorizzare tutta la filiera del software e dei servizi ICT, settore che in Italia ha un valore complessivo, al 2010, di oltre 12 miliardi di euro, senza considerare i nuovi servizi aziendali di testing, collaudo e verifica.

Con un nuovo effettivo impulso alla nascita di un sistema di *governance* della sicurezza ICT, gli ingegneri e gli ingegneri dell'informazione in particolare si candidano, infine, per assumere un ruolo chiave anche nella gestione delle *policy* e degli strumenti operativi pubblici e privati per la sicurezza ICT. Da un lato, questa categoria professionale,

come già osservato, può muoversi su ambiti tecnologici differenti ma complementari, facilitando l'integrazione tra le diverse componenti e funzioni che interagiscono nel sistema della sicurezza; dall'altro, come comunità professionale caratterizzata da una profonda identità culturale e una non comune capacità di assunzione di responsabilità, *essa può svolgere autorevolmente anche un ruolo di indirizzo e dialogo con le istituzioni e con i decisori per contribuire a migliorare la cultura e gli approcci complessivi alla sicurezza dei sistemi di rete ed informativi.*

Il nostro paese, per ora, si è limitato a recepire le indicazioni europee soprattutto rispetto ai reati penali connessi alle violazioni di sicurezza ICT e alle frodi, mentre manca ancora un disegno strategico complessivo per sviluppare un sistema di *governance* della sicurezza ICT coordinato ed effettivo. Si assiste, piuttosto, per effetto di impulsi scaturenti da singoli enti e istituzioni, alla proliferazione di strutture e di soggetti, molti dei quali peraltro non hanno neppure trovato una compiuta operatività.

In particolare, risulta ancora incompleto il percorso di definizione delle norme sottese a garantire la sicurezza della cosiddetta *PA digitale*, mentre assolutamente deficitarie sono le disposizioni connesse all'aggiudicazione dei contratti pubblici ed all'espletamento delle prestazioni relative ai servizi informatici; il valore economico di questa tipologia di contratti, peraltro, è nettamente superiore a quello relativo ai servizi di ingegneria connessi all'iper-regolamentato comparto dei lavori pubblici.

La sicurezza in ambito di *PA digitale* è governata dal *Codice della Amministrazione Digitale* (D.Lgs. n. 82/2005, aggiornato recentemente dal D.Lgs. 235/2010). Il Codice prevede (art.12) che: *"Le pubbliche amministrazioni adottano le tecnologie dell'informazione e della comunicazione nei rapporti interni, tra le diverse amministrazioni e tra queste e i privati, con misure informatiche, tecnologiche, e procedurali di sicurezza, secondo le regole tecniche di cui all'articolo 71"*. Spetta a tali *regole tecniche* l'individuazione (art. 51)

delle "*modalità che garantiscono l'esattezza, la disponibilità, l'accessibilità, l'integrità e la riservatezza dei dati, dei sistemi e delle infrastrutture*". A tutt'oggi queste regole tecniche non sono ancora state emanate.

Secondo l'Autorità per la vigilanza sui contratti pubblici nel 2010, il valore dei contratti aggiudicati relativamente ai servizi informatici (consulenza, sviluppo di software, Internet e supporto) è risultato pari a 2,41 miliardi di euro mentre quello dei contratti aggiudicati per i servizi architettonici, di costruzione, ingegneria e ispezione si è fermato, nello stesso periodo, a 349 milioni di euro. Nonostante questo, il livello di regolamentazione per l'espletamento di tali prestazioni è incomparabilmente più generico rispetto a quello definito per i servizi d'ingegneria connessi ai lavori pubblici, cui è dedicato il maggior numero di articoli sia del Codice (D.Lgs. 163/2006) che del Regolamento (DPR 207/2010).

Il D.Lgs. 163/2006, infatti, è privo di norme specifiche che regolano i contenuti e la validazione della progettazione dei servizi e dei sistemi d'informazione nonché il collaudo degli stessi. Il Regolamento, d'altro canto, presenta solo una generica e insufficiente definizione dei contenuti della progettazione, comune per tutti i servizi e le forniture. Secondo l'art. 279 del DPR 207/2010 la progettazione "*è articolata di regola in un unico livello*" contenente: la relazione tecnica-illustrativa con riferimento al contesto in cui è inserita la fornitura o il servizio, le indicazioni e disposizioni per la stesura dei documenti inerenti la sicurezza, il calcolo della spesa per l'acquisizione del bene o del servizio con indicazione degli oneri della sicurezza non soggetti a ribasso, il prospetto economico degli oneri complessivi necessari per l'acquisizione del bene o del servizio, il capitolato speciale descrittivo e prestazionale, lo schema di contratto.

Di norma la progettazione «è predisposta dalle amministrazioni aggiudicatrici mediante propri dipendenti in servizio» (art. 279, comma 2) mentre possono essere posti a gara solo i contratti aventi ad oggetto

«prestazioni particolarmente complesse sotto il profilo tecnologico ovvero che richiedono l'apporto di una pluralità di competenze ovvero caratterizzate dall'utilizzo di componenti o di processi produttivi innovativi o dalla necessità di elevate prestazioni per quanto riguarda la loro funzionalità» (art. 300, comma 2, lett. b). La stazione appaltante può (e non deve) stabilire di sottoporre a verifica il progetto; infine, non è disposto il collaudo del servizio o sistema d'informazione fornito ma solo una «verifica di conformità» (art. 312 e ss).

Gli ingegneri, e gli ingegneri dell'informazione in particolare, si candidano dunque a favorire, consolidare e orientare questo processo in atto, accelerando e razionalizzando le dinamiche ancora troppo poco incisive, e soprattutto promuovendo la cultura della sicurezza ICT, di fatto non ancora introiettata compiutamente dalla classe politica italiana e dal legislatore, quasi del tutto inconsapevole che un collasso delle infrastrutture critiche informatizzate può, ormai, mettere a repentaglio il benessere sociale e la stessa qualità della vita dei cittadini.

Romeo La Pietra

1. Sicurezza e qualità: il binomio inscindibile della crescita sostenibile dell'Europa tecnologica

Da oltre un decennio, riconoscendo il ruolo strategico dell'ICT, a fronte della crescita esponenziale dei fenomeni di cybercrime, l'Europa ha posto al centro delle sue decisioni strategiche anche la necessità di garantire la sicurezza dei sistemi informatici e di rete.

L'Unione Europea ha attribuito alla questione della sicurezza dei sistemi Informatici e delle reti di comunicazione una valenza ampia, ricomprendendo sia le questioni relative alla protezione dei sistemi da intrusioni e attacchi portati da agenti interni o esterni e da software ostili, sia gli aspetti della qualità, intesa prima di tutto come affidabilità, resilienza e robustezza del software e delle reti ma anche qualità delle procedure di sviluppo e della verificabilità, manutenibilità, leggibilità ed evolvibilità dei sistemi informatici e dei sistemi di rete.

Da anni l 'Europa attraverso Comunicazioni, Direttive, Decisioni sta spingendo gli Stati membri ad individuare strutture e organi di controllo e di sicurezza in ogni paese e a dotarsi di infrastrutture e piani per la sicurezza ICT come pure a cooperare per costruire un quadro europeo di norme condivise in merito a reati informatici e sanzioni.

È utile, allora, ripercorrere il sistema di interventi e misure prodotto a livello europeo.

Il punto di svolta nella produzione di indirizzi, di messa punto di politiche e linee guida per la sicurezza ICT a livello europeo, può essere

fatto risalire all'inizio del 2001 con la comunicazione *Network and Information Security: Proposal for An European Policy Approach*[3] a cui hanno fatto seguito lo stesso anno (subito dopo i fatti dell'11 settembre 2001) atti di indirizzo comprendenti Raccomandazioni e Piani strategici[4] che hanno portato a prevedere alcune prime soluzioni operative per gli Stati membri, in primo luogo prevedendo il potenziamento e la messa in rete dei CERT[5] nazionali ovvero di quegli organismi pubblici e privati preposti all' intervento in caso di emergenza informatica.

Il 2001 è stato anche l'anno di firma della prima "*Convenzione sulla criminalità informatica*" firmata dal Consiglio d'Europa e considerata, ad oggi, come la norma internazionale più completa ed esaustiva sui vari aspetti della criminalità informatica[6].

L'anno successivo è stata la volta della Direttiva quadro sulla sicurezza e l'integrità delle reti e dei servizi di comunicazione (2002/21/Ce),

3. Brussels, 6.6.2001 COM(2001)298 final.

4. Tra cui Comunicazione della Commissione al Consiglio, al Parlamento europeo, al Comitato economico e sociale e al Comitato delle Regioni - Creare una società dell'informazione sicura migliorando la sicurezza delle infrastrutture dell'informazione e mediante la lotta alla criminalità informatica - eEurope 2002 e "*Raccomandazione relativa alla strategia per creare una società dell'informazione sicura*" del Parlamento (2001/2070/CO).

5. Con il termine Cert si intende un Computer Emergency Response Team che si sostanzia in una struttura o un ufficio collocato in genere presso università o enti pubblici e/o governativi, incaricato di raccogliere le segnalazioni di incidenti informatici e potenziali vulnerabilità nei software che provengono dalla comunità degli utenti. In Italia sono presenti 8 Cert. Il Cert di DigitPA fornisce alle amministrazioni pubbliche italiane servizi di prevenzione, monitoraggio, coordinamento informativo e analisi degli incidenti di sicurezza nell'ambito del sistema pubblico di connettività (SPC).

6. La Convenzione è stata ratificata da 17 Stati Membri è entrata in vigore il 1° luglio 2004. L'Italia nel 2008, per ratificare la convenzione ha modificato alcune norme di carattere penale.

e di una Risoluzione del Parlamento in cui si evidenziava la necessità di realizzare una "Task force" sulla sicurezza delle reti con determinati specifici obiettivi[7]. Nel 2004, viene varata l'Enisa (*European Network and Information Security Agency*), l'agenzia finalizzata ad aiutare la Commissione europea, gli Stati membri e la comunità imprenditoriale ad affrontare, rispondere ai problemi di sicurezza delle reti informatiche.

Il tema della difesa dalla criminalità informatica e dei rischi sulla sicurezza informatica da azioni dolose negli anni ha assunto un peso sempre più importante nella discussione europea, in ragione della sempre più estesa diffusione della rete Internet tra i cittadini e della sempre maggiore estensione degli attacchi e dei comportamenti fraudolenti.

Le strategie di intervento sono state così ulteriormente messe a punto nel 2005 con una decisione quadro (2005/222) del Consiglio d'Europa relativa agli attacchi contro i sistemi di informazione, emanata con l'obiettivo di migliorare la cooperazione tra le autorità giudiziarie e le altre autorità competenti degli Stati membri, compresi gli altri servizi specializzati incaricati dell'applicazione della legge, mediante il ravvicinamento delle legislazioni penali degli Stati membri nel settore degli attacchi contro i sistemi di informazione.

Sempre nel 2005 la Commissione ha sottolineato, inoltre, l'urgenza

7. Altri testi importanti in materia di sicurezza informatica sono la Risoluzione del Consiglio UE del 18/02/2003 avente come titolo "*Per una cultura della sicurezza delle reti e dell'informazione*", nella quale, tra l'altro, si invitano gli Stati membri a promuovere la sicurezza quale componente essenziale del governo pubblico e privato, in particolare incoraggiando l'assegnazione delle responsabilità, e la Posizione Comune n. 39-2003, definita dal Consiglio il 26/05/2003 in vista della Decisione del Parlamento Europeo e del Consiglio circa l'adozione di un piano pluriennale (2003-2005) per il monitoraggio del piano di azione *eEurope*, la diffusione delle buone prassi ed il miglioramento della sicurezza delle reti e dell'informazione (MODINIS).

di coordinare le azioni per rafforzare la fiducia di tutti gli interessati nelle comunicazioni e nei servizi elettronici[8], mentre l'anno successivo è stata adottata una strategia per una società dell'informazione sicura a cui ha fatto seguito nel 2007 una nuova risoluzione approvata dal Consiglio e destinata a porre l'attenzione sull'importanza della sicurezza e della resilienza delle infrastrutture ICT[9].

Nel 2009 viene emanata una nuova Direttiva, la n. 140, che per incrementare la sicurezza e l'integrità delle reti e dei servizi di comunicazione modifica la Direttiva quadro 2002/21/Ce, introducendo due nuovi articoli (13 bis e 13 ter); attraverso essi si impone alle imprese di comunicazione di adottare idonee misure di sicurezza nella gestione dei rischi e si rafforzano i poteri delle autorità di controllo, introducendo la facoltà di impartire istruzioni vincolanti e imporre alle imprese di fornire le informazioni necessarie per valutare la sicurezza e l'integrità dei loro servizi e delle loro reti. Le imprese, in base alla nuova direttiva, devono inoltre sottostare a verifiche (a loro carico) sulla sicurezza effettuate da un organismo qualificato indipendente o dall'autorità nazionale.

Nel 2010 l'Agenda digitale europea[10] (una delle sette iniziative faro della strategia Europa 2020) preconizza una nuova direttiva della Commissione *che abroghi la decisione quadro 2005/222/GAI del Consiglio, relativa agli attacchi contro i sistemi di informazione,* e armonizzi le legislazioni penali degli Stati membri nell'ambito degli attacchi contro i sistemi di informazione introducendo norme più adatte ad affrontare al meglio i rischi

8. COM (2005) 229 final - "i2010 – A European Information Society for growth and employment".

9. (2007/068/01) - "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience".

10. COM (2010) 245 – Un'Agenda digitale Europea".

derivanti dai nuovi metodi utilizzati dai criminali, con riguardo in particolare all'uso delle cosiddette tecniche *Botnet*[11] anche in relazione allo svolgimento delle indagini e dei procedimenti giudiziari nei casi transfrontalieri.

11. Si tratta di una tecnica che permette di assoggettare indebitamente al controllo esterno, attraverso software malevoli, reti di computer altrui, al fine di condurre attraverso gli stessi computer azioni di pirateria on line su altri sistemi informativi.

2. Il ruolo dell'ICT e delle infrastrutture critiche informatizzate nel sistema europeo

La percezione di un rischio incombente sui sistemi di rete e sui sistemi Informatici , ha spinto l'Unione Europea non solo ad accelerare i processi che portano ad un rafforzamento complessivo di tutto il sistema di governance e protezione della sicurezza ICT in senso lato ma anche in modo particolare delle infrastrutture critiche informatizzate, così come già previsto per le altre infrastrutture critiche relative alla produzione, al trasporto ed alla distribuzione di energia (elettrica, gas ecc.) e ai trasporti in generale. La Direttiva 114/08 CE ha individuato proprio nel settore della *Information and Communication Technology* (ICT) l'area infrastrutturale più critica sui cui l'Unione deve avviare nel corso del 2011 la procedura di regolazione dei modelli di gestione condivisa dei rischi.

Nell'ambito delle infrastrutture critiche si parla infatti da alcuni anni in Europa anche di *Critical Information Infrastructure* (CII)[12]: ovvero di quei sistemi ICT che rappresentano essi stessi infrastrutture critiche o che sono essenziali per l'operatività di altre infrastrutture critiche (telecomunicazioni, computer, software, Internet, satelliti, etc.). Il rischio di una avaria di sistema in infrastrutture critiche informatizzate, avrebbe, infatti, pos-

12. Bruxelles, 17.11.2005 Com(2005) 576 Definitivo : Libro Verde relativo a "*Un programma europeo per la protezione delle infrastrutture critiche*".

sibili impatti sui sistemi di governo, sulle comunicazioni complessive, sulla distribuzione di energia, sui trasporti e sul sistema finanziario con danni immediati, ma potrebbe anche mettere rischio completamente le funzioni delle infrastrutture critiche complessive dei sistemi paese, attraverso l'innesco di un pericoloso effetto a catena, alimentato dalla sempre maggiore interconnessione esistente tra i sistemi paese e tra le varie infrastrutture.

I temi della sicurezza ICT in senso lato e della sicurezza ICT legata al funzionamento delle infrastrutture critiche nazionali ed europee, pur fortemente interrelati hanno, però, mantenuto, almeno sino ad anni molto recenti, una netta differenziazione a livello di norme e prese di posizione ufficiali europee, probabilmente anche a causa dei diversi organismi e strutture Ue preposti al loro governo e controllo.

Nel 2009 la Commissione ha rilanciato, così, con forza la posizione europea sul tema delle CII intese come autonomo campo di interesse, con una comunicazione[13]in cui ha ribadito la necessità di "*Proteggere le infrastrutture critiche informatizzate e rafforzare la preparazione, la sicurezza e la resilienza per proteggere l'Europa dai ciberattacchi e dalle ciberperturbazioni*", prevedendo un piano d'azione (il "piano d'azione CIIP": Critical Information Infrastructure Protection) destinato a rafforzare la preparazione e la resilienza delle infrastrutture ICT fondamentali.

Scopo di tale comunicazione era quello incentivare e sostenere lo sviluppo, sia a livello europeo che a livello nazionale, di un elevato livello di preparazione, sicurezza e capacità di resilienza[14].

Questo approccio è stato ampiamente sostenuto anche dal Consiglio

13. COM(2009) 149 - Critical Information Infrastructure Protection.

14. Intesa come capacità di un sistema ICT di adattarsi alle condizioni d'uso e di resistere a shock differenti.

nel 2009[15] mentre solo con la già citata *Agenda digitale europea*, adottata nel maggio 2010, e le relative conclusioni del Consiglio[16], la questione delle CII è stata definitivamente collegata al tema della sicurezza ICT in senso lato, sulla base della convinzione che la fiducia e sicurezza dei sistemi ICT sono condizioni fondamentali per un'ampia diffusione delle stesse tecnologie dell'informazione e della comunicazione e, dunque, per il conseguimento stesso degli obiettivi della dimensione di "crescita intelligente" della strategia Europa 2020[17].

L'Agenda digitale europea ha sottolineato del resto la necessità, per tutte le parti interessate, di unire le forze in un impegno globale per rafforzare la sicurezza e la resilienza delle infrastrutture ICT, incentrando il loro intervento sulla prevenzione, la preparazione e la sensibilizzazione e per istituire meccanismi efficaci e coordinati nel rispondere a nuove forme di attacchi e di criminalità informatici sempre più sofisticati, seguendo un approccio basato quindi sulla "*prevenzione*" e sulla "*reazione*".

Successivamente, come annunciato nell'Agenda digitale, sono state adottate altre misure: nel settembre 2010 la Commissione ha adottato una proposta di direttiva relativa agli attacchi contro i sistemi di informazione[18] che mira a rafforzare la lotta contro la criminalità informatica mediante il ravvicinamento delle legislazioni penali degli Stati membri e

15. Risoluzione del Consiglio, del 18 dicembre 2009, su un approccio europeo cooperativo in materia di sicurezza delle reti e dell'informazione (2009/C-321/01).

16. Conclusioni del Consiglio del 31 maggio 2010 su un'Agenda digitale europea (10130/10).

17. COM(2010) 2020 e Conclusioni del Consiglio europeo del 25 e 26 marzo 2010 (EUCO 7/10).

18. COM(2010) 517 definitivo. - Proposta di direttiva del Parlamento Europeo e del Consiglio relativa agli attacchi contro i sistemi di informazione, e che abroga la decisione quadro 2005/222/GAI del Consiglio.

migliorando la cooperazione tra autorità giudiziarie e altre autorità competenti anche per far fronte a nuovi tipi di attacchi informatici, in particolare le offensive da "*botnet*".

Ad integrazione di questo testo, la Commissione ha presentato a fine 2010 una proposta relativa ad un nuovo mandato per rafforzare ed ammodernare l'Agenzia europea per la sicurezza delle reti e dell'informazione (ENISA) istituita nel 2004 con l'obiettivo di implementare la fiducia e la sicurezza delle reti. Il rafforzamento e la modernizzazione dell'ENISA dovrebbe supportare anche l'Unione europea, gli Stati membri e i partner privati a sviluppare le loro capacità e il loro grado di preparazione nel prevenire, individuare e combattere i problemi di sicurezza informatica.

Il quadro normativo europeo relativamente alla protezione delle "*infrastrutture critiche informatizzate*" è stato da ultimo integrato nel marzo del 2011 da una Comunicazione[19] della Commissione al Parlamento europeo: *Realizzazioni e prossime tappe: verso una sicurezza informatica mondiale",* in cui si fa il punto della situazione sulla base della precedente Comunicazione n. 149 del 2009 nella quale si definiva un piano d'azione (CIIP) per rafforzare la sicurezza e la resilienza delle infrastrutture critiche informatizzate.

La comunicazione del 2011 ribadisce così il piano di lavoro che la Commissione, gli Stati membri e/o il settore industriale devono realizzare nell'ambito dei 5 macro obiettivi relativi a:

- preparazione e prevenzione;
- individuazione e risposta;
- mitigazione e recupero;

19. COM (2011) 163 - Critical Information Infrastructure Protection: 'Achievements and next steps: towards global cyber-security'.

- cooperazione internazionale;
- criteri per le infrastrutture critiche europee nel settore delle ICT con l'aiuto dell'Agenzia europea per la sicurezza delle reti e dell'informazione (ENISA).

Per quanto riguarda la *Preparazione e prevenzione* degli attacchi va osservato che già nel 2009 l'ENISA e la rete dei CERT dell'UE hanno definito una base minima di capacità, servizi e "requisiti essenziali" che le CERT nazionali devono possedere. Sulla base di questi requisiti le CERT nazionali dovranno così diventare elementi-chiave delle capacità nazionali in termini di preparazione, scambio di informazioni, coordinamento e reazione agli attacchi informatici. Ad oggi, 20 Stati membri hanno istituito il CERT[20] ma entro la fine del 2011 ogni Stato membro dovrà disporre di un CERT operativo.

Risale ancora al 2009 anche il partenariato pubblico-privato europeo per la resilienza (EP3R) che costituisce un primo tentativo di *governance* a livello europeo della resilienza delle infrastrutture ICT , incentivando la cooperazione tra pubblico e privato sempre al fine di rafforzare la gestione globale dei rischi delle reti informatiche. Nell'ambito dell'EP3R, sono stati istituiti tre gruppi di lavoro su:

a) punti di forza, risorse e funzioni per la fornitura (sicura e continua) di comunicazioni elettroniche tra paesi;
b) requisiti di base in materia di sicurezza e resilienza delle comunicazioni elettroniche;
c) esigenze di coordinamento e cooperazione e meccanismi di preparazione e di reazione nel caso di disfunzioni su larga scala che incidono sulle comunicazioni elettroniche.

Sempre, nel 2009 ha visto la luce anche il Forum europeo degli Stati

20. Cfr. nota 5.

membri (EFMS) per favorire gli scambi tra autorità pubbliche delle "buone pratiche" in materia di:

a) criteri per l'individuazione delle infrastrutture ICT europee;
b) priorità, principi e orientamenti europei per la resilienza e la stabilità di internet.

Nel futuro l'EFMS si occuperà dell'organizzazione di esercitazioni di sicurezza informatica. Inoltre, l'EFMS provvederà a:

- elaborare metodi per la cooperazione tra le CERT nazionali;
- definire prescrizioni minime negli appalti pubblici per rafforzare la sicurezza informatica;
- definire incentivi, di carattere economico e normativo, a favore della sicurezza e della resilienza;
- valutare lo stato della "sicurezza informatica" in Europa.

Per quanto riguarda l'area definita *Individuazione e risposta* verrà creato un Sistema europeo di condivisione delle informazioni e di allarme (EISAS). Durante il 2011 l'ENISA assisterà gli Stati membri nel creare il sistema nazionale di condivisione delle informazioni e di allarme (ISAS). Nel 2012 sarà, invece, la volta dell'integrazione di tutti i sistemi ISAS nazionali nell'EISAS.

Nell'ambito dell'area *Mitigazione e recupero* la Comunicazione del marzo 2011 fa riferimento ai "*Piani di emergenza ed esercitazioni nazionali*" quale strumento da sviluppare, tenuto conto che, a fine del 2010, 12 Stati membri tra cui l'Italia, avevano un piano nazionale di emergenza e/o organizzato esercitazioni. La Commissione evidenzia come l'ENISA abbia elaborato una guida sulle esercitazioni nazionali e che per rafforzare il coordinamento europeo, l'ENISA continuerà a sostenere gli Stati membri nel definire piani di emergenza nazionali e nell'organizzazione di esercitazioni. Le esercitazioni nel settore della sicurezza informatica sono, infatti, un elemento essenziale di una strategia coerente. Le future eserci-

tazioni paneuropee dovrebbero essere varate sulla base di un piano di emergenza europeo che si collega ai piani di emergenza nazionali. Il piano dovrebbe fornire meccanismi e procedure per la comunicazione tra Stati membri. Entro il 2012 tutti gli Stati membri dovranno avere un piano di emergenza nazionale e predisporre esercitazioni periodiche di reazione e ripristino.

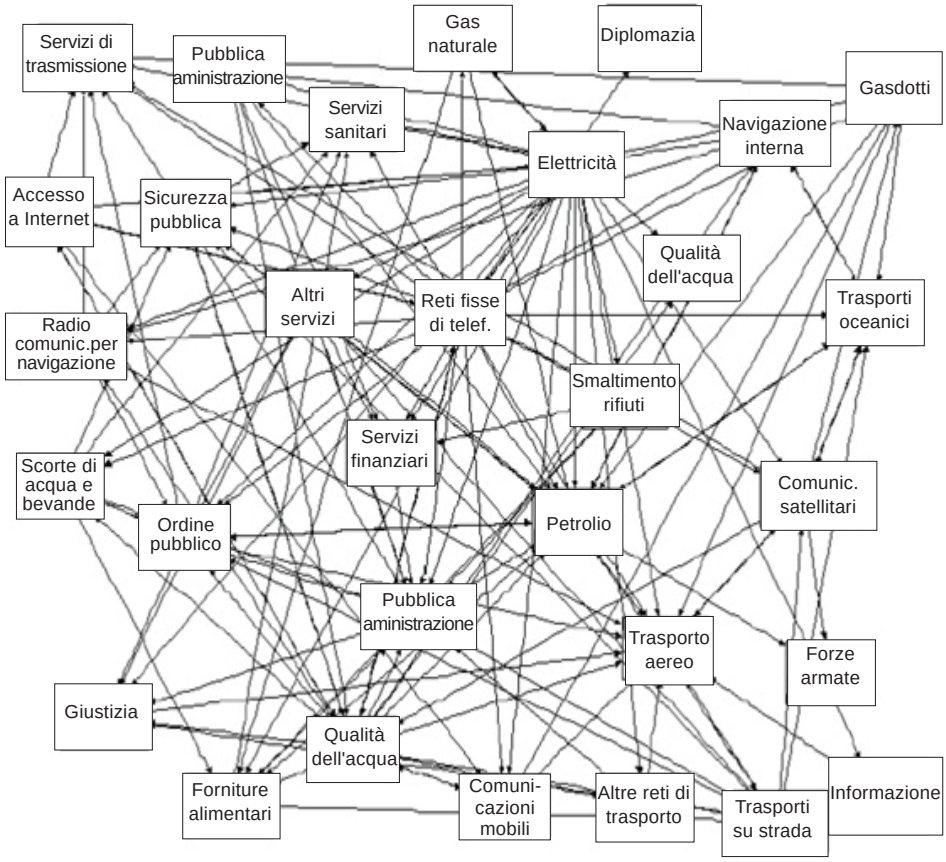
Nell'importante ambito della *Cooperazione internazionale* e sulla base del lavoro dell'EFMS sono stati elaborati principi e orientamenti europei per la resilienza e la stabilità di internet.

Infine, con riferimento ai Criteri per le infrastrutture critiche europee nel settore ICT la comunicazione del marzo 2011 n. 163, osserva come dovranno essere definiti criteri settoriali per l'individuazione delle infrastrutture critiche europee nel settore delle TIC e come le discussioni tecniche abbiano già portato ad una prima versione di questi criteri per le comunicazioni (fisse e mobili) e internet.

Vale la pena osservare come la tematica delle *infrastrutture critiche* (IC) sia un elemento chiave nell'ambito della sicurezza informatica, soprattutto per l'interconnessione e l'interoperabilità che esiste tra le diverse infrastrutture. Queste strette relazioni di interdipendenza tra le IC (pubbliche e private) si possono comprendere meglio osservando la figura 1 che è stata pubblicata in un recente lavoro dell'Ocse (a cura dell'Istituto di ricerca olandese *Tno*). Lo schema prova a descrivere a livello grafico, le innumerevoli connessioni tra strutture anche profondamente diverse e lontane tra loro tra infrastrutture ed è utile a prendere atto, qualora ce ne fosse bisogno, della grande complessità che bisogna essere in grado di gestire e proteggere.

Sulla stessa scia si colloca infine anche il progetto *DOMINO*. Come è noto la Direttiva Europea 114/08/CE è finalizzata alla individuazione di infrastrutture dislocate nel territorio dell'Unione Europea che, qualora

Fig. 1 - L'interdipendenza tra le infrastrutture critiche



Fonte: elaborazione Centro studi CNI su dati OECD/IFP Project on "Future Global Shocks-Reducing Systemic Cybersecurity Risk" Peter Sommer, Information Systems and Innovation Group, London School of Economics Ian Brown, Oxford Internet Institute, Oxford University.

non fossero più in grado di funzionare in modo corretto (sia per cause antropiche, sia per cause naturali), potrebbero indurre, direttamente o per *effetto domino*, una inaccettabile degradazione della qualità di vita dei cittadini. Per poter favorire l'applicazione della Direttiva è, quindi, necessario acquisire informazioni sul funzionamento delle varie strutture (sociali, economiche, fisiche) e individuare *in primis* le interconnessioni funzionali tra esse. Per fare ciò è partita l'"Indagine pilota", che rappresenta il primo passo operativo del progetto *DOMINO*. L'indagine, rivolta ad esperti dei vari settori economici e sociali che forniscono un bene o un servizio, ha lo scopo di acquisire informazioni per comprendere meglio la cosiddetta "catena di fornitura", che può essere definita come l'insieme delle fasi, che a partire dall'approvvigionamento delle materie prime, forniscono beni e servizi a cittadini e imprese. Qui di seguito, nella tavola 1 si può leggere un elenco delle infrastrutture (economiche e sociali) oggetto dell'indagine pilota.

In ambito europeo sono già previste, quindi, una serie di iniziative strategiche di carattere normativo e tecnico già attuate o da attuare nel futuro per garantire una maggiore sicurezza dei cittadini nell'ambito del cyberspazio. E, per capire la rilevanza e la strategicità dei sistemi di rete e sistemi informativi vale la pena osservare i dati dell'ultima *survey* del World Economic Forum condotta nel mese di gennaio 2011, su un ampio panel di decisori, leader politici ed esponenti dell'economia a livello internazionale. Una larga quota di interpellati ha ipotizzato che il verificarsi di una avaria grave nelle infrastrutture critiche informatizzate possa concretamente verificarsi, riconoscendo ad un evento del genere non solo la possibilità di accadere nei prossimi 10 anni (con una probabilità pari al 20%) ma anche indicando una valutazione assai rilevante in termini di impatto sul sistema economico globale (fig.2). Secondo il panel il danno di una grave avaria dei sistemi ICT a livello internazionale sarebbe

Tav. 1 - Elenco delle infrastrutture oggetto dell'indagine pilota del progetto DOMINO

1. Acqua
1.1. Acqua potabile
1.2. Irrigazione
1.3. Acqua per uso industriale

2. Agricoltura, allevamento, pesca e silvicoltura
2.1. L'agricoltura ei suoi prodotti
2.2. L'aumento e suoi prodotti
2.3. La pesca ei suoi prodotti
2.4. Forestale
2.5. Legno

3. **Cibo**
3.1. Alimenti surgelati
3.2. Alimenti freschi
3.3. Alimenti a lunga conservazione
3.4. Bevande (incluse bottiglie acqua)

4. Ambiente
4.1. Conservazione del territorio
4.2. Qualità delle acque (oceani, mari, laghi, fiumi)
4.3. Qualità dell'aria
4.4. Dighe
4.5. Acque reflue
4.6. Smaltimento rifiuti
4.7. Smaltimento rifiuti speciali
4.8. Servizi Meteo e climatici

5. Commercio
5.1. Vendite all'ingrosso
5.2. Vendite al dettaglio

6. Cultura, luoghi di aggregazione
6.1. Istruzione
6.2. Ricerca
6.3. Associazionismo
6.4. Arte, sport, attività di animazione,beni culturali
6.5. Luoghi di culto

7. Energia
7.1. Corrente elettrica
7.2. GPL
7.3. Petrolio grezzo
7.4. Carburanti (benzina, diesel, biodiesel,...)
7.5. Carbone
7.6. Metano

8. Finanza
8.1. Contanti
8.2. Servizi di pagamento (contanti esclusi)
8.3. Assicurazioni, riassicurazioni e fondi pensione
8.4. Borsa e titoli
8.5. Prestiti e mutui

9. Industria
9.1. Filiera Tessile
9.2. Filiera produttori di abbigliamento
9.3. Filiera pelli e pellicce
9.4. Filiera chimica
9.5. Filiera metallurgica
9.6. Filiera elettronica
9.7. Filiera mobilifici
9.8. Filiera prodotti in legno, paglia
9.9. Filiera carta per alimenti
9.10. Filiera gomma e plastica
9.11. Filiera vetro
9.12. Cave minerali non metalliferi
9.13. Filiera ceramica, terracotta, porcellana, minerali non metallici
9.14. Estrazione metalli
9.15. Filiera prodotti metallici per alimentaz.
9.16. Filiera dispositivi elettrici, apparecchi per uso domestico
9.17. Filiera macchinari e metalli
9.18. Filiera delle costruzioni
9.19. Altri beni

Segue

Segue **Tav. 1 - Elenco delle infrastrutture oggetto dell'indagine pilota del progetto DOMINO**

10. Informazioni e comunicazioni (TIC)
10.1. Trasmissioni radio
10.2. Trasmissioni televisive
10.3. Internet e scambio dati
10.4. Editoria (libri, periodici e giornali)
10.5. Poste
10.6. Reti telefoniche
10.7. Reti cellulari
10.8. Servizi satellitari
10.9. Servizi di comunicazione radio

11. Istituzioni e pubblica amministrazione
11.1. Istituzioni politiche (nazionali, regionali e locali)
11.2. Ordine pubblico /sicurezza
11.3. Protezione civile
11.4. Difesa civile
11.5. Pubblica amministrazione e servizi per la popolazione (Ufficio del Registro, ufficio elettorale, licenze, concessioni, autorizzazioni, ecc)
11.6. Giustizia
11.7. Difesa
11.8. Carceri
11.9. Affari esteri (diplomazia)
11.10. Sistemi di riscossione

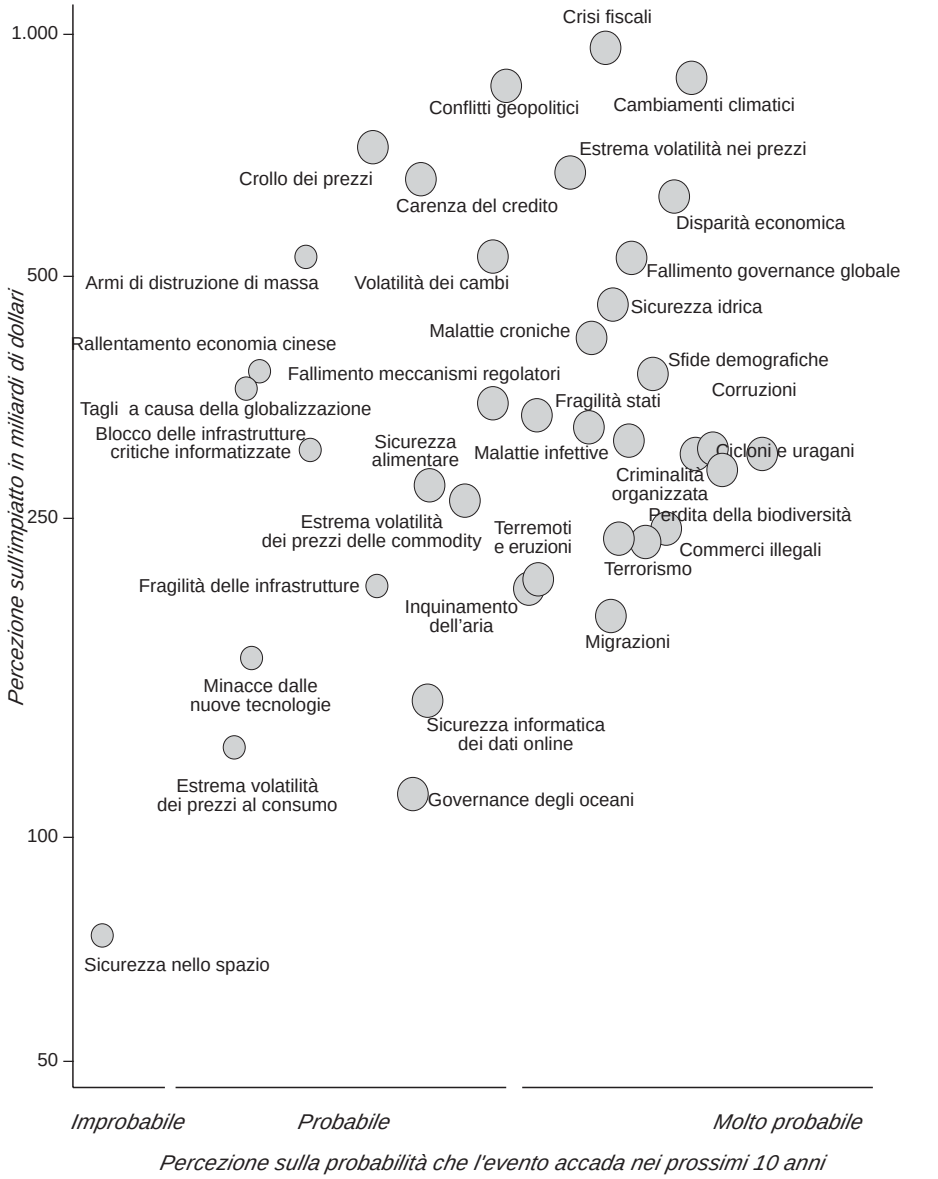
12. Servizi sanitari
12.1. Servizi pubblici e privati, medici
12.2. Consultori di psicologia
12.3. Manodopera
12.4. Assistenza sociale
12.5. Farmacie
12.6. Servizi di emergenza sanitaria
12.7. Servizi veterinari

13. Servizi
13.1. Servizi di alloggio
13.2. Attività ristoranti e alimentari
13.3. Attività software
13.4. Attività informatiche
13.5. Attività immobiliari
13.6. Consulenza (legale, contabilità, analisi dei rischi)
13.7. Pubblicità e ricerche di mercato
13.8. Servizi di *facility* (pulizie, lavanderia, manutenzione…)
13.9. Attività di lavoro dipendente
13.10. Servizi di sicurezza privata
13.11. Altri servizi (grafica, fotografia, ottica ...)

14. Trasporti e Logistica
14.1. Trasporto (pubblico e privato) di passeggeri su strada
14.2. Trasporto di merci su strada
14.3. Trasporto passeggeri per via aerea
14.4. Trasporto di merci per via aerea
14.5. Trasporto ferroviario
14.6. Trasporto merci e logistica su rotaia
14.7. Trasporto passeggeri via mare
14.8. Trasporto di merci e logistica via mare
14.9. Trasporto per via navigabile di passeggeri
14.10. Trasporto di merci per via navigabile

Fonte: Indagine Pilota v. 5.1 -15 settembre 2010 nell'ambito del Progetto Domino.

Fig. 2 - Mappa del grado di probabilità dei rischi globali e loro impatto economico. Anno 2011



Fonte: World Economic Forum, Jan11, survey

quantificabile in termini di effetti sull'economia e sulla produzione e nei servizi in un importo pari a circa 250 miliardi di Euro. Il rischio di una avaria di sistema in infrastrutture critiche, avrebbe, infatti, possibili impatti sui sistemi di governo, sulle comunicazioni complessive, sulla distribuzione di energia, sui trasporti e sul sistema finanziario con danni immediati, ma potrebbe anche mettere rischio completamente le funzioni delle infrastrutture critiche complessive dei sistemi paese, attraverso l'innesco di un pericoloso effetto a catena, alimentato dalla sempre maggiore interconnessione esistente tra i sistemi paese e tra le varie infrastrutture.

Molto avvertito dallo stesso panel qualificato, anche il rischio di una possibile caduta repentina della sicurezza sui sistemi e transazioni on line sempre nel corso dei prossimi anni, rispetto alla loro capacità di garantire privacy e riservatezza, con il rischio di una immediata probabile crescita di frodi on line e di una generalizzata perdita di fiducia rispetto all'*e-commerce* e rispetto alle altre transazioni che riguardano procedure che implicano trasmissione di dati sensibili e o procedure riservate. Gli interpellati del WEF rilevano anche in questo caso come l'impatto complessivo in termini di costi e mancati guadagni raggiunga cifre molto consistenti, valutate nell'ordine di almeno 150 miliardi di euro.

3. Sicurezza dei Sistemi ICT e Crimini Informatici: il quadro delle minacce incombenti

Come osservato il tema della resilienza e della capacità di sostenere attacchi e incidenti con l'aumento del numero e della portata delle minacce esterne ai sistemi informativi si sta spostando necessariamente sempre più sul tema della **potenziale vulnerabilità** a fronte di attacchi minacce informatiche.

Sia le ultime valutazioni europee, a partire da quella che accompagna il piano d'azione CIIP, sia la Comunicazione del marzo 2011, come pure numerose analisi e studi effettuati da parti interessate, private e pubbliche, pongono in evidenza non solo la dipendenza sociale, economica e politica dell'Europa dall'ICT, ma anche l'aumento costante del numero, della portata, della sofisticazione e dell'impatto potenziale delle minacce, non solo naturali ma anche quelle causate dall'uomo.

Come sottolinea la Commissione nell'ultima Comunicazione n. 163 del marzo 2011 negli ultimi anni sono andate emergendo minacce nuove e più sofisticate dal punto di vista tecnologico la cui dimensione geopolitica globale sta diventando sempre più chiara, delineandosi la tendenza ad utilizzare l'ICT per ottenere l'egemonia politica, economica e militare, anche avvalendosi delle capacità offensive. La "guerra informatica" o il "terrorismo informatico" sono, quindi evidenzia la Commissione, dimensioni che ormai si sovrappongono al *cyber crime*.

La Commissione fornisce anche una rappresentazione del quadro delle minacce informatiche che è utile riproporre e che individua le categorie seguenti :

- *minacce con finalità di sfruttamento*, come le "minacce persistenti avanzate"[21] a fini di spionaggio economico e politico (GhostNet[22], ad esempio), i furti di identità, i recenti attacchi contro il sistema di scambio dei diritti di emissioni[23] o contro sistemi informatici delle autorità pubbliche[24] o ancora più recentemente contro Sony;
- *minacce con finalità di perturbazione*, come attacchi di interruzione del servizio con origine da più fonti (*Distribution Denial of Service*) o lo spamming mediante *botnet*[25] (la rete *botnet* denominata *Conficker*[26] ha coinvolto tra il 2008 ed il 2009, 7 milioni di macchine mentre la rete *Mariposa* di origine spagnola ne ha coinvolte successivamente 12,7 milioni[27]);

21. Ossia, attacchi continui e coordinati contro le agenzie governative e il settore pubblico. Sta diventando un vero problema per il settore pubblico (vedi "RSA 2011 cybercrime trends report").

22. Vedi le relazioni nell'ambito del progetto "*Information Warfare Monitor: Tracking GhostNet: investigating a Cyber Espionage Network*" (2009) e "*Shadows in the Cloud: Investigating Cyber Espionage 2.0*" (2010).

23. Vedi domande e risposte su:

http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/11/34&format=HTML&aged=0&language=EN&guiLanguage=fr .

24. Ad esempio i recenti attacchi contro il governo francese.

25. Cfr nota 11.

26. Cfr. John Markoff. «Worm Infects Millions of Computers Worldwide». New York Times, 22 1 2009.

27. Vedi il progetto OCSE/IFP "*Future Global Shocks*", "*Reducing systemic cyber-security risks*", del 14 gennaio 2011 http://www.oecd.org/dataoecd/3/42/46894657.pdf.

- *minacce con finalità di distruzione*. Questo scenario non si è ancora concretizzato compiutamente ma, vista la diffusione sempre più ampia dell'ICT nelle infrastrutture critiche (reti elettriche e sistemi idrici intelligenti), non si può escludere per il futuro[28]. La recente minaccia del virus Stuxnet[29] per interferire e danneggiare centrali nucleari iraniane rappresenta una chiara anticipazione di un preoccupante quanto incombente rischio per i prossimi anni.

È utile per completare il quadro far riferimento ad una recente indagine svolta dall'*European Electronic Crime Task Force*[30] in cui si evidenziano e descrivono le principali minacce individuando:

Malware

Con il termine ***malware*** si indica, solitamente, un generico software realizzato per "accedere" ad un computer remoto senza il consenso dell'utilizzatore. Negli ultimi 3 anni (fig.3) la crescita dei *malware* ha assunto un andamento esponenziale caratterizzandosi per due principali finalità:

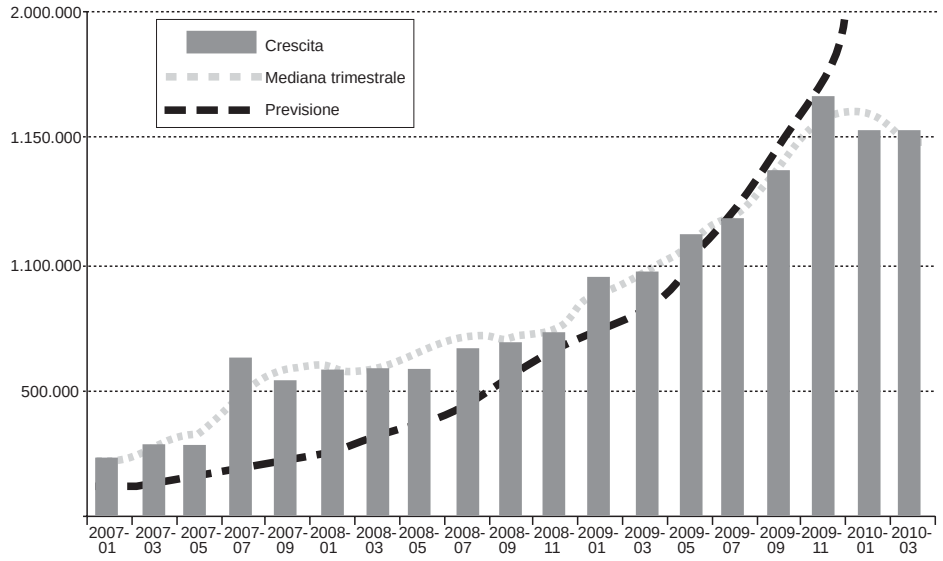
- furto di informazioni o credenziali dell'utilizzatore (home banking o e-commerce website); furto diretto di soldi (attraverso ad esempio i dialer); furto di documenti personali (direttamente dall'hard disk del computer);
- uso non autorizzato del computer infetto dell'utilizzatore che permette la fornitura di servizi illegali venduti al mercato nero, la generazione di traffico illegale, la distruzione di dati, il controllo remoto del computer.

28. Vedi World Economic Forum, Global Risks 2011.

29. Vedi http://www.enisa.europa.eu/media/press-releases/stuxnet-analysis .

30.Organismo istituito tra Poste Italiane e Polizia di Stato con la partecipazione del Governo Usa.

Fig. 3 - La crescita di Malware nel mondo. Anni 2007-2010 (v.a.)



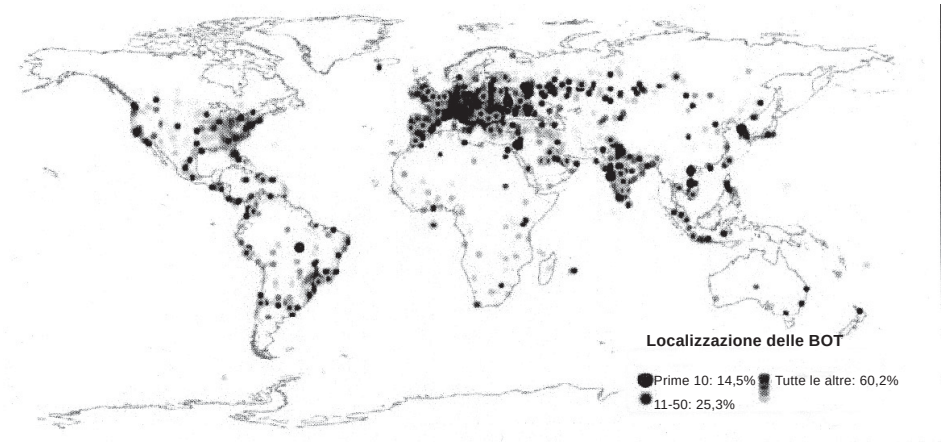
Fonte: 2011, EECTF European Cybercrime Survey

Botnets

La distribuzione geografica delle *botnet*, come si può osservare nelle figure 4 e 5 una alta concentrazione di computer "compromessi" in Europa. La maggioranza di questi, tuttavia, si concentra nell'Europa dell'Est. Il computer che contiene al suo interno una *botnet* può essere controllato da remoto via internet.

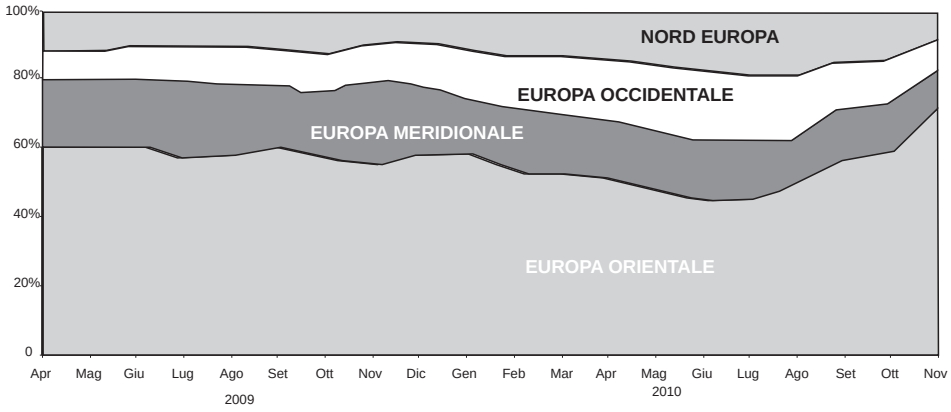
Gli *attacker* possono così portare avanti le loro azioni criminali direttamente da questi computer, senza che l'utilizzatore se ne possa rendere conto. Gli *attacker* ambiscono a "infettare" il maggior numero di computer possibili (che rappresentano un esercito di "bot") che possono poi affittare a terzi, traendone un profitto.

Fig. 4 - Distribuzione geografica delle Botnet a ottobre 2010, nel mondo (val.%)



Fonte: 2011, EECTF European Cybercrime Survey

Fig. 5 - Distribuzione delle Botnet in Europa, per area. Anni 2009-2010 (val.%)



Fonte: 2011, EECTF European Cybercrime Survey

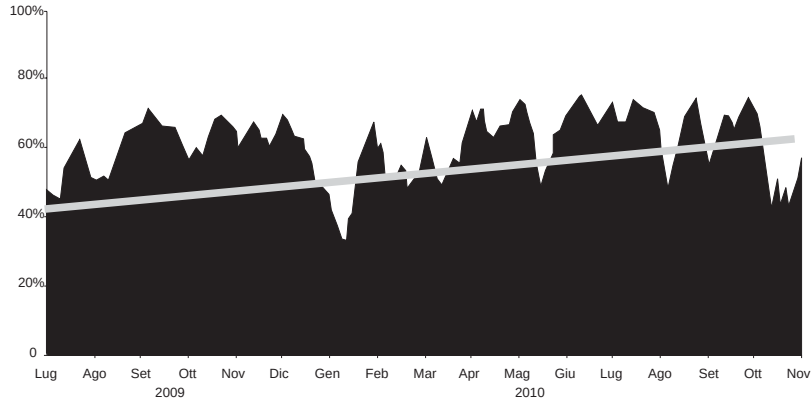
Spam

Spam significa la spedizione di grandi quantità di messaggi indesiderati, generalmente commerciali, soprattutto attraverso l'e-mail. Il fenomeno pur essendo molto fastidioso, non sarebbe troppo grave di per sé ma, purtroppo, è legato al cosiddetto *phising.* Le *botnet* hanno un ruolo fondamentale nell'invio di messaggi spam: secondo Symantec, durante il 2010, circa l'88% dei messaggi spam inviati è stato spedito da computer sotto controllo indiretto da parte di Botnet (fig.6).

Phising

Con il termine **Phising** si intendono tutti quegli strumenti attraverso i quali si cerca di persuadere gli utilizzatori nel comunicare i loro dati sensibili, quali ad esempio, dati dell'home banking, numeri delle carte di credito. Attacchi di questo tipo sono portati avanti attraverso l'invio di e-mail che possono sembrare "originali" ed inviate proprio dal fornitore di servizi (bancari, postali, commerciali) in cui si richiedono le credenziali

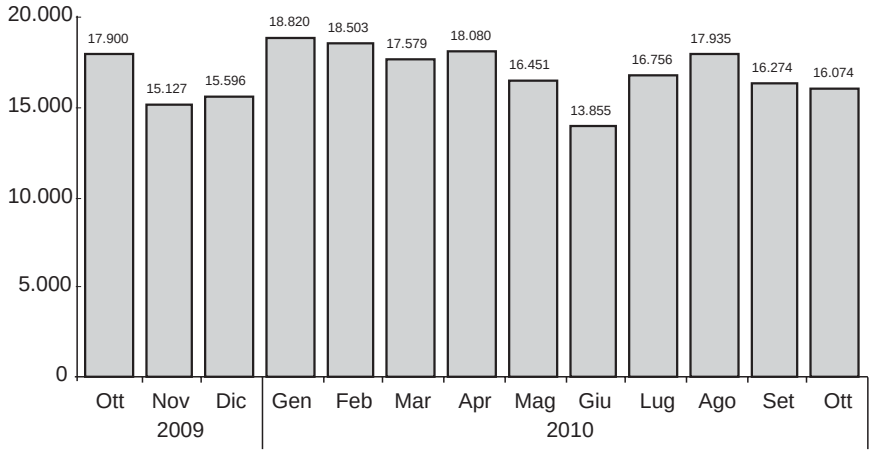
Fig. 6 - Quota di Spam inviato tramite Botnet sul totale dello Spam inviato. Anni 2009-2010 (val.%)



Fonte: 2011, EECTF European Cybercrime Survey

d'accesso ai servizi stessi. Durante il 2010, il numero di attacchi *phising* rilevati è rimasto elevato (compreso tra i circa 14 mila e i circa 19 mila al mese) (fig.7). A livello europeo, facendo riferimento a novembre 2010, l'Italia, insieme ai Paesi Bassi e al Regno Unito è tra i paesi che presentano il più alto numero di attacchi (tab.1).

Fig. 7 - Andamento delle "campagne" di Phising nel mondo. Anni 2009-2010 (v.a.)



Fonte: 2011, EECTF European Cybercrime Survey

Tab. 1 - Le "campagne" di Phising, in Europa a Novembre 2010 (v.a.)

Francia	23
Germania	3
Grecia	6
Irlanda	5
Italia	336
Olanda	207
Polonia	1
Romania	1
Spagna	86
Regno Unito	2.737
Totale	**3.405**

Fonte: 2011,EECTF European Cybercrime Survey.

Riassumendo, esistono "minacce persistenti avanzate" ossia attacchi continui contro agenzie governative e settore pubblico per spionaggio economico o politico (come *Ghostnet*). Oppure si può fare riferimento ai sempre più numerosi tentativi di furto di identità, soprattutto in ambito finanziario e bancario. O ancora, i cosiddetti *Ddos*, o interruzioni di servizio dei sistemi informatici pubblici o privati. Altre minacce derivano dallo *spamming*, o come il citato Stuxnet , da *malware* che compromettono il funzionamento di importanti sistemi di controllo industriale quali quelli delle centrali nucleari. Infine, potrebbero concretizzarsi nel futuro, minacce verso i sistemi informatici che governano le infrastrutture critiche (reti energetiche, di trasporto, *smart grid*) con il rischio di ingenti danni.

La recente comunicazione della commissione al Parlamento Europeo dal titolo *"The Eu internal security strategy in action. Five Steps towards a more secure Europe"*[31] elenca **cinque obiettivi** strategici per incrementare la sicurezza dei cittadini all'interno dell'Unione.

Uno di questi cinque obiettivi fa riferimento alla sicurezza del "Cyberspazio". Infatti, alle minacce derivanti dalle forme "classiche" di criminalità se ne affacciano altre, più recenti, di natura tecnologica, che nascono proprio come conseguenza dello sviluppo, sempre più repentino, della società dell'informazione.

Del resto, tutto il continente Europeo è un obiettivo centrale per i criminali informatici e questo per varie ragioni:

- l'uso, oramai, pervasivo che l'Europa fa delle infrastrutture internet e più in generale degli strumenti informatici;
- la sua economia *internet-mediated*;
- l'alto numero di utilizzatori della rete e i sistemi di pagamento sempre più "virtualizzati" e orientati verso sistemi elettronici.

31. Brussels, 22.11.2010 COM(2010) 673 final.

È in quest'ottica che risulta, quindi, necessario incrementare il livello di sicurezza nel Cyberspazio, per i **cittadini**, per le **imprese** e per le **infrastrutture**.

Sulla base di ciò, sono diverse le azioni intraprese (e da intraprendere) a livello europeo e nazionale che si diramano lungo 3 filoni principali.

Il primo è relativo all'esigenza di **aumentare la capacità investigativa e giudiziaria** degli Stati membri e il loro coordinamento.

Il secondo filone riguarda il **maggior coinvolgimento di cittadini e imprese nel prevenire e contrastare i crimini informatici**.

Il terzo è orientato ad **aumentare la capacità di contrastare gli attacchi informatici** da parte delle imprese private, da parte dei cittadini e da parte del settore pubblico.

Tutto ciò si può raggiungere con il contributo coordinato di tutti gli attori ed in un'ottica di prevenzione, preparazione, sensibilizzazione e definendo meccanismi coordinati di risposta ad un crimine informatico sempre in perenne e rapida evoluzione. È, inoltre, necessaria una risposta più possibile globale ad un problema globale. Infatti, vista l'interconnettività delle reti informatiche, un basso livello di sicurezza e resilienza in un paese potrebbe rendere più vulnerabile e aumentare i rischi in un altro paese.

È, poi, necessario considerare anche i problemi di ***governance*** del sistema che attualmente vede il forte coinvolgimento dei privati, dal momento che questi ultimi controllano un grande numero di reti e infrastrutture. Ma non sempre "il mercato" offre incentivi sufficienti ad investimenti nel settore sicurezza ad un livello almeno pari a quello richiesto dagli Stati.

Un ulteriore elemento di analisi è quello relativo alla **capacità di allarme e reazione in caso di incidenti**. Ma, ad oggi, tuttavia, i processi e i sistemi utilizzati per monitorare lo stato delle reti sono diversi da uno

Stato all'altro. Diversi Stati tra cui l'Italia (che pure come vedremo avanti presenta una nutrita schiera di organismi di analisi, controllo e difesa) non sono dotati di un unico punto di riferimento e monitoraggio nel caso di attacchi . E, inoltre, le reti di scambio di informazioni sono poco sviluppate e prevalentemente di natura informale e con dati non sempre affidabili.

4. Strategie nazionali per la sicurezza ICT

L'approccio nazionale in tema di sicurezza ICT negli ultimi anni, anche per effetto del grande impulso europeo in materia, ha visto un susseguirsi di strategie differenti per la sicurezza, non sempre coordinate tra loro, che hanno di volta in volta visto focalizzare l'attenzione su specifici aspetti: dalla Pa Digitale, alle Infrastrutture Critiche, dai Crimini informatici alla sicurezza delle ICT del sistema finanziaro, sino alla protezione dei dati personali, con una sostanziale difficoltà dei decisori politici a seguire un disegno strategico complessivo e unitario e con l'effetto di aver prodotto una ridondanza di strutture e soggetti.

4.1. La Pubblica Amministrazione

Anche in Italia la sicurezza informatica della PA da diversi anni rientra tra gli obiettivi generali del governo nazionale. Soffermandosi solo sulle norme e regole proposte a partire dal 2002 vale la pena segnalare la direttiva sulla sicurezza ICT, emanata dal Presidente del Consiglio dei Ministri il 16 gennaio 2002, che fissava i requisiti minimi da raggiungere per garantire al sicurezza e prevedeva la nascita del *Comitato Tecnico Nazionale sulla Sicurezza ICT*, cui era affidato il compito di raggiungere gli obiettivi di crescita della sicurezza elaborando e diffondendo linee guida

e fornitura di consulenza e supporto alla realizzazione. Il Comitato, istituito nel corso del 2002 non è più operativo dal 2006.

Nel 2008 il Governo ha istituito, poi, una *Unità di prevenzione degli incidenti informatici* del *Sistema Pubblico di Connettività* (SPC) insediandola presso DigitPA in ottemperanza all'articolo 21, comma 51.a del Decreto del Presidente del Consiglio dei Ministri del 01/04/2008. Tale struttura svolge il ruolo di *Computer Emergency Response Team* (CERT) presso il Sistema pubblico di connettività (SPC). Nello svolgimento di tali compiti, il CERT-SPC si pone quale struttura centrale del sistema e referente delle Unità Locali di Sicurezza (ULS), istituite una per ogni dominio connesso al SPC.

Al CERT SPC, che è referente nazionale per la prevenzione, il monitoraggio, il coordinamento informativo e l'analisi degli incidenti di sicurezza in ambito SPC, è attribuita anche la responsabilità di assicurare l'applicazione di metodologie coerenti ed uniformi in tutto il sistema, per la gestione degli incidenti informatici.

Il Sistema Pubblico di Connettività (SPC) è definito da DigitPa come *l'insieme di infrastrutture tecnologiche e di regole tecniche, per lo sviluppo, la condivisione, l'integrazione e la diffusione del patrimonio informativo e dei dati della pubblica amministrazione, necessarie per assicurare l'interoperabilità di base ed evoluta e la cooperazione applicativa dei sistemi informatici e dei flussi informativi, garantendo la sicurezza, la riservatezza delle informazioni, nonché la salvaguardia e l'autonomia del patrimonio informativo di ciascuna pubblica amministrazione.*

SPC si può quindi definire anche come un insieme d'infrastrutture e regole condivise ed è una ***"rete trusted"***. Ha, pertanto, una politica di sicurezza nota all'esterno e verificabile con processi di "*qualificazione o di monitoraggio*". Gli enti aderenti al SPC sono considerati "*degni di fiducia*" poiché **accettano**, **condividono** e **assicurano** l'attuazione di una serie di norme e prescrizioni, finalizzate a garantire la sicurezza e la stabilità dell'intero sistema.

L'insieme degli obblighi di sicurezza sono distribuiti nell'intero quadro dispositivo di riferimento e vincolano tutti i membri della SPC a **mantenere affidabile il sistema.**

SPC è, quindi, ricapitolando, un sistema dove:

1) la salvaguardia delle informazioni avviene nel rispetto dell'autonomia del patrimonio informativo delle singole Amministrazioni;
2) sono individuate le responsabilità e le competenza di ciascun soggetto che partecipa all'SPC;
3) tutte le amministrazioni condividono e si impegnano reciprocamente ad adottare le misure minime (definite all'interno di SPC), per garantire i livelli di sicurezza necessari all'intero sistema.

Le regole di sicurezza di SPC fanno riferimento allo standard internazionale ISO 27000, che prevede l'adozione di determinate misure di sicurezza per mitigare il rischio.

In quest'ambito vi è la necessità di consolidare l'integrazione tra il centro (CERT-SPC)[32] e le strutture locali della PA (Unità Locali Sicurezza–ULS), che hanno il compito di prevenire e gestire eventuali incidenti che si dovessero verificare sui loro sistemi interni.

32. Il CERT-SPC deve:
- *dotarsi di una rete informativa, finalizzata alla raccolta di dati e informazioni per il coordinamento di tutte le unità;*
- *utilizzare strumenti adeguati per l'analisi delle vulnerabilità e per osservare i comportamenti "ostili";*
- *realizzare un sistema di comunicazione, mediante avvisi e segnalazioni delle emergenze, indirizzato alle strutture di gestione operativa dei sistemi informatici;*
- *impiegare procedure standardizzate di reazione e coordinamento nel caso di incidenti informatici;*
- *interagire con gli interlocutori esterni sulla base delle indicazioni e dei dati ottenuti dalle analisi;*
- *migliorare i meccanismi e le misure di protezione sulla base dell'analisi degli incidenti avvenuti.*

La sicurezza in ambito PA digitale è poi governata dal Codice della Amministrazione Digitale (CAD). Il Codice con l'approvazione del decreto legislativo del 30 dicembre 2010, n. 235 ("Modifiche ed integrazioni al decreto legislativo 7 marzo 2005, n. 82 - Codice dell'Amministrazione Digitale) è stato aggiornato soprattutto per la parte che disciplina dei rapporti tra Stato, Enti locali, cittadini ed imprese che utilizzino le nuove tecnologie, quale modalità di interazione reciproca, con l'obiettivo di migliorare l'efficienza e l'efficacia dell'azione amministrativa delle singole PA e della macchina dello Stato nel suo complesso.

Gli aspetti di sicurezza sono stati ribaditi nella consapevolezza del ruolo trasversale che la materia riveste lungo tutto l'articolato del Codice.

Nello specifico, è previsto (art.12) tra l'altro che "*Le pubbliche amministrazioni adottano le tecnologie dell'informazione e della comunicazione nei rapporti interni, tra le diverse amministrazioni e tra queste e i privati, con misure informatiche, tecnologiche, e procedurali di sicurezza, secondo le regole tecniche di cui all'articolo 71"*.

È inoltre previsto che le **regole tecniche**[33] (art. 71) individueranno *"le modalità che garantiscono l'esattezza, la disponibilità, l'accessibilità, l'integrità e la riservatezza dei dati, dei sistemi e delle infrastrutture "* (art.51). A tal proposito, è stata recentemente firmata a Roma, una Convenzione tra il Consiglio nazionale degli Ingegneri, la Fondazione Ugo Bordoni e DigitPa per la realizzazione di un progetto denominato Italia Sicur@. Il progetto Italia Sicur@ ha l'obiettivo di realizzare un programma di formazione sulla sicurezza informatica cui destinare gli ingegneri iscritti al CNI, per specializzarne le professionalità sulle tematiche di sicurezza. L'iniziativa è stata avviata dal CNI e dalla Fondazione Ugo Bordoni con la partecipazione di DigitPA e, in particolare, fa riferimento a tutte quelle realtà meno "aggiornate" a livello

33. A luglio 2011 ancora in corso di definizione.

tecnologico. Obiettivo è quindi, da un lato, quello di facilitare l'utilizzo di nuove tecnologie, dall'altro accrescere la consapevolezza nell'adozione di misure e politiche di sicurezza ICT, coerenti con il modello di sicurezza adottato nel Sistema Pubblico di Connettività (SPC). L'azione dovrà inoltre fornire elementi conoscitivi finalizzati alla messa punto delle regole della sicurezza previste dal citato art. 71 del CAD.

4.2. Le infrastrutture critiche informatizzate

Con il Decreto del Ministro dell'Interno del 9 gennaio 2008 (GURI n. 101 del 30 aprile 2008) il nostro paese, anticipando la direttiva europea, ha provveduto ad individuare le infrastrutture critiche informatizzate di interesse nazionale, annoverando tra di esse i sistemi ed i servizi informatici di supporto alle funzioni istituzionali di 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, nonché le infrastrutture di *utility* pubbliche che operano su aree metropolitane non inferiori a 500.000 abitanti (comunicazioni, dei trasporti, dell'energia, della salute e delle acque) e infine i sistemi Informatici della Banca d'Italia.

Questa disposizione, in realtà, come è stato fatto osservare da alcuni interlocutori istituzionali *ha risentito di una quadro complessivo di "incompletezza normativa" in materia di protezione delle Infrastrutture Critiche Nazionali (ICN) non esistendo all'epoca della sua emanazione, appunto, una disciplina specifica proprio per l'individuazione e designazione delle ICN stesse.*

Per delineare un primo quadro organico di intervento occorre allora arrivare al 7 aprile 2011, quando la Presidenza del Consiglio ha approvato il decreto legislativo che recepisce la Direttiva europea 2008/114/CE, e

in cui si individua la ***"Struttura Responsabile"*** *che diviene* ***"il Punto di Contatto nazionale"*** all'interno della stessa ***Presidenza del Consiglio*** per "*le attività tecniche e scientifiche riguardanti l'individuazione delle ICE (Infrastrutture Critiche Europee) e per ogni altra attività connessa"* e per tenere i rapporti con la Commissione europea e con le analoghe strutture degli altri Stati membri dell'Unione Europea.

Il Decreto fa nascere, poi, *il* ***Nucleo Interministeriale Situazione e Pianificazione*** *che "determina, in linea di massima, i limiti dei criteri di valutazione intersettoriale, oltre i quali l'infrastruttura è definita potenzialmente critica".*

La norma pubblicata in Gazzetta Ufficiale lo scorso 5 maggio nasce quindi per recepire la direttiva europea sulle ICN e si pone l'obiettivo di potenziare la sicurezza delle grandi infrastrutture energetiche e dei trasporti del Paese nei confronti di azioni terroristiche o criminali, ma anche aumentarne la robustezza rispetto a guasti accidentali ed eventi naturali. L'entrata in vigore della Direttiva in Italia è avvenuta però a soli otto giorni dalla conferenza della Commissione Europea convocata per avviare la revisione della Direttiva stessa.

In base alla Direttiva, ogni azienda "critica" dovrà avere un responsabile della sicurezza unico, che fungerà da punto di contatto per tutte le problematiche di sicurezza, e di un "*Piano della Sicurezza dell'Operatore*", che dovrà contenere una dettagliata analisi delle diverse minacce, vulnerabilità e, soprattutto, delle varie contromisure da adottare in funzione delle specifiche situazioni di rischio. Piano che dovrà poi essere validato e approvato dalle autorità pubbliche: la direttiva e la norma che la recepisce stabilisce che tutti gli oneri sono posti direttamente a carico delle aziende, e vi è quindi il rischio che questi siano in definitiva ribaltati sull'utenza con conseguenti incrementi tariffari.

La nuova revisione Ue della Direttiva porterà ad includere le infrastrutture ICT tra quelle critiche europee, in aggiunta alle attuali energetiche

e dei trasporti. In vista di questo occorrerà promuovere progetti e attività specifiche per sviluppare criteri che meglio identifichino la criticità delle infrastrutture ICT.

Al di là del ritardo nel recepimento, va considerato che sul sistema di governo delle infrastrutture critiche pesa anche il rischio di una certa ridondanza normativa e di indirizzi con possibili sovrapposizioni di ruoli. Rischio che si amplierà nel momento in cui ci si andrà ad occupare di *Infrastrutture critiche informatizzate*.

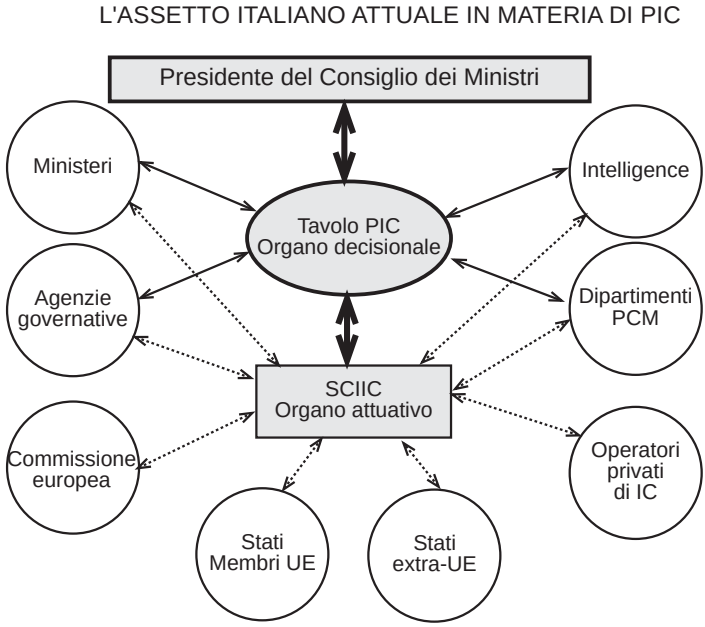
Già nel 2006 infatti il consigliere militare della Presidenza del Consiglio dei Ministri ha avviato il "*Tavolo per la Protezione delle Infrastrutture Critiche* – Tavolo PIC" al quale partecipano i dicasteri e le istituzioni interessate alla protezione delle Infrastrutture Critiche.

Il Tavolo PIC coordina le attività nazionali e definisce la posizione nazionale in sede internazionale. Più dettagliatamente :

- definisce i criteri per l'identificazione delle Infrastrutture Critiche (…);
- sviluppa una lista unica delle infrastrutture critiche individuate (con la loro priorità) da ciascun Ministero/Autorità competente;
- coordina le attività per gli adempimenti della Direttiva 114/08 CE e per la identificazione delle IC Europee;
- studia eventuali misure di protezione delle Infrastrutture Critiche ulteriori rispetto a quelle in atto riguardanti le infrastrutture critiche, alle dipendenze funzionali del Consigliere militare del Presidente del Consiglio dei Ministri.

Sulla base degli accordi interministeriali e sull'Ordinanza del Presidente del Consiglio n. 3836 del 2009, l'assetto istituzionale per la protezione delle *Infrastrutture Critiche* si può riassumere nello schema seguente (fig. 8).

Fig. 8 - La *governance* in Italia delle infrastrutture critiche



Fonte: *Infrastrutture critiche: lo Stato dell'Arte* di Luisa Franchina, Marco Carbonelli, Laura Gratta, Maria Crisci, atti del convegno Icsa del 5 maggio 2010, Roma.

4.3. Lotta ai Crimini informatici in Italia

Sulla scia degli attentati terroristici di Madrid e Londra, dell'agosto 2005, il Parlamento ha votato la legge 31 luglio 2005 n. 155, di conversione, del decreto-legge 27 luglio 2005, n. 144, recante *"misure urgenti per il contrasto del terrorismo internazionale,"* finalizzata ad un miglior coordinamento tra i diversi organi di sicurezza. Nel provvedimento, all'articolo 7-*bis* (sicurezza telematica), si definisce, per la prima volta, un quadro normativo per la protezione delle «*infrastrutture critiche nazionali*» dagli attacchi informatici rimandando ad un successivo decreto del Ministero dell'Interno la definizione delle specifiche infrastrutture.

Solo nel 2008 con Decreto del 9 gennaio 2008 il Ministro dell'Interno ha provveduto all'art.1 all'Individuazione delle infrastrutture critiche informatiche di interesse nazionale elencando in particolare le infrastrutture ICT di:

a) 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;
b) Banca d'Italia ed autorità indipendenti;
c) società partecipate dallo Stato, dalle regioni e dai comuni interessanti aree metropolitane non inferiori a 500.000 abitanti, operanti nei settori delle comunicazioni, dei trasporti, dell'energia, della salute e delle acque;
d) ogni altra istituzione, amministrazione, ente, persona giuridica pubblica o privata la cui attività, per ragioni di tutela dell'ordine e della sicurezza pubblica, sia riconosciuta di interesse nazionale dal Ministro dell'interno, anche su proposta dei prefetti autorità provinciali di pubblica sicurezza e protezione civile (forze dell'ordine, forze armate);
e) reti a supporto delle istituzioni e degli organi costituzionali;
f) servizi particolari forniti da alcuni enti ed aziende strategiche.

Un'ulteriore tappa importante della costruzione normativa sulla lotta al crimine informatico è la ratifica della Convenzione del Consiglio d'Europa sul *Cybercrime*, firmata a Budapest il 23 novembre 2001, avvenuta con la legge 18 marzo 2008, n. 48. Attualmente, aderiscono alla Convezione 29 paesi e non tutti appartenenti al Consiglio d'Europa, e tra cui spiccano gli Stati Uniti.

La legge di ratifica ha modificato, allineandole con quelle degli altri Paesi aderenti alla Convenzione, le norme esistenti nell'ordinamento ita-

liano in ambito *cyber-crime*. Ad esempio, sul piano della collaborazione giudiziaria, al fine di rendere veloce lo scambio di dati investigativi durante le indagini sui crimini informatici, la Convenzione prevede, su richiesta dello Stato che procede all'indagine, il "congelamento", per un periodo di tre mesi, dei dati informatici eventualmente in possesso di altri Stati. Le richieste devono transitare attraverso il *network* dei rispettivi «punti di contatto» nazionali. E con un decreto interministeriale dei Ministri dell'Interno e della Giustizia del 24 novembre 2009, si definisce la **Polizia postale come punto di contatto nazionale all'interno della rete di cooperazione dei Paesi**.

Il primo presidio di lotta contro i crimini informatici è, quindi, la Polizia postale.

Ad essa viene, quindi, demandata:

- la sicurezza delle infrastrutture informatiche, incluse quelle definite critiche;
- la prevenzione e il contrasto degli attacchi di livello informatico;
- la regolarità dei servizi di telecomunicazione;
- il contrasto della pedopornografia *online*;
- la lotta agli illeciti nei mezzi di pagamento delle attività di commercio elettronico e nella violazione del diritto d'autore.

Nell'ambito della lotta al *cyber-crime* e della protezione delle infrastrutture critiche, è da segnalare nel giugno 2009 l'attivazione del *Centro nazionale anticrimine informatico per la protezione delle infrastrutture critiche* (CNAIPIC), previsto dal decreto del Capo della Polizia del 7 agosto 2008.

La struttura, già prevista all'interno della direttiva europea sulla protezione delle infrastrutture critiche del 2008, ha al suo interno personale specializzato con funzioni operative e tecniche della Polizia postale e si raccorda con gli operatori di infrastrutture critiche informatiche identificati nel decreto del Ministero dell'interno del 9 gennaio 2008.

Al fine di facilitare il dialogo con gli operatori privati, la Polizia di Stato ha sottoscritto diverse convenzioni triennali con organizzazioni private (Consob, RAI, ACI, Ferrovie dello Stato, Vodafone, Telecom e Unicredit). È stata, poi, istituita una segreteria tecnica per facilitare il coordinamento interministeriale delle attività nazionali, anche in ambito internazionale, su questioni relative alle infrastrutture critiche comprese quelle di natura informatica.

Il Paese si sta quindi dotando di alcuni strumenti operativi per la lotta al *cyber-crime* e, soprattutto su impulso di iniziative internazionali e comunitarie, sta tentando di definire un approccio coordinato alla protezione delle infrastrutture critiche, comprese quelle di natura informatica.

Le infrastrutture informatiche sono sempre più interdipendenti. Quindi oltre alla gestione e repressione nei casi di attacchi informatici, è necessario disporre di idonei strumenti per la prevenzione. In Italia in questo ambito sono, attualmente operativi:

- il «Commissariato online»: dedicato a segnalare reati o comportamenti anomali, rilevati durante la navigazione, o per la richiesta di informazioni;
- il «Centro Nazionale per il Contrasto alla Pedopornografia *online*» – CNCPO: previsto dalla legge 38 del 2006 inaugurato il 10 febbraio 2008;
- il già citato «Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche» (CNAIPIC), istituito in attuazione dell'articolo 7-*bis* della legge 155 del 2005 e inaugurato il 23 giugno 2009. Si tratta di una sala operativa, disponibile 24 ore al giorno, 7 giorni su 7. È un servizio per la prevenzione e la repressione di minacce criminali o terroristiche che arrivano dalla rete, dedicato a mantenere l'integrità e il funzionamento delle infrastrutture;

- il «Nucleo Speciale Frodi Telematiche» della Guardia di Finanza: istituito nel 2001, è specializzato nel contrasto alle frodi informatiche.

In un fenomeno complesso come quello che riguarda la sicurezza informatica, la collaborazione tra pubblico e privato è essenziale e risulta parte integrante della strategia nazionale. Sono, infatti, numerosi gli accordi che vedono lavorare insieme università, enti di ricerca, pubblica amministrazione e forze di polizia.

A questo proposito la cosiddetta attività di *informatica forense*[34] è uno dei più importanti strumenti investigativi nel contrasto del *cyber-crime* e attualmente è un settore centrale all'interno della Polizia delle comunicazioni. Inoltre, esistono numerosi «Protocolli d'Intesa» con le principali università italiane per la formazione del personale di polizia, ma anche degli studenti attraverso *master* universitari in sicurezza informatica.

Da ultimo, per fronteggiare in maniera più decisa il rischio di frodi finanziarie in rete, è stata costituita, nel giugno 2009, una struttura composta dalla Polizia postale, da Secret Service, agenzia di *law enforcement* statunitense – e da Poste Italiane. Il gruppo chiamato «*European Electronic CrimeTask Force*» è finalizzato al contrasto del *cyber-crime*, ed è aperto anche ad altre organizzazioni pubbliche e private con interessi comuni.

Sempre Poste Italiane ha, poi, costituito il "Centro di Eccellenza Nazionale sulla cyber security (CENSec)", con la finalità di "farsi catalizzatore della cultura nazionale sulla sicurezza informatica; di identificare e diffondere le soluzioni di contrasto alla minaccia; di contribuire allo svilup-

34. **L'informatica forense** (computer *forensics*) studia le diverse forme di trattamento del dato informatico (conservazione, protezione, estrazione, ecc.) ai fini una loro valutazione processuale. La disciplina studia ai fini probatori, le tecniche e gli strumenti per l'esame metodologico dei sistemi informatici.

po di nuove soluzioni organizzative, procedurali, tecnologiche e di regolamentazione"[35].

Nel 2003, inoltre, è stato elaborato un progetto di collaborazione per la prevenzione e il contrasto agli accessi illeciti e ai tentativi di accesso ai sistemi di gestione della sicurezza della circolazione ferroviaria. Progetto che ha portato, in data 15 luglio 2003, alla stipula di una "*Convenzione per la prevenzione dei crimini informatici sui sistemi di gestione della sicurezza della circolazione ferroviaria utilizzati dalla Rete Ferroviaria Italiana Spa*". A seguito della costituzione del CNAIPIC, la Convenzione consente la condivisione e l'analisi di informazioni utili alla prevenzione della minaccia; la segnalazione di emergenze relative a vulnerabilità, minacce e incidenti; l'identificazione dell'origine tecnica degli attacchi contro l'infrastruttura ferroviaria e le altre infrastrutture critiche; la realizzazione e la gestione di attività di comunicazione per fronteggiare situazioni di crisi o di emergenza. Inoltre, dato il carattere globale dei crimini informatici – la Polizia postale fa parte di diverse reti di cooperazione internazionale, per aumentare l'efficacia dei normali canali di cooperazione giudiziaria e investigativa. Esiste a tal proposito una **rete dei punti di contatto** che, ad oggi, conta sulla partecipazione di uffici specializzati in 56 Paesi.

4.4. Il sistema finanziario nazionale

Un'ulteriore area di criticità riguarda il sistema finanziario nazionale. Che se attaccato, può portare al blocco dei sistemi di pagamento e/o

35. Comitato Parlamentare sulla sicurezza della Repubblica ; " Relazione sulle possibili minacce per la scurezza nazionale derivanti dall'utilizzo dello spazio cibernetico. " Camera dei deputati, 7 Luglio 2010.

dell'accesso ai mercati finanziari, sino ad arrivare a incidere sul funzionamento dell'intera piazza finanziaria nazionale. E determinare gravissime ripercussioni soprattutto sul livello di fiducia che i cittadini nutrono verso questi avanzati sistemi di pagamento.

In sostanza, si tratta della protezione di tutte quelle attività di regolamento interbancario, compensazione, garanzia e liquidazione degli strumenti finanziari, servizi per l'accesso ai mercati, ed erogazione di denaro agli utenti.

Dal 2004 la Banca d'Italia ha emanato la Normativa di Vigilanza "*Continuità operativa in casi di emergenza"*, che impone alle 800 banche italiane di dotarsi di un Piano di Continuità Operativa (*Business Continuity Plan)*. Come previsto dalla Banca Centrale Europea, nel 2007 la Banca d'Italia ha emanato le disposizioni per la continuità operativa degli operatori finanziari in caso di attacco informatico. Il tavolo CODISE[36](Continuità Di Servizio), coordinato dalla Banca d'Italia d'intesa con la CONSOB, al quale partecipano i principali gruppi bancari e le società che gestiscono le infrastrutture di sistema rilevanti per l'ordinato funzionamento del sistema finanziario, rappresenta il principale punto di incontro istituzionale per la definizione di iniziative per la protezione delle infrastrutture di rete di interesse nazionale.

Le disposizioni della Banca d'Italia richiedono che le banche o gli istituti finanziari nominino un responsabile per la gestione dei piani di continuità operativa e definiscano gli "scenari di rischio" rilevanti per la continuità operativa dei processi a rilevanza sistemica, inclusi quelli di attacco informatico, che devono essere documentati e costantemente aggiornati[37]. Sempre le stesse disposi-

36. http://www.bancaditalia.it/sispaga/codise

37. Banca d'Italia - Disposizioni di vigilanza - Requisiti particolari per la continuità operativa dei processi a rilevanza sistemica Marzo 2007.

zioni prevedono che gli istituti finanziari si dotino di siti di *recovery* per la gestione di questi processi, situati ad una certa distanza dai siti primari in modo da garantire un certo livello di indipendenza.

Per ridurre al minimo i disagi, le disposizioni prevedono anche la definizione dei tempi di ripristino, in caso di attacco, che devono essere contenuti nelle quattro ore. Gli istituti finanziari infine, devono effettuare, con frequenza almeno annuale, verifiche ai propri sistemi e devono partecipare attivamente ai test di sistema organizzati dalle autorità, dai mercati o da altre organizzazioni finanziarie.

In questo ambito si può segnalare l'attività dell'ABI LAB, struttura localizzata all'interno dell'Associazione Bancaria Italiana, che si occupa di definire e di sviluppare *best practices* di sicurezza informatica e continuità operativa.

Secondo gli ultimi dati usano l'*internet banking* in Italia circa 13 milioni di persone, e sono numeri in crescita costante. Perciò sulla base di questa consistenza risulta particolarmente pericoloso il furto d'identità, che avviene essenzialmente attraverso due strumenti: il *phishing* e il *crimeware*[38]. E, quello dei tentativi di furto di identità è un fenomeno particolarmente diffuso che tutti noi abbiamo sperimentato. Una recente indagine proprio a cura dell'Abi, conferma questa percezione. Secondo una indagine di Abi Lab, infatti, nel 2009 l'89% delle banche intervistate, ha dichiarato di aver avuto tentativi di furto delle credenziali di autenticazione all'*home banking*. Nel 37,9% degli attacchi subiti si tratta di *phishing*, nel 47,5% di *crimeware*; mentre nel 14,6% dei casi non è stato possibile determinare la causa di perdita delle credenziali da parte dei clienti.

38. Crimeware è una tipologia di malware sviluppata specificamente per automatizzare azioni di Cybercrime.

Nel prendere atto che quello bancario è tra i sistemi più passibile di infiltrazioni delle reti criminali informatiche, esistono diverse sedi di cooperazione internazionale finalizzate a contrastare il fenomeno.

Tra le altre si possono segnalare:

- *IT Fraud Working Group* (Federazione Bancaria Europea): gruppo di lavoro per lo scambio di informazioni sul fenomeno delle frodi informatiche;
- FI-ISAC: gruppo di lavoro dell'ENISA dedicato alle istituzioni finanziarie;
- CISEG (*Cybercrime Information Sharing Expert Group)* con l'obiettivo di favorire lo scambio di informazioni rilevanti per il fenomeno del crimine informatico.

Esistono inoltre numerosi gruppi tecnici di lavoro nelle sedi internazionali preposte alla vigilanza del sistema bancario e finanziario.

4.5. La protezione e la riservatezza dei dati

In un economia dal carattere prevalentemente immateriale, la protezione dell'informazione e la *privacy* dei dati è un altro aspetto fondamentale nella gestione delle organizzazioni di cui bisogna tenere conto.

A tal proposito, risulta centrale il ruolo dell'Autorità Garante per la protezione dei dati personali, che verifica presso privati, enti pubblici o imprese, l'attuazione delle misure tecnico-organizzative indicate nel **Codice per la protezione dei dati personali**.

Il Codice, indica al Titolo II le regole generali per il trattamento dei dati, prevede poi al Titolo IV, le responsabilità per i soggetti titolari del trattamento dei dati e disciplina, infine al Titolo V gli obblighi di sicurezza nella gestione dei dati.

L'attività svolta dal Garante presso le infrastrutture critiche si concretizza negli accertamenti ispettivi (artt. 157 e 158 del Codice) che possono portare a redigere provvedimenti *per adeguare o migliorare le misure di sicurezza e protezione dei dati e dei sistemi fisici o logici che li custodiscono o li trattano*. O a redigere documenti di carattere generale indirizzati alla tutela dei sistemi informatici delle infrastrutture critiche.

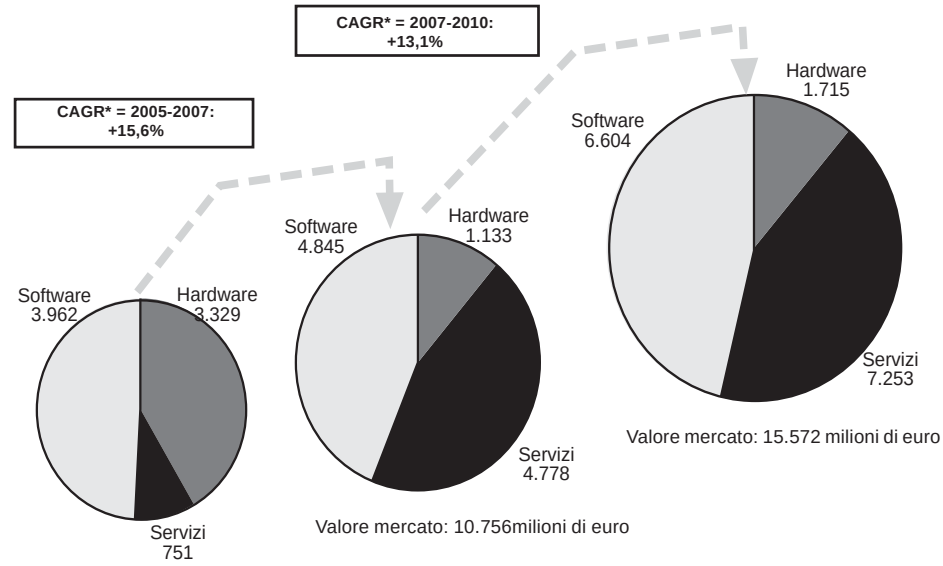
5. Il mercato della sicurezza delle reti e dei sistemi informativi

Il mercato europeo della sicurezza delle reti e dei sistemi informativi, nonostante la crisi economico-finanziaria che ha continuato a produrre effetti almeno sino al primo semestre del 2010 in tutti i paesi europei , alla fine dello scorso anno ha raggiunto i 15,5 miliardi di euro, con una crescita media dal 2007, del 13,1% annuo (fig.9) Il dato, in assoluta controtendenza rispetto all'economia europea in generale, ma anche rispetto agli altri ambiti dell'ICT, evidenzia la significatività del tema sicurezza.

Il mercato Europeo della sicurezza sui network e sui sistemi Informativi (NIS) oltre ad essere molto dinamico rispetto ai volumi di spesa, evidenzia anche un elevata evoluzione e progressiva ricomposizione dei segmenti di mercato: da una prevalenza di spese per software si è passati in pochi anni ad una prevalenza di spese per servizi, ad indicare una maturazione di questo segmento di mercato e un approccio più sofisticato al tema. La quota dei servizi informatici per la sicurezza nel 2010, secondo le stime IDC, avrebbe così raggiunto il 47% del totale delle spese in tecnologie dell'informazione in sicurezza, per un totale complessivo continentale pari a 7,2 miliardi di euro, a fonte di quote per spese di hardware pari a 1,7 miliardi (11%) e per il software pari a 6,6 miliardi (42%).

La dinamica di mercato che spinge sempre più verso lo sviluppo di servizi articolati e complessi, scaturisce dalla crescente sofisticazione e diffusione dei problemi, come pure dalla consapevolezza che lo sviluppo

Fig. 9 - La crescita del mercato Europeo della sicurezza Informatica (hardware, servizi, software). Anni 2005, 2007, 2010 (v.a. in milioni di euro)



*CAGR = Tasso Annuo di crescita composto.
Fonte: The European Network Information security market IDC 2010.

ed il mantenimento di una sicurezza effettiva non è più garantita da certificazioni di prodotto, che hanno una valenza ed una effettività limitata e ciò a maggior ragione anche a fronte della continua evoluzione dei rischi, soprattutto derivanti da comportamenti volontari e azioni fraudolente. Nella stessa direzione, verso, cioè, un ruolo sempre più importante dei servizi e della consulenza, agisce anche la crescente regolazione pubblica che impone strategie e modalità complesse per aderire alle prescrizioni normative.

Questi fattori spostano la domanda di servizi informatici, dal software standard, via via al servizio personalizzato e complesso, mentre aumenta anche l'attrattività dell'outsourcing, anche a seguito di più attente valutazioni dei costi complessivi e di una più esatta valutazione del rischio.

5.1. Il caso italiano

Sulle dinamiche e sui volumi di spesa per la sicurezza dei sistemi informatici nazionali, pesa il ritardo strutturale che limita lo sviluppo di un mercato nazionale dei sistemi ICT in generale.

Nel nostro paese, infatti, si registra un deficit complessivo di investimenti e spese per l'informatica che è ben evidenziato, sia dal dato che riguarda le spese pro capite, sia dalla spesa informatica in % sul Prodotto Interno Lordo (tab.2). In entrambi i casi, i valori nazionali non solo sono al di sotto della media dell'Europa a 15 ovvero della media del gruppo storico e più evoluto di Stati membri, ma anche sotto la media generale europea che comprende anche i paesi di nuovo ingresso provenienti dall'Est Europa.

In un quadro di spesa relativamente contenuto, rispetto al resto dei grandi paesi europei, le dinamiche di mercato generali evidenziano un quadro di spesa in prodotti e servizi informatici sempre più orientato verso i servizi, replicando anche nel nostro paese la tendenza generale europea (tab. 3).

Sebbene il quadro tendenziale evidenzi dunque sia i tratti di un sistema delle tecnologie dell'informazione maturo sia aspetti di arretratezza sistemica, è bene considerare come in realtà pesino ancora fortemente sulla domanda di nuovi servizi ad elevata prestazione professionale, tutti i limiti strutturali che condizionano lo sviluppo dell'informatica in Italia: dalla ridotta alfabetizzazione informatica a dei cittadini, all'arretratezza del sistema della Pa, sino alla polverizzazione del tessuto produttivo. Fattori che necessariamente condizionano il livello e la qualità della domanda di servizi ICT.

La tabella che segue riassume il quadro del deficit che complessivamente penalizza il sistema paese rispetto alla media europea (tab.4).

Tab. 2 - Spesa in informatica Pro capite e incidenza sul Pil (v.a in euro e val.%). Anno 2008

	Spese It Pro capite (euro)	Spesa It % PIL
Danimarca	1.309	3,20
Svezia	1.277	3,75
UK	1.104	3,52
Olanda	1.072	3,32
Finlandia	1.022	3,20
Francia	913	3,08
Austria	847	2,76
Belgio	843	2,98
Germania	819	2,91
Eu 15	**770**	**2,72**
Irlanda	659	1,51
Eu	**635**	**2,71**
Italia	**437**	**1,71**
Spagna	345	1,40
Slovenia	314	3,18
Repubblica ceca	285	3,20
Portogallo	272	1,81
Ungheria	203	2,49
Grecia	199	1,09
Estonia	181	2,86
Slovacchia	166	2,48
Polonia	139	2,58
Lettonia	113	2,34
Lituania	96	1,76
Bulgaria	58	1,95
Romania	54	2,13

Fonte: EITO, 2009

Tab. 3 - Valore del mercato del software e servizi (per componenti). Anno 2010 e previsioni 2011 (v.a. in migliaia di euro)

	2010	2011 (Previsioni)
Software	4.268	4.336
di cui		
Applicativo	2.584	-
Middleware	1.091	-
Software di sistema	593	-
Servizi		
di cui	8.432	8.480
Sistemi *embedded*	982	-
Servizi di elaborazione	759	-
Formazione	447	-
System integration	963	-
Outsourcing	2.507	-
Consulenza	920	-
Sviluppo e manutenzione	1.854	-
Totale	12.700	12.816

Fonte : Assinform 2011

Tab. 4 - Lo stato della "Società digitale" in Italia e confronto con la media europea a 27 paesi. Anno 2011. (val.%)

	Europa (27)	Italia
Pmi che vendono online	13,4	3,8
Imprese che acquistano online	26,4	16,5
Popolazione che usa frequentemente Internet	53,1	45,7
popolazione che usa servizi di online banking	36,0	17,6
cittadini che usano servizi di eGover*n*ment	31,7	17,4
famiglie con accesso a banda larga	60,8	48,9
famiglie con accesso a Internet	70,1	59,0
Popolazione che acquista online	40,4	14,7
Fatturato imprese attraverso *eCommerce*	13,9	5,4

Fonte: EC, Digital Agenda Scoreboard (maggio 2011)

In questo scenario nazionale ancora una volta dunque l'apporto degli ingegneri rispetto al contributo di cultura tecnica, professionalità e responsabilità che essi detengono, può essere decisivo per contribuire a diffondere la consapevolezza di come l'ICT sicuro e di qualità possa aiutare le imprese e le istituzioni ad affrontare le sfide del mondo attuale e le competizioni future.

6. Le prospettive per gli ingegneri dell'informazione

Per contrastare le frodi informatiche e gli attacchi esterni ai sistemi ICT ed in particolare alle infrastrutture critiche informatizzate nonché per contenere i rischi da eventi incidentali, le istituzioni europee ed i singoli Stati hanno avviato un profondo processo di aggiornamento e revisione del sistema di norme e regole sui crimini informatici e sulla *governance* della sicurezza ICT ampliando le funzioni e le istituzioni preposte al suo controllo.

È evidente, tuttavia, che per rendere le reti ed i sistemi ICT più sicuri, accanto ad un nuovo sistema di regole e nuovi assetti di *governance*, occorra tuttavia anche innalzare e rafforzare il ruolo ed il contributo degli specialisti nelle tecnologie dell'informazione e della comunicazione, chiamati a progettare e realizzare quegli stessi sistemi ICT da difendere e quelle infrastrutture di comunicazione e informatiche considerate strategiche e/o critiche.

Le istituzioni ed i decisori pubblici come pure i manager di imprese private a partire da quelli assoggettati a controllo pubblico sulla sicurezza ICT, devono perciò necessariamente preoccuparsi di individuare e identificare fornitori di servizi in grado di offrire un adeguato apporto professionale, e di dotarsi di personale interno qualificato per garantire la stabilità, la resilienza e in generale sicurezza dei sistemi ICT e dei servizi veicolati da tecnologie dell'informazione e della comunicazione.

Per affrontare e minimizzare i rischi migliorando la sicurezza dei sistemi ICT e soprattutto delle grandi infrastrutture critiche informatizzate sempre più interconnesse e complesse e sempre più esposte a comportamenti illeciti di soggetti esterni o interni o a veri e propri attacchi (cyber-attacchi) organizzati, i responsabili dei sistemi informativi devono, perciò, preoccuparsi anche di individuare risorse professionali capaci di affrontare il tema della sicurezza ICT, in termini complessivi e sistemici.

Le strategie attuali, anche sulla base delle indicazioni raccolte presso un panel qualificato di esperti[39]provenienti da ambiti, aziendali, istituzionali accademici e professionali, tendono a considerare il tema della sicurezza ICT avendo a riferimento tre componenti chiave ampiamente interrelate tra di loro e il cui presidio congiunto appare ormai imprescindibile, sia nelle organizzazioni pubbliche che in quelle private.

Si tratta di tre aree così identificabili:

- *ICT security*: ovvero l'area dell'ICT aziendale che riguarda la protezione dei sistemi ICT al fine di salvaguardare i dati, le infrastrutture e gli applicativi ed i servizi;
- *Information security*: area della sicurezza aziendale che riguarda la protezione dei beni intangibili (informazioni, know how, brevetti, licenze ecc) al fine di salvaguardare riservatezza, integrità e disponibilità;
- *Operation security*: area della sicurezza aziendale che riguarda la protezione dei beni tangibili, (sedi aziendali, impianti di produzione, prodotti) e delle risorse umane.

39. Per realizzare la presente ricerca è stato interpellato anche un panel qualificato di esperti, provenienti da ambiti accademici, professionali, istituzionali e dal mondo aziendale.

Tenendo conto di questo articolato sistema di governo e gestione della sicurezza ICT in contesti organizzati, le possibili prospettive professionali in ambito della sicurezza ICT devono tendere, perciò, necessariamente ad ampliarsi.

È in questa prospettiva, allora che gli *ingegneri dell'informazione* possono giocare un ruolo molto più importante rispetto al recente passato, potendosi chiaramente distinguere da altri gruppi professionali proprio per le capacità e competenze tecniche ampie e trasversali che abbracciano sia la progettazione, con modelli di sviluppo orientati alla qualità, sia competenze gestionali.

Gli stessi *ingegneri dell'informazione* possono, poi, in particolare, rispondere meglio di altre figure alla necessità di integrare tecnologie per la sicurezza all'interno di infrastrutture informatizzate e infrastrutture più tradizionali, potendo dialogare agevolmente con altre figure di estrazione ingegneristica preposte al controllo di altri domini tecnologici sempre allo scopo di affrontare le problematiche della sicurezza e della qualità ICT.

Alte capacità e competenze tecnico professionali nella progettazione e realizzazione di sistemi ICT e nei modelli di sviluppo orientati alla qualità, con una deontologia codificata, e integrazione con le altre discipline ingegneristiche rappresentano dunque un valore strategico degli *ingegneri dell'informazione* soprattutto rispetto alla necessaria prospettiva sistemica che occorre perseguire per affrontare le problematiche connesse alla sicurezza dei sistemi ICT.

L'ingegnere dell'informazione appare ovviamente come il soggetto massimamente in grado di fornire le competenze più specifiche e specialistiche. Si tratta del professionista iscritto al settore *dell'ingegneria dell'informazione* dell'Ordine degli Ingegneri, abilitato, in base all'art. 46, 1 comma, lettera *c* del DPR n. 328/01, all'esercizio delle seguenti attività: *la*

pianificazione, la progettazione, lo sviluppo, la direzione lavori, la stima, il collaudo e la gestione di impianti e sistemi elettronici, di automazione e di generazione, trasmissione ed elaborazione delle informazioni. Si tratta dunque sia di sistemi informatici, ovvero come quegli insiemi di hardware e software finalizzati alla produzione, al trattamento, alla conservazione e alla trasmissione delle informazioni, di qualsiasi natura e sotto qualsiasi forma, sia di apparecchiature elettroniche inglobate (*embedded*) in altre apparecchiature, mobili o fisse, che contribuiscono, in tutto o in parte, con software precaricato, al loro controllo nell'ambito delle opere di ingegneria civile e/o industriale, nonché i meccanismi elettronici quali quelli per il controllo di impianti di produzione (sistemi di automazione industriale) o della rete elettrica di casa (sistemi di automazione civile) e sistemi automatici di gestione e controllo di infrastrutture, strutture militari, porti aeroporti, stazioni ferroviarie, ministeri, enti locali, tribunali, data warehouse, reti locali, reti geografiche, server di vari tipo, ecc.).

L'interlocuzione con i testimoni privilegiati ha evidenziato, in tal senso, anche alcune concrete aree di sviluppo e alcune possibili aree di specifica attività rispetto alle quali gli *ingegneri dell'informazione* stanno già assumendo un ruolo chiave, sempre in un'ottica di approccio sistemico alla sicurezza, soprattutto nelle grandi imprese e nelle grandi organizzazioni che gestiscono sistemi informativi, telecomunicazioni e altre infrastrutture critiche o in grandi imprese industriali con un patrimonio informativo strategico da tutelare.

Gli interlocutori intervistati hanno evidenziato la nascita di nuove funzioni aziendali all'interno della quale sono presenti varie strutture dedicate alle attività di analisi e gestione di tutte le componenti di sicurezza (fisica, logica ICT e finanziaria), secondo un modello di tipo "integrato e centralizzato", attraverso la stretta collaborazione con funzioni di business e ICT.

È in contesto di questo tipo che le professionalità dell'ingegnere dell'informazione appaiono, dunque, centrali (sebbene i numeri non possano che essere limitati in Italia in ragione della ridotta presenza di grandi imprese) soprattutto nelle seguenti attività:

- esperti di piattaforme di sicurezza perimetrale;
- progettazione di sistemi tecnologici e di contromisure;
- progettazione implementazione di sistemi di gestione sicuri;
- definizione di policy e procedure;
- difesa preventiva;
- analisi dei rischi (metodologie);
- business continuity e disaster recovery;
- incident management.

Gli ingegneri dell'informazione sono le figure più idonee a svolgere anche altre attività inerenti l'analisi delle nuove tipologie di minacce provenienti da Internet, dei rischi e delle eventuali contromisure per la messa in sicurezza dei canali e per l'erogazione dei servizi, magari attraverso un ampliamento delle proprie competenze con elementi di diritto e privacy e conoscenze in campo economico-finanziario soprattutto per il contrasto alle frodi finanziarie.

Agli *ingegneri dell'informazione* dovrebbero essere, inoltre, affidate nuove attività riguardanti le verifiche di sicurezza degli interi sistemi ICT; per essere effettivamente attendibili, tali verifiche devono essere effettuate da soggetti professionali terzi e indipendenti rispetto ai produttori od ai fornitori di servizi, allo scopo di testare dall'esterno la validità delle misure adottate e la impenetrabilità del sistema informatico, evidenziando le eventuali "falle" delle reti e suggerendo, al bisogno, gli eventuali rimedi.

Sempre agli ingegneri dell'informazione può essere validamente attribuita anche la cosiddetta fase di "collaudo" dei sistemi ICT, attraverso la quale verificare il corretto funzionamento e la qualità del sistema infor-

mativo realizzato da altri, prevedendo e verificando il funzionamento, per quanto possibile, per tutte le condizioni operative.

L'ingegnere dell'informazione può e deve giocare in questa nuova prospettiva un ruolo centrale per gestione della sicurezza dei sistemi ICT, potendo inserirsi sia nelle attività di pianificazione, progettazione, sviluppo dei sistemi software e sistemi di rete, sia nelle attività di identificazione dei requisiti di sicurezza dei sistemi ICT, sia in quelle attività di definizione delle soluzioni, favorendo l'integrazione di tecnologie per la sicurezza all'interno dell'infrastruttura ICT, preoccupandosi di far si che il sistema informativo sia in grado di resistere ad eventi imprevisti o ad atti dolosi (come i cyber-attacchi), che possano compromettere la disponibilità, l'autenticità, l'integrità e la riservatezza dei dati conservati o trasmessi e la fruizione stessa dei servizi offerti o resi accessibili tramite la rete o lo stesso sistema informatico.

Gli ingegneri dell'informazione possono avere un ruolo molto importante anche nella governance stessa della sicurezza intesa come bene pubblico da tutelare assumendo responsabilità dentro gli enti e gli organismi di controllo e indirizzo.

La figura professionale dell'ingegnere dell'informazione, potendo muoversi su ambiti tecnologici differenti ma complementari, costituisce il soggetto più idoneo a sovrintendere le diverse componenti e funzioni che interagiscono nel sistema della sicurezza. Come gruppo professionale caratterizzato da una profonda identità culturale e una non comune capacità di assunzione di responsabilità e una struttura di rappresentanza ben radicata, gli ingegneri e gli ingegneri dell'informazione in particolare possono, però, svolgere autorevolmente anche un ruolo di indirizzo e dialogo con le istituzioni e con i decisori per contribuire a migliorare la cultura e gli approcci complessivi alla sicurezza dei sistemi di rete ed informatici

È, infatti, evidente come gli ingegneri con il loro valore tecnico ed esperienziale possano contribuire a rendere più efficaci le scelte pubbliche in merito alla sicurezza delle infrastrutture critiche e delle infrastrutture informatiche critiche in particolare. Non si tratta solo della necessità di assegnare a figure dalle alte capacità tecniche la rappresentanza degli enti preposti per stare ai vari tavoli decisionali, quanto di affermare, piuttosto, la necessità di dar voce all'intera categoria degli ingegneri in quanto tale nei diversi tavoli tecnici riaffermando il ruolo pubblico dell'Ordine professionale.

In questo senso, nei modelli di partenariato pubblico e privato che vanno delineandosi anche in questo ambito con una rete sempre più estesa di soggetti chiamati a svolgere funzioni di controllo del sistema della sicurezza ICT, gli ingegneri ed il loro Ordine deve poter assumere un ruolo centrale.

Pubblicazioni del Centro Studi
del Consiglio Nazionale Ingegneri

no. 1 / 1999	Piano di attività - Triennio 1999 - 2002
no. 2 / 1999	La via dell'Etica Applicata, ossia delle politiche di prevenzione: una scelta cruciale per l'Ordine degli ingegneri
no. 3 / 1999	Monitoraggio sull'applicazione della direttiva di tariffa relativa al D. Lgs. 494/96 in tema di sicurezza nei cantieri
no. 4 / 2000	La dichiarazione di inizio attività - Il quadro normativo e giurisprudenziale
no. 5 / 2000	L'Autorità per la vigilanza sui lavori pubblici - Organi, poteri e attività
no. 6 / 2000	Le ipotesi di riforma delle professioni intellettuali
no. 7 / 2000	Le strutture societarie per lo svolgimento delle attività di progettazione - Il quadro normativo e giurisprudenziale
no. 8 / 2000	Le tariffe professionali - Il quadro giurisprudenziale in Italia e in Europa
no. 9 / 2000	Le assunzioni di diplomati e laureati in ingegneria in Italia
no. 10/2000	Il ruolo degli ingegneri per la sicurezza
no. 11/2000	Il nuovo regolamento generale dei lavori pubblici. Un confronto con il passato
no. 12/2000	Il nuovo capitolato generale dei lavori pubblici
no. 13/2000	Il responsabile del procedimento - Inquadramento, compiti e retribuzione
no. 14/2000	Il mercato dei servizi di ingegneria. Analisi economica e comparativa del settore delle costruzioni -Parte prima
no. 15/2000	Il mercato dei servizi di ingegneria. Indagine sugli ingegneri che svolgono attività professionale - Parte seconda
no. 16/2000	La professione di ingegnere in Europa, Canada e Stati Uniti. I sistemi nazionali e la loro evoluzione nell'epoca della globalizzazione
no. 17/2000	L'intervento delle Regioni in materia di dichiarazione di inizio attività
no. 18/2000	Opportunità e strumenti di comunicazione pubblicitaria per i professionisti in Italia
no. 19/2000	I profili di responsabilità giuridica dell'ingegnere - Sicurezza sul lavoro, sicurezza nei cantieri, appalti pubblici, dichiarazione di inizio attività
no. 20/2001	Spazi e opportunità di intervento per le amministrazioni regionali in materia di lavori pubblici
no. 21/2001	Imposte e contributi sociali a carico dei professionisti nei principali paesi europei
no. 22/2001	Le tariffe relative al D.Lgs 494/96. Un'analisi provinciale
no. 23/2001	Le nuove regole dei lavori pubblici. Dal contratto al collaudo: contestazioni, eccezioni, riserve e responsabilità
no. 24/2001	L'evoluzione dell'ingegneria in Italia e in Europa
no. 25/2001	La riforma dei percorsi universitari in ingegneria in Italia
no. 26/2001	Formazione e accesso alla professione di ingegnere in Italia
no. 27/2001	Le strutture societarie per lo svolgimento delle attività professionali in Europa
no. 28/2001	La direzione dei lavori nell'appalto di opere pubbliche
no. 29/2001	Analisi delle pronunce dell'Autorità per la vigilanza sui lavori pubblici. Febbraio 2000 -marzo 2001
no. 30/2001	Osservazioni sul D.P.R. 328/2001
no. 31/2001	La copertura assicurativa del progettista. Quadro normativo e caratteristiche dell'offerta

no. 32/2001	Qualificazione e formazione continua degli ingegneri in Europa e Nord America
no. 33/2001	Le verifiche sui progetti di opere pubbliche. Il quadro normativo in Europa
no. 34/2001	L'ingegneria italiana tra nuove specializzazioni e antichi valori
no. 35/2001	La domanda di competenze d'ingegneria in Italia. Anno 2001
no. 36/2001	Il mercato dei servizi di ingegneria. Evoluzione e tendenze nel settore delle costruzioni
no. 37/2002	Il riparto delle competenze normative in materia di professioni. Stato, Regioni, Ordini
no. 38/2002	Note alla rassegna stampa 2001
no. 39/2002	Ipotesi per la determinazione di un modello di stima basato sul costo minimo delle prestazioni professionali in ingegneria
no. 40/2002	Tariffe professionali e disciplina della concorrenza
no. 41/2002	Ipotesi per una revisione dei meccanismi elettorali per le rappresentanze dell'Ordine degli ingegneri
no. 42/2002	Installare il Sistema Qualità negli studi di ingegneria. Un sussidiario per l'applicazione guidata di ISO 9000:2000 - Volume I
no. 43/2002	Installare il Sistema Qualità negli studi di ingegneria. Un sussidiario per l'applicazione guidata di ISO 9000:2000 - Volume II
no. 44/2002	La remunerazione delle prestazioni professionali di ingegneria in Europa. Analisi e confronti
no. 45/2002	L'accesso all'Ordine degli ingegneri dopo il D.P.R. 328/2001
no. 46/2002	La domanda di competenze d'ingegneria in Italia. Anno 2002
no. 47/2003	Imposte e struttura organizzativa dell'attività professionale in Europa
no. 48/2003	Il mercato dei servizi di ingegneria. Anno 2002
no. 49/2003	Le nuove regole in materia di progettazione delle opere pubbliche. Tariffe, prestazioni gratuite, consorzi stabili e appalto integrato
no. 50/2003	La riforma del sistema universitario nel contesto delle Facoltà di Ingegneria
no. 51/2003	Una cornice di riferimento per una tariffa professionale degli ingegneri dell'informazione
no. 52/2003	La possibile " terza via"alla mobilità intersettoriale degli ingegneri in Italia
no. 53/2003	Il Testo Unico in materia di espropriazioni per pubblica utilità. Analisi e commenti
no. 54/2003	Il tortuoso cammino verso la qualità delle opere pubbliche in Italia
no. 55/2003	La disciplina dei titoli abilitativi secondo il Testo Unico in materia di edilizia
no. 56/2003	La sicurezza nei cantieri dopo il Decreto Legislativo 494/96
no. 57/2003	Analisi delle pronunce dell'Autorità per la vigilanza sui lavori pubblici. Aprile 2001- dicembre 2002
no. 58/2003	Le competenze professionali degli ingegneri secondo il D.P.R. 328/2001
no. 59/2003	La domanda di competenze d'ingegneria in Italia. Anno 2003
no. 60/2004	La riforma del sistema universitario nel contesto delle Facoltà di Ingegneria
no. 61/2004	Identità e ruolo degli ingegneri dipendenti nella pubblica amministrazione che cambia
no. 62/2004	Considerazionie ipotesi su possibili strategie e azioni in materia di SPC (Sviluppo Professionale Continuo) degli iscritti all'Ordine degli ingegneri
no. 63/2004	Le regole della professione di ingegnere in Italia: elementi per orientare il processo di riforma

no. 64/2004 Guida alla professione di ingegnere -Volume I: Profili civilistici, fiscali e previdenziali

no. 65/2004 Guida alla professione di ingegnere -Volume II: Urbanistica e pianificazione territoriale. Prima parte e seconda parte

no. 66/2004 La normativa tecnica per le costruzioni in zona sismica in Italia, Stati Uniti e Nuova Zelanda
Parte prima: profili giuridici
Parte seconda: applicazioni e confronti

no. 67/2004 Ipotesi e prospettive per la riorganizzazione territoriale dell'Ordine degli ingegneri

no. 68/2004 Le assunzioni degli ingegneri in Italia. Anno 2004

no. 69/2004 La direttiva 2004/18/CE relativa al coordinamento delle procedure di aggiudicazione degli appalti pubblici di lavori, di forniture e di servizi

no. 70/2004 La formazione degli ingegneri in Italia. Anno 2004

no. 71/2004 Occupazione e remunerazione degli ingegneri in Italia. Anno 2004

no. 72/2005 La verifica del progetto. Primi commenti allo schema di regolamento predisposto dalla Commissione ministeriale istituita dal vice ministro on. Ugo Martinat

no. 73/2005 Guida alla professione di ingegnere -Volume III: Formazione, mercato del lavoro ed accesso all'albo

no. 74/2005 Il mercato dei servizi di ingegneria. Anno 2004

no. 75/2005 Le tariffe degli ingegneri ed i principi di libertà di stabilimento e di libera prestazione dei servizi

no. 76/2005 Occupazione e remunerazione degli ingegneri in Italia. Anno 2005

no. 77/2005 Le assunzioni di ingegneri in Italia. Anno 2005

no. 78/2005 Analisi di sicurezza della Tangenziale Est-Ovest di Napoli

no. 79/2005 La formazione degli ingegneri in Italia. Anno 2005

no. 80/2005 Le competenze in materia di indagini geologiche e geotecniche e loro remunerazione in Italia ed Europa

no. 81/2005 Appalti sotto soglia e contratti a termine. Le recenti modifiche alla legge quadro sui lavori pubblici

no. 82/2005 Gli ingegneri e la sfida dell'innovazione

no. 83/2005 Responsabilità e copertura assicurativa del progettista dipendente

no. 84/2005 Guida alla professione di ingegnere -Volume IV: Le tariffe professionali e la loro applicazione

no. 85/2005 D.M. 14 settembre 2005 Norme tecniche per le costruzioni. Comparazioni, analisi e commenti

no. 86/2005 Il contributo al reddito e all'occupazione dei servizi di ingegneria

no. 87/2006 Guida alla professione di ingegnere -Volume V: Le norme in materia di edilizia

no. 88/2006 Analisi di sicurezza della ex S.S. 511 "Anagnina"

no. 89/2006 Le assunzioni di ingegneri in Italia. Anno 2006

no. 90/2006 Occupazione e remunerazione degli ingegneri in Italia. Anno 2006

no. 91/2006 Il mercato dei servizi di ingegneria. Anno 2005

no. 92/2006 Guida alla professione di ingegnere -Volume VI: La valutazione di impatto ambientale (VIA) e la valutazione ambientale strategica (VAS)

no. 93/2006 La formazione degli ingegneri in Italia. Anno 2006

no. 94/2007 La Direttiva 2005/36/CE relativa al riconoscimento delle qualifiche professionali.

no. 95/2007 Guida alla professione di ingegnere -Volume VII: La disciplina dei contratti pubblici
no. 96/2007 Criticità della sicurezza nei cantieri. Norme a tutela della vita dei lavoratori
no. 97/2007 Gli incentivi per la progettazione interna dei lavori pubblici
no. 98/2007 Le assunzioni di ingegneri in Italia. Anno 2007
no. 99/2007 Occupazione e remunerazione degli ingegneri in Italia. Anno 2007
no.100/2007 Guida alla professione di ingegnere -Volume VIII: Il collaudo: nozione, adempimenti e responsabilità
no.101/2008 Il mercato dei servizi di ingegneria. Anno 2006
no.102/2008 Energia e ambiente. Una nuova strategia per l'Italia
no.103/2008 Le competenze professionali degli ingegneri *iuniores*
no.104/2008 La formazione degli ingegneri in Italia. Anno 2007
no.105/2008 Occupazione e remunerazione degli ingegneri in Italia. Anno 2008
no.106/2008 Note e commenti al Decreto del Ministero dello Sviluppo economico del 22 gennaio 2008, n. 37
no.107/2008 La sicurezza nel settore delle costruzioni. Analisi dei dati e confronti internazionali
no.108/2008 Le assunzioni di ingegneri in Italia. Anno 2008
no.109/2008 Monitoraggio sui bandi di progettazione. Luglio-dicembre 2008
no.110/2009 Il mercato dei servizi di ingegneria. Anni 2007-2008
no.111/2009 L'abolizione del valore legale del titolo di studio. Inquadramento e possibili prospettive
no.112/2009 La formazione degli ingegneri in Italia. Anno 2008
no.113/2009 L'attualità delle tariffe professionali per le prestazioni d'ingegneria. I contenuti del nuovo *Honorarordnung für Architekten und Ingenieure – HOAI*
no.114/2009 L'indagine conoscitiva riguardante il settore degli Ordini professionali (IC34) predisposta dall'Autorità garante della concorrenza e del mercato. Analisi e commenti
no.115/2009 La sicurezza nel settore delle costruzioni. Analisi dei dati e confronti internazionali. Anno 2009
no.116/2009 Occupazione e remunerazione degli ingegneri in Italia. Anno 2009
no.117/2009 La formazione degli ingegneri in Italia. Anno 2009
no.118/2010 Il mercato dei servizi di ingegneria. Anni 2008-2009
no.119/2010 Monitoraggio sui bandi di progettazione. Anno 2009
no.120/2010 La libera prestazione di servizi in regime occasionale e l'attività professionale in regime di stabilimento a seguito del D.Lgs. 26 marzo 2010, n. 59. *"Attuazione della direttiva 2006/123/CE relativa ai servizi nel mercato interno"*
no.121/2010 L'inattendibilità dell'indicatore di intensità della regolamentazione della professione di ingegnere elaborato dall'Ocse. *La regolamentazione della professione di ingegnere negli Stati Uniti*
no.122/2010 Occupazione e remunerazione degli ingegneri in Italia. Anno 2010
no.123/2011 Monitoraggio sui bandi di progettazione. Anno 2010
no.124/2011 Il mercato dei servizi di ingegneria. Anni 2009-2010
no.125/2011 La formazione degli ingegneri in Italia. Anno 2010
no.126/2011 Il sistema di aggiudicazione dei bandi pubblici per i servizi d'ingegneria e architettura negli Stati Uniti

Finito di stampare nel mese di agosto 2011
Stampa: tipografia WebColor Srl, Località Le Campore, 67038 Oricola (AQ)