Luisa Franchina
Director General
Secretariat for Critical Infrastructures
Military Advisor Office
Presidency of the Council of the Ministers

Alessia Amodio
Master universitario di II livello in Protezione da eventi CBRNe

Francesco Unali
Giornalista e divulgatore dei temi della sicurezza e protezione civile

In questo lavoro viene messa in evidenza la stringente necessità di proteggere le IC da numerose minacce e viene esposto il contenuto del Decreto Legislativo 61/2011, con cui l'Italia ha recepito la Direttiva 114/08 CE, Direttiva che "stabilisce una procedura d'individuazione e designazione delle IC europee e un approccio comune per la valutazione della necessità di migliorarne la protezione al fine di contribuire alla protezione delle persone" [1]

La protezione delle Infrastrutture Critiche tra minacce vecchie e nuove. Il decreto 61/2011

Le minacce

Le innovazioni che hanno caratterizzato il XX secolo in tutti i settori dell'attività umana hanno certamente contribuito a migliorare la qualità della nostra vita. In quest'ottica, ad esempio, definiscono un certo livello di "qualità di vita" i servizi di fornitura dell'energia, la tutela della salute, il sistema dei trasporti, il sistema bancario. La fruibilità di questi "servizi" di base è ormai data per scontata, tanto è vero che, nel caso non fossero più disponibili, non sapremmo più come comportarci. La protezione delle IC è quindi divenuta indispensabile per la rilevanza che quel "complesso di opere e servizi pubblici" ha nella vita dei cittadini e dello Stato.

Un elemento che aggiunge complessità e urgenza al tema della protezione delle IC è associato alle dipendenze che le legano reciprocamente; a causa di tali dipendenze, per il corretto funzionamento di una infrastruttura è necessario che altre infrastrutture forniscano in modo adeguato nel tempo e nello spazio il loro apporto in termini di qualità dei servizi e dei prodotti. Lo scenario delle dipendenze tra IC, già in sé complesso, si è negli ultimi anni ulteriormente complicato (liberalizzazione del mercato, esternalizzazione di servizi e forniture, uso dei sistemi ICT (Information and Communication Technology). Quindi, un'interruzione o un malfunzionamento nella fornitura di un servizio può causare interruzioni a catena con ripercussioni in settori spesso apparentemente non correlati.

Innumerevoli e di natura diversa sono le minacce che possono compromettere il funzionamento delle IC, con ripercussioni che possono andare dal semplice disagio ad un considerevole numero di vittime con blocchi di servizio in molti settori della vita umana.

Alcune di queste minacce sono nate con l'uomo e da sempre l'uomo convive con esse, sono le minacce di origine naturale: terremoti, alluvioni, eruzioni vulcaniche, ecc. Generalmente, quando si parla di questo tipo di minacce si pensa a catastrofi che hanno causato un grande numero di vittime, tale da rendere del tutto di poco rilievo la perdita o il danneggiamento di "qualche IC",

perché si è portati a pensare che questo tipo di perdita non influenzi ulteriormente le nostre vite. Invece non è così. Per fare un esempio, nel 2010 il risveglio del vulcano islandese *Eyjafjallajokull* e la conseguente nube di polveri, che per fortuna non ha provocato perdite umane, ha provocato molte "vittime". I dati di impatto di questo evento di origine naturale, dopo solo 2 giorni di disagi, che ha coinvolto gravemente 20 paesi europei sono impressionanti [2]:

- 200 milioni di euro al giorno di perdita totale per le compagnie aeree;
- 7 milioni di passeggeri bloccati in tutta Europa;
- treni e trasporti su strada in crisi per picco di carico;
- assenza di *manpower* per importanti attività;
- assenza di beni in trasporto Cargo con gravi perdite nel settore delle derrate alimentari che sono andate in deperimento (pesce, carne, formaggi, ecc);
- servizi sanitari in grande difficoltà;
- servizi di emergenza attivati per il ricovero notturno in aeroporto e nelle stazioni ferroviarie.

La crisi è perdurata per alcuni giorni, portando anche a tensioni in ambito UE tra le istituzione politiche, le compagnie aeree (che premevano per riavviare i servizi per limitare i danni economici) e gli utenti dei mezzi aerei.

Gli agenti CBRNe (Chimici, Biologici, Radiologici, Nucleari ed esplosivi) rappresentano, invece, un tipo di minaccia che nel corso degli anni ha assunto un significato diverso. Gli agenti chimici e biologici venivano usati fin dall'antichità generalmente con scopi bellici e per controllare sommosse o rivolte, in ogni caso al fine di uccidere o ferire direttamente il nemico. Lo stesso uso è stato fatto degli agenti radiologici e nucleari, anche se scoperti molto tempo dopo.

Il primo uso non bellico di questi agenti si è avuto nel marzo 1995 con il rilascio di sarin (un agente nervino letale) nella metropolitana di Tokyo, ad opera della setta di Aum Shinrikyo.

Questa azione terroristica dimostrò per la prima volta la grande vulnerabilità dei centri urbani o comunque di luoghi ad alta densità di persone. Il segnale più forte si è avuto però in seguito all'attentato dell'11 settembre da quel giorno, infatti, tutti i Paesi occidentali hanno avviato, seppur con diversa enfasi, programmi per il rafforzamento della sicurezza nazionale e per la protezione sia delle infrastrutture ritenute critiche sia delle risorse fondamentali per la vita dello Stato [3,4,5,6]. Negli ultimi anni, quindi, questi agenti da sempre usati in campo di battaglia sono diventati una minaccia anche civile. L'impiego di questi agenti a scopo terroristico offre infatti molti vantaggi, talvolta unici, rispetto a sistemi di offesa convenzionali (elevata perdita di vite umane, limitata capacità di intervento, elevata efficienza, difficoltà tecnologica di rilevare queste sostanze), inoltre, questi agenti creano una risonanza mediatica tale da indurre panico generalizzato e risentimento nelle Istituzioni (basta ricordare le lettere all'antrace in America). La minaccia dell'uso terroristico delle armi CBRNe è attualmente uno dei temi di difesa prioritari per molti paesi.

Gli eventi legati agli agenti CBRNe possono essere suddivisi in due grandi categorie: quelli causati dall'uomo (che si distinguono a loro volta in eventi di tipo non intenzionale e intenzionale) e quelli generati da fenomeni naturali.

Innumerevoli possono essere gli scenari in cui si verificano eventi del genere. È pertanto evidente come sia difficile se non impossibile fornire un elenco completo di possibili scenari. Questi possono determinare serie conseguenze soprattutto se avvengono in zone affollate, ambienti chiusi, edifici pubblici, luoghi di riunione, mezzi di trasporto o se determinano la contaminazione d'aria, alimenti, acqua e/o terreno.

Da questo punto di vista la protezione delle IC da tali tipologie di rischi si manifesta come un'esigenza vitale dell'intero sistema.

Ne è un triste esempio il disastro di *Fukushima Dai-ichi*, gli incidenti occorsi presso la centrale nucleare omonima a seguito del terremoto e dello *Tsunami* (marzo 2011). L'acqua dell'onda anomala avrebbe infatti messo fuori uso i si-

I gravi episodi terroristici verificatisi negli ultimi anni, così come alcuni eventi occasionali di origine naturale o antropica, hanno dimostrato come le moderne società siano sempre più strettamente dipendenti dal corretto funzionamento di alcune infrastrutture, a ragione definite "critiche"

stemi elettrici che governano i sistemi di raffreddamento dei reattori della centrale innescando così la crisi e la conseguente fusione dei noccioli dei reattori 1, 2 e 3 [3]. L'incidente ha provocato ingenti danni tra morti, contaminati, perdite economiche e psicosi globale, causata dal dilagare di notizie, più o meno scientifiche, sull'arrivo della nube radioattiva.

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. Il terzo tipo di minaccia, infatti, è recente e viene dal *cyberspace.* Per "cyberspace" si intende comunemente l'infrastruttura di comunicazione globale, con tutte le informazioni che essa veicola, quali per esempio la voce, le e-mail, le transazioni bancarie, i video, le foto o qualsiasi altra informazione digitale che può essere trasmessa ed elaborata da una rete informatica. Questa infrastruttura non solo è di per sé un'IC (la Direttiva 114/08 CE riconosce la necessità di estendere in futuro la lista dei settori critici, e assegna la priorità al settore dell'*Information and Communication Technology* (ICT) [8]), ma questa infrastruttura ha acquisito via via un ruolo centrale rispetto ad un numero sempre più ampio di attività quotidiane e costituisce quindi un servizio trasversale rispetto ai vari settori, capace, se in crisi, di provocare impatti devastanti. Perciò, il tema della sicurezza e della qualità delle reti e dei sistemi informativi ha assunto una rilevanza assoluta. È necessario prevenire default tecnologici nei sistemi ICT, causati sia da eventi incidentali (di origine naturale o antropica) ma soprattutto da quelli di origine dolosa. Il rischio di una avaria di sistema, avrebbe, infatti, possibili impatti sui sistemi di governo, sulle comunicazioni complessive, sulla distribuzione di energia, sui trasporti e sul sistema finanziario con danni immediati.

Come sottolinea la Commissione nella Comunicazione n. 163 del marzo 2011 [9] negli ultimi anni sono emerse minacce nuove e più sofisticate dal punto di vista tecnologico la cui dimensione geopolitica globale sta diventando sempre più chiara. Si delinea attualmente la tendenza ad utilizzare le ICT per ottenere l'egemonia politica, economica e militare, anche avvalendosi delle capacità offensive. La "guerra informatica" o il "terrorismo informatico" sono dimensioni che ormai si sovrappongono al *cyber crime*.

Perché si tratta di una minaccia pericolosa e insidiosa? Innumerevoli sono i fattori che concorrono a rendere questo tipo di minaccia potenzialmente letale: la maggior parte dei sistemi di IC non sono stati progettati tenendo conto della sicurezza cibernetica (all'interno del settore elettrico, per esempio, la preoccupazione principale è sempre stata quella di mantenere una fornitura costante di energia elettrica ed un sistema efficiente); la natura mutevole di questa minaccia rende lo sviluppo dei sistemi di protezione generalmente più lento di quello della minaccia stessa; la precisa attribuzione della responsabilità degli attacchi informatici è estremamente difficile; i sistemi sono sempre più vulnerabili a causa dell'automazione e degli accessi remoti, dal momento che ci sono più punti d'accesso da cui lanciare gli attacchi.

I sistemi di controllo operativo sono ormai di largo uso. SCADA (*Supervisory Control And Data Acquisition*), un software di controllo industriale, è uno di questi ed è stato recentemente il bersaglio di *Stuxnet*, un *malware* molto sofisticato e insidioso. *Stuxnet* infetta i computer sfruttando alcune vulnerabilità di *Microsoft Windows*. Caricato sul computer tramite, tra gli altri, drive USB, file di rete condivisi o database SQL, *Stuxnet* mira a programmi SCADA specifici di *Siemens*. Se questo tipo di software è in funzione, *Stuxnet* ricerca una configurazione particolare di attrezzature industriali e poi lancia un attacco volto a manipolare alcuni microcontrollori per eseguirli casualmente ma segnalando ai responsabili del sistema un funzionamento regolare. Questo è sabotaggio puro e semplice (*Stuxnet* non ha un payoff criminale evidente), motivo che ha indotto a fare ampie congetture sul fatto che *Stuxnet* fosse volto ad

sul tema della protezione delle Infrastrutture Critiche (IC) si sono da tempo avviate in vari Paesi intense attività di normativa e regolamentazione. Al fine di ottenere una protezione mirata e quanto più possibile efficace è necessario conoscere le minacce che mirano a colpire le IC

infiltrarsi nel sito iraniano per l'arricchimento dell'uranio di Natanz, estremamente protetto [10]. La comparsa di questo *malware*, che può, in breve, essere considerato un'arma, dimostra che si può facilmente mirare ai sistemi SCADA da cui i sistemi di energia elettrica, gas, petrolio, rifornimento idrico e smaltimento delle acque nere di una nazione, superando le difese su cui la maggior parte delle aziende conta. Gli attacchi a questo tipo di sistemi sono particolarmente insidiosi perché consentono agli hacker di assumere il controllo diretto dei sistemi operativi, aprendo potenzialmente la strada a *blackout* di vaste proporzioni o disastri ambientali dolosi.

A *Stuxnet*, si è aggiunto di recente (l'allarme è stato lanciato da Symantec, una società di sicurezza americana, nell'ottobre del 2011) Duqu (o W32.Duqu) [11], scoperto da alcuni laboratori di ricerca europei. *W32.Duqu* è stato scritto partendo dal codice sorgente di *Stuxnet*, dice *Symantec*, ma non è progettato per attaccare i sistemi SCADA: piuttosto, il *trojan* cattura informazioni riservate e le trasferisce a un server remoto, non si replica, evita accuratamente di lasciare tracce della propria presenza e si auto-cancella dopo 36 giorni di "attività" spionistica. Lo scopo di Duqu è insomma "raccogliere dati di *intelligence* e *asset* da entità quali i produttori di sistemi di controllo industriale", continua Symantec, "così da condurre più facilmente un futuro attacco contro un'azienda terza" e, stando alle ricerche, il virus dovrebbe essere in circolazione già da dicembre 2010.

Il Decreto Legislativo 11 aprile 2011, n.61

L'Italia ha recepito, la Direttiva con il D.Lgs n. 61 dell'11 aprile 2011, "Attuazione della Direttiva 2008/114 CE recante l'individuazione e la designazione delle Infrastrutture Critiche Europee (ICE) e la valutazione della necessità di migliorarne la protezione" [12].

Il decreto stabilisce le procedure per l'individuazione e la designazione di ICE, nei settori dell'Energia e dei Trasporti, nonché le modalità di valutazione della sicurezza di tali infrastrutture e le relative prescrizioni minime di protezione dalle minacce di origine umana, accidentale e volontaria, tecnologica e dalle catastrofi naturali.

Le procedure riguardano, ovviamente, infrastrutture che si trovano in territorio nazionale e quelle che, pur trovandosi nel territorio di altri Stati membri dell'UE, l'Italia ha interesse a far designare ICE. Il decreto, inoltre, non modifica le competenze dei Ministeri coinvolti e, comunque, non modifica le disposizioni vigenti in ordine alle situazioni di emergenze che sono affrontate e gestite nelle sedi, anche interministeriali a ciò preposte, e dai singoli Ministeri, enti ed organizzazioni locali cui è attribuita tale competenza.

Il D.Lgs. affida al Nucleo Interministeriale Situazione e Pianificazione (NISP), istituito con Decreto del Presidente del Consiglio dei Ministri (DPCM) il 25 maggio 2010, le funzioni specificate nel decreto stesso per l'individuazione e la designazione delle ICE.

Per tali fini il NISP è integrato dai rappresentanti del Ministero dello sviluppo economico, per il settore energia, del Ministero delle infrastrutture e dei trasporti ed enti vigilanti, per il settore trasporti.

Il D.Lgs. individua una "struttura responsabile" (art.4, comma 3), con DPCM del 17 maggio 2011 la "struttura responsabile" è individuata nella Segreteria per le IC (SIC), istituita, con DPCM di organizzazione dell'Ufficio del Consigliere Militare della Presidenza del Consiglio dei Ministri (PCM) del 22 dicembre 2010, presso il medesimo Ufficio. Alla SIC sono affidate, per il supporto al NISP, le attività tecniche e scientifiche riguardanti l'individuazione delle ICE e per ogni altra attività connessa, nonché per i rapporti con la Commissione Europea (CE) e con le analoghe strutture degli altri Stati membri dell'UE.

Per gli aspetti connessi con la difesa civile, il NISP acquisisce il preventivo parere del Ministero dell'interno che si avvale, a tal fine, anche della Commissione Interministeriale Tecnica di Difesa Civile (CITDC), costituita a ottobre 2008

per supportare l'organizzazione nazionale di gestione delle crisi e di elaborare i criteri per l'individuazione delle IC nazionali.

Parallelamente, per gli aspetti connessi con le attività e i compiti di protezione civile, il NISP acquisisce il preventivo parere del Dipartimento della Protezione Civile della PCM.

La SIC, in collaborazione con il Ministero dello sviluppo economico, per il settore energia, e con il Ministero delle infrastrutture e dei trasporti ed enti vigilanti, per il settore dei trasporti, tenendo conto delle linee guida elaborate dalla CE, determina il limite del criterio di valutazione settoriale oltre il quale l'infrastruttura può essere potenzialmente critica. Il Ministero delle infrastrutture e dei trasporti e il Ministero dello sviluppo economico individuano le possibili ICE (sia quelle situate in territorio nazionale, sia quelle situate in altri Stati membri dell'UE che, nell'ambito dello stesso settore, potrebbero essere d'interesse significativo).

Ogni infrastruttura situata in territorio nazionale, ai fini della sua designazione come ICE, deve risultare essenziale per il mantenimento delle funzioni vitali della società, della salute, della sicurezza e del benessere economico e sociale della popolazione e, a tale fine, è esaminata la gravità dei possibili effetti negativi esterni ed intrinseci, in caso di danneggiamento o distruzione, in base a criteri di valutazione settoriali e intersettoriali. I criteri introdotti nel decreto legislativo sono gli stessi contenuti nella Direttiva 114/08 CE, sono riportati nelle linee guida emesse dalla CE in accompagnamento alla direttiva e sono riservati. Le soglie sono stabilite caso per caso dalla SIC con i Ministeri competenti a livello settoriale.

Anche i criteri di valutazione intersettoriali (*cross-cutting*) sono gli stessi individuati dalla Direttiva:

a. le possibili vittime, in termini di numero di morti e di feriti;
b. le possibili conseguenze economiche, in termini di perdite finanziarie, di deterioramento del bene o servizio e di effetti ambientali;
c. le possibili conseguenze per la popolazione, in termini di fiducia nelle istituzioni, di sofferenze fisiche e di perturbazione della vita quotidiana, considerando anche la perdita di servizi essenziali.

Si osservi che i criteri *cross-cutting* comprendono sia dei riferimenti numerici assoluti (come nel caso degli effetti sulla salute o di quelli economici), che sono quindi difficilmente scalabili alle diversificate realtà nazionali nella UE, sia dei parametri di carattere socio-politico e psicologico, che sono fortemente dipendenti dalla singole realtà nazionali. In ogni caso, le soglie per l'applicazione dei criteri saranno basate sulla severità dell'impatto sui cittadini a causa dell'interruzione del servizio dell'infrastruttura in esame.

Per ogni infrastruttura devono essere esaminate e valutate diverse ipotesi, tenendo conto della disponibilità di alternative, delle possibili diverse durate del danneggiamento e dei tempi per il ripristino della funzionalità.

La SIC, insieme al Ministero degli affari esteri, dell'interno e della difesa, e al Dipartimento della Protezione Civile della PCM, effettua le negoziazioni con gli Stati membri interessati. Le discussioni bilaterali o multilaterali hanno lo scopo di fissare limiti comuni dei criteri di valutazione intersettoriali e di verificare se i possibili effetti negativi esterni ed intrinseci, in caso di danneggiamento o distruzione dell'infrastruttura, superano tali limiti per gli Stati membri interessati; ove ciò si verifichi l'infrastruttura è individuata come ICE e il NISP, integrato dal Ministero delle infrastrutture e trasporti e dal Ministero dello sviluppo economico, designa le ICE su territorio italiano.

La SIC informa della designazione esclusivamente gli Stati membri con cui è stata sottoscritta l'intesa e comunica annualmente alla CE solo il numero di ICE ubicate nel territorio nazionale, per ciascun settore, nonché il numero degli Stati membri che dipendono da ciascuna di esse.

I Ministeri dell'interno, della difesa, dello sviluppo economico, per il settore energia, e quello delle infrastrutture e dei trasporti, per il settore trasporti, il Dipartimento della

Protezione Civile della PCM, pongono in essere, nell'ambito delle rispettive competenze, tutte le azioni e le misure indispensabili a garantire la protezione delle ICE ubicate in territorio nazionale, avvalendosi dei propri organi centrali o delle articolazioni locali, ove esistenti, e tenendo informato il NISP.

A livello locale la responsabilità della protezione delle ICE è attribuita al Prefetto territorialmente competente. Qualora l'ICE abbia estensione tale da investire la competenza di più Prefetti, il Ministero dell'interno individua con apposito decreto dirigenziale il Prefetto responsabile.

Alle ICE designate sono richiesti alcuni adempimenti e cioè, in particolare, la nomina di un funzionario di collegamento in materia di sicurezza che è anche funzionario alla sicurezza in materia di tutela delle informazioni classificate e la redazione di un Piano di Sicurezza dell'Operatore (PSO). L'operatore nel predisporli si avvale dei funzionari, appositamente nominati per ogni infrastruttura, dal Ministero dello sviluppo economico (settore energia), dal Ministero delle infrastrutture e dei trasporti (settore trasporti), dal Ministero dell'interno, dal Ministero della difesa, dal Dipartimento della Protezione Civile della PCM. L'operatore si avvale altresì della SIC, che lo assiste anche per l'aggiornamento del piano eventualmente esistente.

L'Allegato B al D. Lgs. 61/2011, riporta i requisiti minimi del PSO [12], gli stessi identificati dalla Direttiva 114/08 CE.

Il Prefetto responsabile approva il PSO e, ove l'ICE designata disponga già di un PSO ai sensi delle disposizioni normative vigenti, si limita ad accertare che tali disposizioni rispettino i parametri minimi.

Il NISP è punto di contatto nazionale per la protezione delle ICE con gli Stati membri e con la CE. Il NISP può altresì coordinare l'elaborazione di direttive interministeriali, contenenti parametri integrativi di protezione, ferme restando le competenze del Ministro dell'interno, e quelle del Dipartimento della Protezione Civile della PCM.

Il NISP, in base alle informazioni comunicate dalle Amministrazioni competenti:

- entro un anno dalla designazione di un'ICE, elabora una valutazione delle possibili minacce nei riguardi del sottosettore nel cui ambito opera l'ICE designata e la struttura responsabile ne informa la SIC;
- ogni due anni elabora i dati generali sui diversi tipi di rischi, minacce e vulnerabilità dei settori in cui vi è un'ICE designata e la struttura responsabile comunica, tali dati generali, alla SIC.

Conclusioni

Le IC, proprio per il loro ruolo fondamentale nel garantire la qualità di vita dei cittadini, possono essere oggetto di crisi nell'erogazione del servizio che potrebbero avere quindi un considerevole impatto. Numerose sono le minacce, dalle più "classiche" alle più tecnologicamente avanzate. L'aumento dell'automazione e le nuove piattaforme di distribuzione dei servizi, quali i sistemi interoperabili di "lettura intelligente" dei contatori dell'energia elettrica o di home banking su dispositivi portatili, creano nuove vulnerabilità ma offrono anche nuove opportunità. Innumerevoli sono le sfide ancora da affrontare in materia di protezione di IC, per raggiungere l'obiettivo è necessaria la partecipazione degli operatori/proprietari di IC e dei Governi. Gli operatori sicuramente devono partire dall'adozione su larga scala di misure di sicurezza chiave. I governi possono incoraggiare la sicurezza collaborando con il settore industriale di riferimento e adottando normative che richiedono una sicurezza migliore di quanto non faccia il mercato. La natura di tali collaborazioni sarà diversa da nazione a nazione e varierà dall'incoraggiamento all'azione obbligatoria, ma la natura delle nuove minacce che il settore si trova ad affrontare richiede il coinvolgimento del governo.

Da questo punto di vista la Direttiva europea e, di conseguenza il D. Lgs. 61/2011 rappresentano un buon esempio, oltre che un punto di partenza fondamentale perché, oltre a generare un livello comune di protezione, permette la condivisione di informazioni e *best practice* che consentono di migliorare ulteriormente il livello di protezione globale. Anche se il cammino è ancora lungo il passo successivo, la revisione della Direttiva, dovrebbe iniziare proprio quest'anno.

Riferimenti

[1] Direttiva del Consiglio relativa all'individuazione e alla designazione delle IC europee e alla valutazione della necessità di migliorarne la protezione, COM(2008), Bruxelles, 6 giugno 2008.

[2] Ansa, 17-04-2010

[3]Homeland Security Presidential Directive/Hspd-7, 17 dicembre 2003; www.whitehouse.gov/news/releases/2003/12/20031217-5.html

[4] National Infrastructures Protection Plan, Department of Homeland Security, 2009, www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf

[5] International CIIP Handbook 2006, an inventory of 20 national and 6 international critical Infrastructure Protection Policies, ETH, Zurich, marzo 2006.

[6] International CIIP Handbook 2008-2009, an inventory of 25 national and 7 international critical Infrastructure Protection Policies, ETH, Zurich, settembre 2008.

[7] *WNN, World Nuclear Association, Efforts to manage Fukushima Daiichi 3, 13-03-2011.*

[8] L. Franchina, M. Carbonelli, L. Gratta, D. Perucchini, La protezione delle IC: la proposta di Direttiva Europea, ICT Security, anno VII, maggio 2008, p.16-20.

[9] Comunicazione della Commissione al Consiglio e al Parlamento Europeo - Realizzazioni e prossime tappe: verso una sicurezza informatica mondiale, COM(2011) 163, Bruxelles, 31-03-2011

[10] McAfee, Minacce nell'ombra – Le infrastrutture critiche affrontano gli attacchi cibernetici www.mcafee.com/it/resources/reports/rp-critical-infrastructure-protection.pdf

[11] Symantec Security Response, W32.Duqu – The precursor to the next Stuxnet, Version 1.2, 20-10-2011

[12] DECRETO LEGISLATIVO 11 aprile 2011, n. 61, Attuazione della Direttiva 2008/114/CE recante l'individuazione e la designazione delle infrastrutture critiche europee e la valutazione della necessità di migliorarne la protezione.