OSSERVATORIO
DI POLITICA INTERNAZIONALE

C*yber-security*: Europa e Italia

n. 32 - maggio 2011

Approfondimenti

a cura dell'Istituto Affari Internazionali (IAI)

C*yber-security*: Europa e Italia

n. 32

maggio 2011

Cyber-security: Europa e Italia

Federica Di Camillo, Valérie Vicky Miranda e Stefano Felician*

Questo studio fornisce un'introduzione a concetti e dinamiche essenziali relativi alla *cyber-security*, nonché una panoramica delle più significative iniziative europee ed italiane nel settore.

Il primo capitolo delinea il quadro concettuale delle principali problematiche legate alla *cyber-security*. Si rileva in primo luogo l'assenza di definizioni condivise a livello UE della *cyber-security* e di fenomeni collegati, aspetto che rende difficile la creazione e l'applicazione di chiare fattispecie legali. Viene anche discusso il rapporto tra *cyber-security* e *cyber-warfare*, ossia l'utilizzo della rete digitale come dimensione di guerra. Il capitolo si conclude con una breve esposizione delle due aree che l'Unione Europea sembra considerare prioritarie: la protezione delle infrastrutture critiche informatizzate e il contrasto al cyber-crimine (*cyber-crime*).

Il secondo capitolo esamina le maggiori iniziative dell'UE in materia di *cyber-security*. L'analisi evidenzia sovrapposizioni e dinamiche in parte ancora in via di sviluppo, ma anche potenziali sinergie per definire risposte efficienti alle problematiche inerenti alle diverse aree. Fermo restando il carattere sussidiario della competenza UE in materia (per cui la responsabilità primaria resta in capo agli Stati) si mette in luce il crescente ruolo dell'UE nella gestione della *cyber-security* che, da un lato, incoraggia il dialogo e lo scambio di *best practices* tra gli Stati membri e tra questi e le istituzioni europee – anche grazie alla creazione di strutture dedicate come l'Agenzia europea per la Sicurezza delle Reti e dell'Informazione (*European Network and Information Security Agency*, ENISA), dall'altro, promuove il miglioramento delle capacità di risposta europee e nazionali ad eventuali attacchi o incidenti informatici.

Il terzo capitolo è dedicato alle iniziative italiane. Le istituzioni italiane prestano crescente attenzione ai temi legati alla *cyber-security*, in un quadro che deve armonizzare ruoli e competenze di una pluralità di attori coinvolti.

Infine, nelle conclusioni viene proposta una serie di suggerimenti per massimizzare l'efficacia della protezione delle reti digitali. Le raccomandazioni spaziano dal campo teorico (con la ricerca di chiarezza ed armonizzazione terminologica) a quello legale, da quello politico-istituzionale a quello tecnico-operativo e degli investimenti in ricerca e sviluppo (R&S). Tutte le raccomandazioni sono state elaborate avendo come riferimento il decisore politico nazionale. Tuttavia, la natura transnazionale della *cyber-security* – in cui le vulnerabilità non conoscono confini geografici – impone una riflessione sviluppata anche in senso multilaterale e, in particolare, comunitario.

* Federica Di Camillo è responsabile di ricerca e Valérie Vicky Miranda e Stefano Felician sono assistenti alla ricerca presso l'Istituto Affari Internazionali (IAI) di Roma.

Indice

Indice delle tabelle e figure

Introduzione

Cyber-security, *cyber-crime*, *cyber-terrorism*, *cybersabotage*, *cyber-attack*, *cyber-war*, *information warfare*, *cyber-espionage*… queste ed altre "*cyber* categorie" continuano ad essere utilizzate più o meno indistintamente in molti ambiti. Ciò va in parte attribuito al fatto che il settore è in rapida evoluzione, ad un quadro legale assente o in divenire, nonché alla complessità derivante dalla combinazione delle tecnologie per le informazioni e comunicazioni (*Information and Communication Technology*, ICT) con altri sistemi fondamentali per la sostenibilità delle funzioni chiave delle società moderne (le c.d. infrastrutture critiche).

L'approfondimento è volto a facilitare la comprensione di questo tema. Nel primo capitolo si forniranno gli elementi fondamentali dell'approccio europeo alla *cyber-security*: il perimetro concettuale e l'ordine di priorità delle differenti minacce. Nel secondo capitolo si riassumeranno e valuteranno le iniziative intraprese a livello di Unione Europea (UE). Nel terzo capitolo si analizzerà la collocazione dell'Italia in termini di rispondenza al quadro europeo ed internazionale. Infine, nelle conclusioni si forniranno alcune opzioni realisticamente percorribili per rendere più efficaci le varie iniziative adottate sia a livello nazionale che europeo.

Capitolo 1 – Delimitazione del problema: cos'è la *cyber-security*?

Al fine di delimitare il campo di studio, consideriamo innanzitutto quale sia l'approccio strategico sviluppato e condiviso a livello europeo. Procediamo rilevando i riferimenti al concetto "*cyber*" che possiamo trovare nei seguenti documenti strategici europei, tutti dell'ultimo decennio:

1) *Un'Europa sicura in un mondo migliore – Strategia europea in materia di sicurezza* (2003)
2) *Relazione sull'attuazione della Strategia europea in materia di sicurezza – Garantire sicurezza in un mondo in piena evoluzione* (2008)
3) Dichiarazione del Consiglio dell'8 dicembre 2008 sul rafforzamento della sicurezza internazionale (2008)
4) *Strategia di sicurezza interna per l'Unione Europea: "Verso un modello di sicurezza europeo* (2010)
5) *La strategia di sicurezza interna dell'UE in azione: cinque tappe verso un'Europa più sicura* (2010)

Selezionando i riferimenti terminologici più significativi all'interno di questi documenti, si osserva una certa varietà semantica e la completa mancanza di definizioni formali [corsivo aggiunto]:

1) "la dipendenza europea da *un'infrastruttura interconnessa* […] nel settore *dell'informazione* […]; i *movimenti terroristici* possono contare su risorse finanziarie ingenti, *sull'allacciamento in reti telematiche*".[1]

2) "*Cybersecurity*";*"*Le economie moderne dipendono fortemente da *infrastrutture critiche quali* i trasporti, le *comunicazioni* e l'approvvigionamento energetico, ma anche *Internet*. […] gli *attacchi contro sistemi informatici privati o governativi* hanno dato a tale questione una nuova dimensione, quella di una *nuova arma potenziale di tipo economico, politico e militare*. […]"; "È necessario lavorare ulteriormente in questo settore, al fine di ricercare un approccio globale dell'UE, prestare opera di sensibilizzazione e rafforzare la cooperazione internazionale".[2]

3) "*L'uso di internet da parte di gruppi di terroristi*"; "[...] (aggiornare la legislazione) per *far sì che sia previsto come reato il reclutamento e l'istigazione al terrorismo effettuato con internet*"; "attacchi cibernetici"; "interferenze con enti pubblici e privati"; "[…] aumentare *la protezione e la resilienza delle nostre reti*, migliorando la cooperazione a livello operativo fra Stati Membri".[3]

4) "[…] *la cibercriminalità* costituisce una *minaccia* globale, tecnica, transfrontaliera e anonima *per i nostri sistemi d'informazione*"; "il terrorismo […] la propaganda su internet"; "nuovi rischi e minacce quali […] *l'arresto delle TIC (tecnologie dell'informazione e della comunicazione*)".[4]

5) *"Criminalità informatica*"; "L'Europa ne è un bersaglio chiave, per la sua infrastruttura Internet avanzata, l'alto numero di utenti e il fatto che i circuiti economici e i sistemi di pagamento sono supportati da Internet"; "*Cittadini, imprese, amministrazioni pubbliche e infrastrutture critiche*: tutti devono godere di maggiore protezione dalle forme di criminalità che sfruttano le tecnologie moderne."; "*La sicurezza delle reti informatiche* è un fattore essenziale per il buon funzionamento della società dell'informazione: è quanto riconosce l'Agenda Digitale europea[5], di recente pubblicazione, che tratta questioni legate alla *criminalità informatica, alla sicurezza informatica, all'uso sicuro di internet* e alla *privacy* quali presupposti per instaurare un clima di fiducia e sicurezza per gli utenti della rete."; "Lo sviluppo e l'applicazione rapida delle nuove tecnologie dell'informazione hanno creato anche *nuove forme di attività criminale*. La criminalità informatica è un fenomeno mondiale che provoca *danni ingenti al mercato interno dell'UE*. *E se la struttura di Internet*

---

[1] Consiglio dell'Unione Europea, *Un'Europa sicura in un mondo migliore, Strategia europea in materia di sicurezza,* 2003, Bruxelles, http://www.consilium.europa.eu/uedocs/cmsUpload/031208ESSIIIT.pdf p. 2 e p. 3.

[2] Consiglio dell'Unione Europea, *Relazione sull'attuazione della Strategia europea in materia di sicurezza – garantire sicurezza in un mondo in piena evoluzione,* S 407/08, 2008,Bruxelles, http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressdata/IT/reports/104641.pdf p. 5.

[3] Libera traduzione da: Consiglio dell'Unione Europea, *Statement on tighter International security*, 16751/08, 2008, Bruxelles http://register.consilium.europa.eu/pdf/en/08/st16/st16751.en08.pdf

[4] Consiglio dell'Unione Europea, *Progetto di strategia di sicurezza interna per l'Unione Europea: "Verso un modello di sicurezza europeo",* 5842/2/10 2010, Bruxelles, http://register.consilium.europa.eu/pdf/it/10/st05/st05842-re02.it10.pdf p. 6, 5 e 12.

[5] Per un approfondimento sull'Agenda Digitale europea si veda il Capitolo 2 del presente lavoro.

non conosce frontiere, le competenze a perseguire la criminalità informatica restano ancora di livello nazionale. Gli Stati membri devono riunire gli sforzi a livello UE: l'High Tech Crime Centre, presso Europol, svolge già un importante *ruolo di coordinamento per le attività di contrasto*, ma bisogna fare di più".[6]

Il trascorrere degli anni non ha dunque portato a convergenze terminologiche né di significato. Mai in questi documenti strategici, né in quelli più specifici relativi alle politiche in materia (cfr. capitolo 2) viene fornita una definizione della parola "*cyber-security*", pur utilizzata.

La stessa constatazione è stata espressa in un passaggio di un recente rapporto di Chatham House (prestigioso centro studi internazionali britannico) in cui si sostiene che la *cyber-security* (intesa come sicurezza "nel" e "dal" *cyber*-spazio) è un problema dalla natura non ben definita, che troppo spesso risulterebbe da un'infelice "combinazione di intuizione e incertezza uniti a pessimismo" (!). Questo elemento fondamentalmente irrazionale che caratterizza la percezione della *cyber-security* contribuisce a far sì che le analisi di valutazione della minaccia si concentrino quasi esclusivamente su eventi di grande effetto, ma di bassa probabilità, distogliendo importanti risorse dalla gestione di problemi più ordinari, ma anche più urgenti.[7]

Pur nella diversità di contesti (dimensioni interna ed esterna della sicurezza), di paternità istituzionale, e di valore politico e legale, i cinque documenti sopra considerati tentano comunque di fissare delle priorità in termini di risposta alla minaccia.

Prima di passare ad esaminare più in dettaglio il contenuto dei documenti europei, è opportuno soffermarsi su un aspetto che invece non vi è presente e che è dunque escluso dall'area di interesse primaria dell'Unione Europea, e cioè la "guerra cibernetica" o *cyber-warfare.*[8] Per avere un'idea della rilevanza di questo elemento, è utile ricordare che *cyber-security* e *cyber-warfare* sono da anni parte integrante della dottrina di difesa americana, al punto che il *cyber*-spazio viene considerato dalle forze armate USA alla stregua delle quattro "dimensioni" fisiche della guerra (terra, mare, aria, spazio). Il problema della *cyber-security* è affrontato sia in documenti di dottrina militare sia in quelli di più ampio orientamento strategico. Per esempio, la Rassegna quadriennale di difesa del 2010 (*Quadriennal Defense Review*, una specie di libro bianco della difesa periodicamente aggiornato dal Pentagono) si riferisce agli attacchi *cyber* senza fornire una definizione precisa, ma evidenziando la possibilità che gli obiettivi possano essere sistemi di

---

[6] Commissione Europea, *La Strategia di sicurezza interna dell'Unione Europea in azione: cinque tappe verso un'Europa più sicura,* COM(2010) 673*,* Bruxelles http://eur-lex.europa.eu/Notice.do?mode=dbl&lang=en&ihmlang=en&lng1=en,it&lng2=bg,cs,da,de,el,en,es,et,fi,fr,hu,it,lt,lv,mt,nl,pl,pt,ro,sk,sl,sv,&val=534356:cs&page=

[7] Paul Cornish, Rex Huges, David Livingstone, *Cyberspace and the National Security of United Kingdom,* 2009, Londra, http://www.chathamhouse.org.uk/files/13679_r0309cyberspace.pdf

[8] Da non confondere con la guerra elettronica, che è un'attività militare che utilizza lo spettro elettromagnetico (costituito da tutte le possibili frequenze delle radiazioni elettromagnetiche, dalle onde radio ai raggi gamma) per attacco, difesa o sorveglianza (o acquisizione di informazioni). La guerra elettronica si divide in tre settori: attacco, protezione e supporto. Nel primo caso si cerca di impedire all'avversario l'uso dello spettro elettromagnetico (ad esempio "confondendo" un sistema radar nemico); nel secondo si cerca di difendersi dagli attacchi avversari o quantomeno di limitarne la portata; nella terza categoria sono infine comprese attività di "ascolto", controllo e identificazione di fonti elettromagnetiche avversarie.

comando e controllo e infrastrutture del *cyber*-spazio che servono piattaforme di sistemi d'arma. La Strategia di sicurezza nazionale (*National Security Strategy*, un documento di orientamento strategico più generale preparato dalla Casa Bianca), sempre del 2010, individua nelle tecnologie spaziali e informatiche che assicurano funzioni sociali quotidiane (come l'uso di cellulari o di internet) così come in sensibili attività militari una vulnerabilità specifica delle societàmoderne.[9]

Nei documenti strategici europei questo aspetto è solo vagamente menzionato, ad esempio quando si mette in evidenza che attacchi contro sistemi informatici pubblici o privati possono configurarsi come una specie di azione militare.[10] La conclusione è che in Europa il *cyber-warfare* è per il momento considerato di esclusiva competenza della NATO[11] oltre che degli Stati membri.[12] È infatti in ambito NATO che si è assistito ad un dibattito sull'opportunità di considerare attacchi cibernetici su larga scala, come quelli perpetrati ai danni dell'Estonia (membro NATO) nel 2007 e della Georgia (aspirante membro NATO) nel 2008, come fattispecie rientranti negli artt. 4 e 5 del Trattato di Washington (l'accordo istitutivo della NATO), tali dunque da attivare la clausola di difesa collettiva tra gli Alleati.

Se ripercorriamo il caso della Georgia gli attacchi presero la forma, come del resto per l'Estonia[13], di DDoS (*Distributed Denial of Service*, letteralmente "negazione diffusa di servizio").[14] Si tratta di un attacco relativamente semplice e dai costi contenuti, a fronte del notevole impatto di riuscita, che andò a paralizzare i siti governativi (es. quello del Presidente e della Banca nazionale georgiana) e d'informazione. In Georgia gli attacchi iniziarono già dalle settimane precedenti

[9] White House, National Security Strategy*,* May 2010*,*
http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf

[10] Consiglio dell'Unione Europea, *Relazione sull'attuazione della strategia europea in materia di sicurezza - Garantire sicurezza in un mondo in piena evoluzione*, 2008, http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressdata/IT/reports/104641.pdf

[11] La politica di cyberdifesa è attuata dalle autorità politiche, militari e tecniche della NATO come dai singoli Stati alleati. Uno dei principali aspetti di questa politica è stata la creazione della NATO Cyber Defence Management Authority (CDMA) con l'unica responsabilità di coordinare la difesa informatica in tutti i quartieri generali dell'Alleanza e nei comandi e nelle agenzie associate spostando le molteplici reti informatiche di oggi verso un sistema amministrato a livello centrale. Il CDMA della NATO è gestito dal Cyber Defence Management Board, che comprende i responsabili degli uffici politici, militari, operativi e tecnici della NATO che si occupano di difesa informatica. Il CDMA è il principale organo di consulenza del Consiglio Atlantico in materia di difesa informatica, e offre pure consulenza agli stati membri su tutti i principali aspetti della difesa cibernetica. Il CDMA della NATO opera sotto l'egida della divisione Emerging Security Challenges (sfide emergenti alla sicurezza) del NATO HQ (comando e staff). Traduzione degli autori da NATO, *Defending against cyber attacks,* http://www.nato.int/cps/en/natolive/topics_49193.htm.

[12] Si consideri ad esempio il CCD COE (Cooperative Cyber Defence Centre of Excellence): attivo a Tallinn dal 2008, si occupa di cyberdefence e, in generale, di tutte le problematiche connesse alla dimensione "informatica" e del miglioramento delle capacità Nato in materia. Si tratta di una struttura creata da alcune nazioni dell'Alleanza, ma non è finanziato dalla Nato, non è un comando operativo né rientra nella struttura di comando Nato. Le diverse aree di competenza vanno dagli aspetti legali a quelli strategici, fino alla protezione delle infrastrutture critiche.

[13] Nell'aprile del 2007, dopo la rimozione dalla capitale estone Tallin di una statua in bronzo, monumento ai "liberatori" sovietici, la rete informatica del Paese, in particolare ministeri, banche, giornali, televisioni,è stata vittima di un cyber-attacco su larga scala che ne ha causato la temporanea interruzione.

[14] Il Distributed Denial of Service consiste nell'"infettare" una serie di computer con programmi come malware o virus che vanno a formare una botnetwork (una rete) di computer zombie, cioè controllabili non solo dal proprietario, ma anche da terzi che ne utilizzano le potenzialità per attaccare un obiettivo (come un server o un sito) inondandolo di dati (ad esempio con richieste di informazioni, di accesso) in modo da rallentarne la funzionalità o paralizzarlo. Maggiori sono le dimensioni della botnet, maggiore sarà la potenzialità di un DDoS.

l'intervento armato della Russia per il controllo dell'Ossezia del Sud e dell'Abkhazia, risultando, secondo le parole dell'ambasciatore georgiano presso la NATO, in "un attacco informatico coordinato con le operazioni terrestri, aeree e navali […], che sconvolsero i sistemi bancari e le comunicazioni in un momento decisivo del conflitto."[15]

Gli attacchi cibernetici di cui sono state vittime Estonia e Georgia hanno posto agli strateghi NATO un duplice problema. Da un lato ci si è chiesti se la natura degli attacchi sia tale da giustificare l'attivazione della clausola di difesa collettiva contenuta nell'art. 5 del trattato NATO. Dall'altro lato si è cominciato a discutere sul contributo dell'Alleanza al rafforzamento delle capacità di difesa cibernetica dei suoi Stati membri.

La questione della *cyber-security* è stata trattata anche nel rapporto del Gruppo dei saggi (2010) in vista del nuovo Concetto strategico NATO nei seguenti termini [corsivo aggiunto]: "*Capacità di difesa informatica*. Il prossimo attacco di un qualche rilievo contro l'Alleanza potrebbe essere sferrato tramite un cavo di fibra ottica. Già adesso gli *attacchi informatici contro i sistemi della NATO* sono frequenti, ma restano molto spesso sotto la *soglia di preoccupazione politica*. Tuttavia il rischio di un *attacco su larga scala contro i sistemi NATO di comando e controllo o contro le reti energetiche* potrebbero facilmente giustificare le consultazioni di cui all'articolo 4 o potrebbero forse portare alle misure di difesa collettiva di cui all'articolo 5 del Trattato".[16]

Da notare il riferimento a "sistemi della NATO", ad attacchi su larga scala e alla discriminante della "soglia di preoccupazione politica", che rappresentano questioni fondamentali poi riconfermate dal vertice NATO di Lisbona.[17] Infatti, il nuovo Concetto strategico[18], approvato in occasione del vertice, prevede, a fini di deterrenza e difesa da minacce alla sicurezza dei cittadini lo sviluppo ulteriore di capacità di prevenzione, identificazione, difesa e recupero dagli attacchi informatici, ivi inclusi il ricorso alla pianificazione NATO per migliorare e coordinare le capacità nazionali di difesa informatica, la protezione informatica di tutte le strutture dell'Alleanza con un sistema centralizzato, nonché la migliore integrazione tra i sistemi di allerta e risposta della NATO e degli

---

[15] Security and Defence Agenda, *Cyber Security: a transatlantic perspective,* 2010*,* Bruxelles, http://www.securitydefenceagenda.org/Portals/7/2010/Publications/Report_Cyber_security_Final.pdf

[16] Libera traduzione da: *NATO 2020: assured security; dynamic engagement - Analysis and recommendations of the group of experts on a new strategic concept for NATO,* 2010, http://www.nato.int/strategic-concept/expertsreport.pdf

[17] [corsivo aggiunto]: "40. La minaccia cibernetica sta rapidamente crescendo e modificandosi in complessità. Per assicurare alla NATO il costante ed illimitato accesso al ciberspazio e l'integrità dei suoi sistemi critici, noi considereremo la dimensione informatica dei conflitti moderni nella dottrina della NATO e miglioreremo le sue capacità di rilevare, giudicare, prevenire, difendere e riprendersi in caso di attacchi cibernetici contro sistemi di importanza critica per l'Alleanza", *Dichiarazione del Summit di Lisbona fatta dai capi di Stato e di governo che parteciparono all'incontro del Consiglio Atlantico a Lisbona il 20 novembre 2011*, http://www.nato.int/cps/en/natolive/official_texts_68828.htm?mode=pressrelease

[18] [corsivo aggiunto]: "gli attacchi informatici stanno diventando più frequenti, più organizzati e più costosi nei danni che causano alle amministrazioni governative, alle imprese, alle economie e potenzialmente ai trasporti e alle reti energetiche, nonché alle infrastrutture critiche; *questi attacchi possono raggiungere una soglia tale da minacciare la prosperità, la sicurezza e la stabilità nazionale e quella Euro-Atlantica*. *Forze armate straniere e agenzie di intelligence, la criminalità organizzata e/o i gruppi estremisti possono essere ciascuno una fonte di questo tipo di attacchi*". NATO, *Strategic Concept For the Defence and Security of The Members of the North Atlantic Treaty Organisation, 2010*, http://www.nato.int/lisbon2010/strategic-concept-2010-eng.pdf

Stati membri .[19] Nei riferimenti di cui sopra non si possono però ravvisare progressi in termini di chiarificazione di aspetti importanti della questione "*cyber-security*". Al contrario, il Concetto strategico ha in parte deluso le aspettative del Gruppo dei saggi e di altri esperti.[20] Diverse sono le domande senza risposta, riguardo non solo alla valutazione politico-strategica di un attacco, ma anche e soprattutto all'*inquadramento giuridico di elementi che rimettono in causa il tradizionale confine tra sicurezza interna ed esterna e tra competenze civili e militari;* quando, per esempio, una risposta civile è più appropriata di una militare, e viceversa?[21] Nel caso in cui uno Stato non conduca un attacco in prima persona, ma dia indirettamente o direttamente supporto ad un operatore privato, lo Stato in questione è legalmente responsabile per le azioni dei suoi cittadini che credono di operare al suo posto?

La questione dell'attribuzione della responsabilità legale è centrale, dal momento che non è sempre possibile individuare l'origine degli attacchi. L'entità del problema è tale da portare l'Amm. Giampaolo Di Paola, presidente del Comitato Militare della NATO, a ritenere se non sia opportuno che la *cyber-security* venga inclusa tra i compiti fondamentali dell'Alleanza e se non sia quindi il caso di considerare come una fattispecie "art. 5" un attacco cibernetico condotto contro i sistemi informatici di uno Stato membro. [Corsivo aggiunto]: "C'è una convergenza totale tra i Paesi membri sul fatto che la sicurezza del *cyber-spazio è una delle nuove sfide alla sicurezza comune, e che la Nato debba dotarsi di capacità per farvi fronte. L'Art. 5 ha una formulazione chiara, ma su cosa si debba considerare un attacco ai sensi dell'Art. 5 si decide volta per volta*. Non dimentichiamo che finora questo articolo è stato invocato una sola volta, dopo gli attacchi dell'11 settembre, e che nei decenni precedenti nessuno avrebbe pensato che quel tipo di attacco non militare sarebbe rientrato nell'Art. 5. Perciò anche in futuro questo articolo mantiene una sua ampiezza di interpretazione. *Nel caso della cyber-security dipenderà dalle caratteristiche dell'attacco, dalle sue dimensioni ed effetti, e dalla capacità di individuarne gli autori*. Questo vale per la sicurezza cibernetica come per altre minacce asimmetriche, come il terrorismo. Nel paleolitico le armi d'attacco erano le pietre, durante la Guerra Fredda erano le armate sovietiche, l'11 settembre 2001 sono stati aerei civili dirottati dai terroristi, in futuro può essere un attacco missilistico o un attacco cibernetico, o altro ancora".[22]

Così come la NATO, anche l'UE ha incontrato notevoli difficoltà a produrre definizioni coerenti e condivise della dimensione "*cyber-security*". Ciò non toglie tuttavia che si possa entro certi limiti tentare di ricostruire in che modo l'UE interpreti la *cyber-security*. A questo scopo, tuttavia, i cinque documenti menzionati in apertura di capitolo non sono sufficienti. È necessario guardare anche alle politiche di risposta concrete adottate dall'UE, e di lì operare una sintesi.

---

[19] NATO, *Strategic Concept For the Defence and Security of The Members of the North Atlantic Treaty Organisation, 2010*, http://www.nato.int/lisbon2010/strategic-concept-2010-eng.pdf

[20] Si confronti per es. l'opinione dell'Amm. Giampaolo Di Paola, presidente del Comitato militare della NATO, su cui si veda oltre.

[21] Negli Stati Uniti la situazione è meno confusa perché i documenti strategici e di policy contengono delle definizioni più precise e condivise e una chiara divisione delle competenze tra Dipartimento per la Difesa e Dipartimento per la Sicurezza interna (Homeland Security) nella gestione delle questioni del settore cyber.

[22] Alessandro Marrone, *La NATO guarda al futuro*, 2010, http://www.affarinternazionali.it/articolo.asp?ID=1580.

Le politiche UE in materia di *cyber-security* si concentrano soprattutto su due aspetti della c.d. *Network and Information Security* (NIS), una sorta di "macro-categoria" che comprende tutte le iniziative volte a rafforzare la protezione e la "resilienza" (*resilience*, la capacità di resistenza e di recupero) delle reti e delle informazioni. Questi due aspetti o "sotto-categorie" della NIS sono: la protezione delle infrastrutture critiche informatizzate (*Critical Information Infrastructures*, CIIs) e le iniziative di contrasto alla *cyber*-criminalità.

Mettendo insieme l'analisi di questi due ordini di attività con quanto contenuto nei documenti strategici menzionati, dunque, è possibile concludere che le due principali priorità individuate dall'UE in termini di *cyber-security* sono le seguenti:

(1) Infrastrutture basate su tecnologie per le informazioni e le comunicazioni, ovvero le *Information and Communication Technologies*[23] (ICT);

(2) Criminalità cibernetica o *cyber-crime*.

Nel secondo capitolo ci si occuperà più diffusamente delle iniziative adottate dall'UE in relazione a queste priorità. È però il caso di anticipare alcune riflessioni sul carattere e la rilevanza di queste due aree prioritarie di intervento.

(1) Il fattore *cyber*/ICT[24] è alla base della maggior parte delle infrastrutture critiche delle società moderne e può essere non solo un obiettivo diretto di attacchi (intenzionali) o di incidenti (non intenzionali) a *cyber*-infrastrutture/CII, ma anche un tramite per colpire indirettamente le infrastrutture critiche che vi basano la propria operatività (per esempio reti dei trasporti, di distribuzione energetica e delle acque, centrali nucleari, sistema bancario e finanziario).

Ciò determina una sorta di effetto moltiplicatore della rilevanza del problema per ragioni geografiche e funzionali. Geografiche, perché le infrastrutture critiche sono in molti casi transnazionali e dunque richiedono il coinvolgimento di più Stati. Funzionali, perché le interconnessioni delle infrastrutture critiche odierne determinano una interdipendenza in base alla quale le vulnerabilità si trasmettono da un sistema all'altro: ad esempio dal sistema ICT si possono ripercuotere sul sistema elettrico (il collasso di una rete ICT pubblica o privata può coinvolgere la distribuzione elettrica) e viceversa (la mancanza di elettricità può interrompere il funzionamento di reti ICT).

---

[23] La definizione di cosa sia una infrastruttura ICT è un'operazione complessa. E anche le categorie indicate dalla Direttiva 2008/114/CE del Consiglio dell'8 Dicembre 2008 relativa all'individuazione e alla designazione delle infrastrutture critiche europee e alla valutazione della necessità di migliorarne la protezione sono estremamente vaste: "il settore delle "tecnologie dell'informazione e della comunicazione" (ICT) include i sistemi informatici e la protezione della rete; l'automazione e i sistemi di controllo (SCADA); internet; la fornitura di telecomunicazioni su rete fissa; la fornitura di telecomunicazioni su rete mobile; le comunicazioni radio e la navigazione; le comunicazioni e trasmissioni satellitari"nel testo ufficiale italiano del *Libro Verde relativo ad un programma europeo per la protezione delle infrastrutture critiche*, COM (2005) 576, Bruxelles, http://eur-lex.europa.eu/LexUriServ/site/it/com/2005/com2005_0576it01.pdf queste parole sono riportate in inglese.

[24] Gli Stati Uniti hanno una dipendenza dall'ICT ancora più marcata dell'Europa e la sicurezza delle reti informatiche è diventata una top priority al punto che Obama ha dichiarato che le infrastrutture digitali sono un assetto strategico nazionale e la loro difesa è una priorità della sicurezza nazionale; White House, *National Security Strategy*, maggio 2010, p. 27.

Questi effetti-domino geografici e funzionali delle vulnerabilità dei sistemi hanno un altissimo potenziale di impatto, e possono coinvolgere soggetti sia pubblici che privati. Il settore privato è assolutamente in prima linea in qualità di proprietario di infrastrutture e/o gestore della sicurezza delle stesse.[25]

Gli attacchi inoltre possono realizzarsi in termini di interruzioni (*disruptions*), interruzioni parziali e malfunzionamenti, ma anche attraverso intromissioni non manifeste volte a modificare i dati oggetto di scambio all'interno dei sistemi[26], ipotesi questa ben peggiore: si pensi ad esempio all'intrusione nel sistema del controllo del traffico aereo con la diffusione di coordinate errate.

(2) Quello del *cyber-crime* è un ambito per alcuni aspetti più noto a livello europeo di quanto non lo sia la protezione delle infrastrutture critiche, e che gode di una copertura normativa più sviluppata anche in mancanza di categorie univoche e in presenza di aree di sovrapposizione con la protezione delle infrastrutture ICT[27] (cfr. capitolo 2). È da rilevare che l'interesse per il *cyber-crime* è particolarmente elevato per categorie come frodi bancarie, furto di identità e di informazioni (es. spionaggio industriale) e simili che, pur rappresentando casi forse poco eclatanti, arrecano danni patrimoniali ingenti. Inoltre, questo tipo di attacchi statisticamente rappresenta la maggior parte degli attacchi *cyber* ed è perciò percepito come più urgente dai cittadini e dal settore privato (certamente più di questioni considerate remote dall'opinione pubblica, come la *cyber-war*).

Nel *cyber-crime* rientrano poi anche forme terroristiche come reclutamento, propaganda, diffusioni di informazioni, etc.

Come vedremo nel capitolo seguente, l'UE ha adottato politiche ed iniziative con diversa valenza normativa e ha creato differenti strutture di gestione per far fronte ai problemi relativi alla *cyber-security*.

[25] Ad esempio negli Stati Uniti circa l'85% delle reti informatiche è di proprietà e/o è operato dal settore privato.

[26] Come gli attacchi Man-in-the-middle (MITM) volti ad intercettare e manipolare le comunicazioni informatiche fra due o più parti tramite un inserimento nel flusso di dati non noto a queste ultime.

[27] Il settore ICT non è ancora coperto dalla Direttiva 2008/114/CE sulle infrastrutture critiche europee (pur essendo probabilmente prossima una decisione in tal senso).

Tabella 1 - Le minacce alla sicurezza europea nei documenti strategici dell'UE

	Strategia Sicurezza UE (SSE) 2003	**Rapporto sulla SSE 2008**	**Dichiarazione del Consiglio 2008**	**Strategia Sicurezza Interna (SSI) 2010**	**SSI – 5 Tappe 2010**
Terrorismo	✓	✓	✓	✓	✓
Criminalità organizzata	✓	✓	✓	✓	✓
Armi di distruzione di massa	✓	✓	✓		
Cyber	✓	✓	✓	✓	✓
Pandemie	✓	✓		✓	
Pirateria	✓	✓	✓		
Conflitti regionali	✓	✓			
Sicurezza/Dipendenza energetica	✓	✓	✓	✓	
Povertà	✓	✓			
Stati falliti		✓			
Crimine transnazionale				✓	✓
Sicurezza dello spazio			✓		
Disastri naturali o provocati dall'uomo				✓	✓
Cambiamento climatico		✓			
Incidenti stradali				✓	
Sicurezza alle frontiere					✓
Violenza				✓	

Capitolo 2 – La *cyber-security* e l'Unione Europea

Dalla seconda metà dei primi anni duemila, il tema della *cyber-security* ha acquisito una rilevanza crescente per l'Unione Europea. Non poteva essere diversamente, se si pensa che l'economia digitale europea ammonta a oltre 500 miliardi di euro all'anno.[28]

Il numero dei *cyber*-attacchi non accenna a diminuire e nei primi mesi del 2011 le stesse istituzioni comunitarie sono state colpite da due diversi attacchi informatici. Il primo, a gennaio, ha riguardato il sistema di scambio di quote delle emissioni di anidride carbonica, l'*Emissions Trading System* (EU ETS), il mercato in cui le aziende acquistano quote cui corrisponde il tetto massimo di CO_2 che sono autorizzate ad emettere. Dopo diversi accessi non autorizzati ad alcuni registri nazionali, l'attacco si è intensificato e si è arrivati a veri e propri furti di quote a danno di paesi come la Repubblica Ceca (per un valore accertato di circa sette milioni di euro) e l'Austria. La Commissione è stata costretta a sospendere l'ETS per una settimana.[29] Più recentemente, nel marzo 2011, i sistemi informatici della Commissione, del Servizio europeo per l'azione esterna (il "corpo diplomatico" dell'UE) e, in misura minore, del Parlamento europeo sono stati messi temporaneamente fuori uso, impedendo ai funzionari l'accesso alla posta elettronica da terminali esterni agli uffici comunitari.[30]

Problemi simili sono riscontrati dai privati cittadini. Un sondaggio di Eurobarometro ha indicato ad esempio che negli ultimi cinque anni il 78% degli utenti internet ha avuto problemi di sicurezza e che il 65% è stato vittima di spam (messaggi di posta elettronica indesiderati); il 46% (quindi quasi uno su due) ha invece trovato dei virus nel proprio computer.[31]

Se varie e complesse sono le minacce alla sicurezza informatica, altrettanto diversificate devono essere le risposte. Le principali azioni messe in campo finora dall'UE rispondono alla comune esigenza di garantire la sicurezza delle reti e delle informazioni (*Network and Information Security*, NIS): protezione delle infrastrutture critiche informatizzate (*Critical Information Infrastructure Protection*, CIIP); lotta alla *cyber*-criminalità; regolamentazione delle comunicazioni elettroniche (ivi inclusa la protezione della privacy e dei dati personali).[32]

È tuttavia importante sottolineare che sono gli Stati membri ad avere le principali responsabilità in materia di *cyber-security*. Ciò significa che l'UE interviene solo in via sussidiaria, integrando e, dove possibile, armonizzando le iniziative nazionali.

---

[28] Nelie Kroes,*Working together to strenghten cyber-security*, Speech 11/275, 15 aprile 2011.

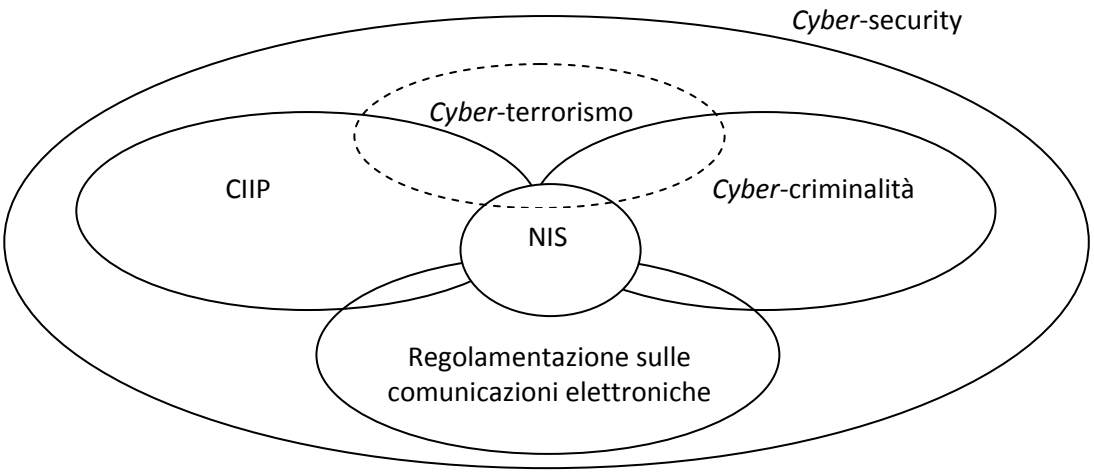
[29] Si veda Kara Segedin, *Cyber attacks stop of transfers in EU ETS registries*, 2011, http://www.theenergyevent.com/energy11/website/NewsDetails.aspx?PressId=pressRe30

[30] Si veda *Cyber attack on European Commission Reported,* 2011, http://www.euractiv.com/en/future-eu/cyber-attack-european-commission-reported-news-503461.

[31] Flash Eurobarometer "Confidence in Information Society", aprile 2009.

[32] Per questo aspetto, non trattato ai fini del presente approfondimento, si faccia riferimento, tra gli altri, alla *Proposta di regolamento del Parlamento europeo e del Consiglio che istituisce un'Autorità europea del mercato delle comunicazioni elettroniche*, COM2007(699), Bruxelles, presentata dalla Commissione europea.

Fig. 1 L'approccio europeo alla *cyber-security*



Fonte: Elaborazione IAI, maggio 2011

La *Strategia per una società dell'informazione sicura* del 2006 definisce la sicurezza delle reti e dell'informazione come "*la capacità di una rete o di un sistema d'informazione di resistere (…) ad eventi imprevisti o atti dolosi che compromettono la disponibilità, l'autenticità, l'integrità e la riservatezza dei dati conservati o trasmessi e dei servizi forniti o accessibili tramite la suddetta rete o sistema*".[33]

Cruciale in tal senso è la protezione delle infrastrutture critiche informatizzate (CIIP) che, come visto nel capitolo 1, o sono infrastrutture critiche di per sé o servono all'operatività di altre infrastrutture critiche.[34] Le CIIP includono dunque "*tutte le attività dei proprietari o degli operatori delle infrastrutture volte ad assicurare il loro funzionamento al di sopra di un livello minimo di servizi in caso di interruzioni, attacchi o incidenti*".[35]

Per quanto riguarda invece la *cyber*-criminalità, non esiste ancora una definizione univoca, a causa soprattutto delle differenze nella legislazione dei vari Stati membri. La definizione, molto generale, che ne fornisce la Commissione in una Comunicazione del 2007, comprende "*gli atti criminali commessi contro reti di comunicazioni elettroniche e sistemi di informazione o avvalendosi di tali reti e sistemi*".[36] Si possono distinguere in particolare: i reati tradizionali come la frode o la

[33] Commissione europea, *Una strategia per una società dell'informazione sicura – "Dialogo, partenariato e responsabilizzazione"* COM(2006)656, Bruxelles, p. 3.

[34] Commissione europea, *Libro verde relativo a un programma europeo per la protezione delle infrastrutture critiche*, COM(2005)576, Bruxelles, Annex I (traduzione dall'inglese degli autori). Il processo di identificazione delle infrastrutture critiche europee avviato con la Direttiva 2008/114 del Consiglio UE ha riguardato finora il settore energetico e dei trasporti. Le ICT saranno la priorità successiva. Sono infatti in corso consultazioni tra gli Stati membri per la definizione dei criteri per la loro identificazione (Cfr. Commissione europea, *Communication on Critical Information Infrastructure Protection – "Achievements and next steps: towards global cyber-security",* COM(2011)163, Bruxelles).

[35] Ibidem.

[36] Commissione europea, *Verso una politica generale di lotta contro la cibercriminalità*, COM(2007)267, Bruxelles, pp. 1-2. Un importante riferimento in materia è anche la Convenzione del Consiglio d'Europa sulla cybercriminalità (2001), presa come modello dalle stesse istituzioni comunitarie. Tuttavia, manca ancora la ratifica di alcuni Stati membri

falsificazione tramite reti elettroniche; la pubblicazione sul web di contenuti illegali (ad esempio materiale pedopornografico); infine, gli attacchi contro i sistemi informatici, come il già citato *Distributed Denial of Service*[37] e la pirateria (ossia l'utilizzo improprio di applicazioni, software o reti informatiche).[38]

Si intuisce dalle definizioni fin qui fornite che, nell'approccio europeo, le iniziative di protezione di reti e infrastrutture e la lotta al *cyber*-crimine sono strettamente correlate tra loro, e in parte si sovrappongono. Ciò comporta che le proposte per il miglioramento delle politiche per la sicurezza contenute in diversi documenti adottati dall'UE negli ultimi anni hanno molti aspetti in comune.

In linea anche con le raccomandazioni contenute nella *Strategia di Sicurezza Interna dell'UE* e dell'Agenda Digitale Europea lanciata nell'agosto 2010[39], due sono gli obiettivi più urgenti: da un lato, accrescere la consapevolezza dei principali rischi connessi alla cyber-security; dall'altro, su un fronte più operativo, migliorare la preparazione e le capacità di risposta europee e nazionali a possibili attacchi o incidenti informatici.

Per quanto riguarda il primo obiettivo, la Commissione Europea sostiene attivamente un maggiore dialogo tra gli Stati membri e tra questi ultimi e le istituzioni comunitarie, così come tra tutti gli attori chiave del settore, sia pubblici che privati. Un primo importante passo in tal senso è stata la creazione di strutture *ad hoc*, come l'Agenzia Europea per la Sicurezza delle Reti e dell'Informazione (*European Network and Information Security Agency*, ENISA). Creata nel 2004 e con sede a Creta[40], l'ENISA è essenzialmente una piattaforma di scambio di informazioni e *best practices* tra le istituzioni UE, le autorità nazionali e le imprese. Può inoltre fornire pareri tecnici sia alle autorità degli Stati membri che alle istituzioni comunitarie.

L'ENISA sembra avere al momento due limiti principali. In primo luogo, dispone di un budget relativamente basso – poco meno di 8 milioni di euro per il 2010 – di cui solo il 25% è destinato alle *core activities*, che includono la gestione di incidenti informatici, campagne di

---

dell'UE. Si veda qui per un aggiornamento al 1 maggio 2011, Consiglio d'Europa, *Convention on Cybercrime*, http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=&CL=ENG.

[37] Si veda nota 14.

[38] Ibidem. Come parte integrante della lotta alla cyber-criminalità, già nel 1999 la Commissione ha varato un programma specifico, Safer Internet, rivolto in particolare a giovani e bambini, con l'intento di rendere più sicura la loro navigazione in rete, accrescendo la consapevolezza dei rischi e contrastando la pubblicazione di materiale illecito. Si veda *Safer Internet programme: Empowering and protecting children online*, http://ec.europa.eu/information_society/activities/sip/index_en.htm

[39] A proposito della Strategia di Sicurezza interna dell'UE, si veda anche Commissione Europea, *La strategia di sicurezza interna dell'UE in azione: cinque tappe verso un'Europa più sicura*, COM(2010)673, Bruxelles. L'agenda digitale dell'UE è invece una delle sette iniziative della Strategia Europa 2020, la quale fissa degli obiettivi per la crescita nell'Unione Europea da realizzarsi entro il 2020. Strumentale in tal senso è l'Agenda digitale che propone una serie di azioni concrete per sfruttare al meglio il potenziale delle ICT per favorire la crescita economica, il progresso e l'innovazione.

[40] Regolamento (CE) n. 460/2004 del Parlamento Europeo e del Consiglio del 10 marzo 2004 che istituisce l'Agenzia europea per la sicurezza delle reti e dell'informazione, GUUE L 077, 13/03/2004. Nel 2008, il mandato di ENISA è stato esteso *à l'identique* fino al 2012.

sensibilizzazione, rapporti con gli Stati membri, etc. Significativamente, invece, oltre il 50% del budget copre i costi del personale (circa 60 funzionari) e delle strutture fisiche.[41]

Un secondo limite è legato al mandato dell'ENISA, che non ha al momento un ruolo operativo e non si occupa di questioni legate al *cyber*-terrorismo o alla *cyber*-criminalità.[42] Tuttavia, la Commissione ha presentato nel settembre 2010 una proposta di direttiva per estendere il mandato dell'ENISA fino al 2017 e per ampliarne le funzioni. Se la direttiva venisse approvata, l'Agenzia verrebbe dotata di una più ampia gamma di strumenti di risposta, diventando così il principale referente europeo nel settore della *cyber-security*, e potrebbe coinvolgere gli Stati membri e altri attori in esercitazioni congiunte.[43]

Anche le iniziative europee contro il *cyber-crime* sono caratterizzate dalla ricerca di dialogo e maggiore cooperazione tra i vari attori interessati. Un ruolo di rilievo è svolto da Europol, l'Ufficio Europeo di Polizia, che ospita la Piattaforma Europea per la *Cyber*-criminalità la cui funzione è favorire la raccolta, lo scambio e l'analisi di informazioni in materia di *cyber*-crimini tra gli Stati membri. L'UE lancerà inoltre a breve uno studio di fattibilità per la creazione di un Centro Europeo per la *Cyber*-criminalità entro il 2013. Nelle intenzioni, il Centro sarà il punto di riferimento europeo per la lotta alla *cyber*-criminalità e contribuirà a rispondere in tempi più rapidi ad un *cyber*-attacco. Gli esiti dello studio di fattibilità saranno alla base di discussioni tra gli Stati membri nel corso del 2012.

Più recentemente, nel quadro del Piano d'Azione per la Protezione delle Infrastrutture Critiche Informatizzate varato dalla Commissione nel 2009[44], sono state incluse due iniziative tese a favorire il dialogo e il miglioramento delle capacità di prevenzione e preparazione dell'UE a incidenti/attacchi informatici.[45]

La prima di queste iniziative è il Forum Europeo degli Stati membri, istituito nel 2009 e sostenuto dall'ENISA, che si è rapidamente affermato come una valida piattaforma di discussione e di scambio di idee tra i ventisette paesi UE. Si riunisce trimestralmente e finora ha dato un notevole impulso al dibattito sulle infrastrutture critiche informatizzate europee, sulle priorità delle politiche UE in ambito *cyber* e allo scambio di *best practices*.

Altrettanto significativa è l'altra iniziativa contenuta nel Piano d'Azione, la *Partnership* Europea Pubblico-Privata per la Resilienza (EP3R) – intendendo con "resilienza" la capacità di un sistema di adattarsi e resistere nel tempo alle condizioni d'utilizzo e garantire così la disponibilità dei servizi erogati. La *Partnership* risponde all'esigenza di incentivare i contatti e la cooperazione tra attori pubblici e privati. Dal momento che i privati possiedono od operano oltre l'80% delle infrastrutture

[41] Per ulteriori riferimenti, si veda ENISA, *Amending budget 01/2010*, http://www.enisa.europa.eu/about-enisa/accounting-finance/files/amending-budget-2010-01/view.

[42] Il ruolo marginale dell'ENISA in caso di un cyber-attacco è stato reso manifesto in occasione dell'ampio attacco informatico in Estonia del 2007, in cui il principale interlocutore operativo in Europa è stata la NATO.

[43] Commissione europea, *Proposta per un regolamento del Parlamento europeo e del Consiglio riguardante l'ENISA* COM(2010) 521, Bruxelles.

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

[45] Commissione europea, *Communication on Critical Information Infrastructure Protection – "Achievements and next steps: towards global cyber-security",* COM(2011)163, Bruxelles.

critiche, i partenariati pubblico-privato sono fondamentali per un'efficace politica di *governance* informatica. In particolare, nell'ambito della EP3R, sono stati istituiti alla fine del 2010 tre gruppi di lavoro che nel corso dell'anno dovranno fornire raccomandazioni in merito a strumenti e risorse necessari per il funzionamento delle reti elettroniche transnazionali e per la loro resilienza, nonché meccanismi di coordinamento in caso di interruzioni informatiche su larga scala.

Con riferimento invece agli aspetti più operativi, le capacità di risposta ad attacchi o incidenti informatici variano sensibilmente tra gli Stati membri UE. Gli sforzi per colmare il divario tra i più e i meno attrezzati si concentrano sulla creazione di capacità (*capacity building*) e addestramento e formazione (*training*), ma soprattutto sulla creazione, in ogni Stato membro, dei *Computer Emergency Response Teams* o CERT. Si tratta di squadre per la risposta ad emergenze informatiche, finanziate da università, enti governativi, o, più recentemente, grandi imprese, e costituite da esperti del settore che svolgono una duplice funzione: da un lato, fornire assistenza immediata in caso di anomalie alle reti elettroniche; dall'altro, svolgere attività di prevenzione, monitoraggio e formazione. Il Piano d'Azione UE per la Protezione delle Infrastrutture Critiche Informatizzate prevede che, entro il 2012, non solo tutti gli Stati membri, ma anche le istituzioni comunitarie si dotino di almeno un CERT.

I CERT sono alla base del Sistema di Allerta e di Scambio di Informazioni che l'ENISA progetta di sviluppare entro il 2013 e hanno un ruolo chiave nelle esercitazioni che vengono regolarmente condotte per testare le capacità informatiche degli Stati membri. Nel novembre 2010 ha avuto luogo per la prima volta, sotto l'egida dell'ENISA, un'esercitazione congiunta a livello europeo, *Cyber Europe 2010*. Vi hanno partecipato esperti degli enti pubblici (ministeri, agenzie regolamentari, CERT) di ventidue Stati membri, i quali si sono dovuti confrontare con oltre trecento attacchi che simulavano una perdita di connessione internet su larga scala con ricadute evidenti sull'erogazione di servizi online di importanza critica in tutta Europa. Per avere un'idea del potenziale impatto di una simile eventualità, si pensi che un attacco può estendersi in dodici paesi in appena dodici secondi.[46] A parere degli organizzatori, l'esercitazione è stata un successo, ma ha anche palesato alcune criticità operative (peraltro già note) che dovranno essere risolte in futuro.

[46] Si veda Cecilia Malmstrom, *It's time to take cyber criminals off line*, Speech/11/260, in occasione della Conferenza sulla cyber-criminalità, organizzata a Budapest il 13 aprile 2011 dalla Presidenza di turno ungherese.

Capitolo 3 La *cyber-security* e l'Italia

Alla pluralità di minacce alla sicurezza informatica l'Italia ha reagito con iniziative in linea con i più recenti orientamenti europei ed internazionali. Gli interventi spaziano da azioni in ambito legale per un adeguamento dell'ordinamento nazionale ai *cyber*-crimini ad iniziative di carattere più operativo, ripartite tra istituzioni centrali e regionali, Forze dell'Ordine, agenzie di informazione e sicurezza e, non da ultimo, importanti attori privati, tra cui Poste Italiane, Enel, Telecom e Banca d'Italia.

L'accresciuta rilevanza della *cyber-security* è testimoniata dalle relazioni annuali del Sistema di Informazione per la Sicurezza della Repubblica (il Sistema è l'insieme delle istituzioni e agenzie nazionali preposte alle attività di intelligence). Nella Relazione 2010, la *cyber-security*, considerata marginale fino a qualche anno fa[47], è inserita invece tra le "sfide crescenti".[48] Il documento attesta che dagli inizi del 2010 il governo considera la minaccia *cyber* non più come mero problema di criminalità, ma come questione di sicurezza nazionale. La relazione termina con un cenno ai *social media,* che seppure non menzionati esplicitamente sono segnalati come possibile strumento di confronto, diffusione di idee e trasferimento di informazioni sensibili di gruppi estremisti interni.[49]

L'aspetto preventivo è di particolare importanza in materia informatica. Un ruolo chiave in questo senso è svolto proprio dal Sistema di Informazione per la Sicurezza Nazionale, in particolare tramite la Divisione INFOSEC dell'Agenzia per l'Informazione e la Sicurezza Esterna (AISE) e la Sezione Controingerenza Telematica dell'Agenzia per l'Informazione e la Sicurezza Interna (AISI). La prima è responsabile dell' "individuazione e della neutralizzazione degli attacchi alle risorse informative dell'Agenzia e del Paese, attuati mediante mezzi informatici".[50] La seconda invece si concentra su minacce emananti all'interno del territorio nazionale, e si basa sulla stretta cooperazione con gli attori strategici pubblici nazionali e i reparti specializzati delle Forze di Polizia. Il Dipartimento Informazioni per la Sicurezza (DIS) ha infine competenze sulla sicurezza delle comunicazioni classificate e su quella delle infrastrutture che le gestiscono.

Contestualmente alle misure preventive, l'iniziativa istituzionale si estende anche agli ambiti legale ed operativo. Sotto il profilo normativo, già dagli anni Novanta si è proceduto ad un progressivo adeguamento dell'ordinamento vigente con l'introduzione di nuove fattispecie criminose, norme più precise in materia di *privacy* e protezione dei dati personali[51], nonché alla firma e ratifica di importanti convenzioni internazionali come la Convenzione del Consiglio d'Europa sul *Cyber-Crime* (firmata dall'Italia nel 2001, ma ratificata solo nel 2008).

---

[47] Ad esempio le relazioni del 2007 e del 2008 inserivano brevemente le minacce cibernetiche in un'ottica di minacce alla sicurezza economica nazionale

[48] Dipartimento Informazioni e Sicurezza (DIS), *Relazione sulla politica dell'informazione per la sicurezza nell'anno 2010*, Presidenza del Consiglio dei Ministri, Roma, 2011, p. 23-35; relazione completa rinvenibile su http://www.sicurezzanazionale.gov.it/web.nsf/pagine/relazione_al_parlamento

[49] DIS, *Relazione sulla politica dell'informazione per la sicurezza nell'anno 2010*, cit., p. 59.

[50] COPASIR, *Relazione sulle possibili implicazioni e minacce per la sicurezza nazionale derivanti dallo spazio cibernetico,* Camera dei Deputati/Senato della Repubblica, Roma, 2010, p. 85, su http://www.parlamento.it/service/PDF/PDFServer/DF/234494.pdf.

[51] Per una disamina più approfondita dell'adeguamento dell'ordinamento italiano si veda COPASIR, *Relazione sulle possibili implicazioni e minacce per la sicurezza nazionale derivanti dallo spazio cibernetico,* cit., pp. 62-66.

Dal punto di vista istituzionale, le responsabilità sono divise tra vari ministeri, le cui competenze specifiche non è sempre semplice individuare. Un ruolo generale di coordinamento e supervisione nel settore della sicurezza delle reti e dell'informazione spetta al Dipartimento delle Comunicazioni del Ministero dello Sviluppo Economico. Tra le varie iniziative e nell'ottica del miglioramento della cooperazione e del dialogo interministeriale, quest'ultimo ha creato nel 2003, con i Ministeri dell'Interno e della Giustizia, l'Osservatorio Permanente per la Sicurezza e la Tutela delle Reti e delle Comunicazioni, erede di un gruppo di lavoro simile istituito già nel 1998. L'Osservatorio ha il compito di monitorare gli sviluppi tecnologici e normativi degli aspetti più legati alla sicurezza del settore telecomunicazioni. Significativamente, ne fanno parte, oltre agli esperti del Ministero dello Sviluppo Economico, anche rappresentanti del Ministero della Difesa e dei Dipartimenti Funzione Pubblica e Digitalizzazione e Innovazione Tecnologica del Ministero per la Pubblica Amministrazione e l'Innovazione.[52]

Per quanto riguarda il contrasto operativo alle forme ordinarie di *cyber-crime* le competenze sono divise tra Guardia di Finanza, Carabinieri e Polizia di Stato.

La Guardia di Finanza si occupa di sicurezza informatica mediante il Nucleo Speciale Frodi Telematiche anche noto come "GAT", ovvero Gruppo Anticrimine Tecnologico.[53] Per i Carabinieri è invece responsabile il Raggruppamento Investigazioni Scientifiche e in particolare il Reparto Tecnologie Informatiche.[54]

All'interno della Polizia di Stato è la Polizia Postale e delle Comunicazioni[55] che ha competenza sul *cyber-crime*[56], occupandosi principalmente di pedopornografia, *cyber*-terrorismo, *copyright* e "diffusione illegale di file"[57], *hacking*[58], protezione delle infrastrutture critiche[59], *e–banking*, giochi e scommesse *on line*.

All'interno della Polizia Postale sono poi presenti ulteriori strutture in materia di *cyber-crime* con funzioni soprattutto di natura preventiva. Queste includono l'Unità di Analisi sul Crimine Informatico (UACI)[60], che affianca gli operatori della Polizia con ricerche e studi sul fenomeno della

[52] Si veda *Osservatorio permanente per la sicurezza e la tutela delle reti e delle comunicazioni,* http://www.sviluppoeconomico.gov.it/index.php?view=article&catid=686%3Apresentazioni&id=2017543%3Aosservatorio-permanente-per-la-sicurezza-e-la-tutela-delle-reti-e-delle-comunicazioni-&format=pdf&option=com_content

[53] *Guardia di Finanza – GAT – Nucleo Speciale Frodi Telematiche*, http://www.gat.gdf.it/sito_php/index.php

[54] *Arma dei Carabinieri – Indagini scientifiche*, 2008, http://www.carabinieri.it/Internet/Arma/Oggi/RACIS/

[55] Creata nel 1981, Polizia Postale e delle comunicazioni, *La Storia*, 2010, http://www.poliziadistato.it/articolo/view/984/

[56] Questa specialità della Polizia è articolata su 20 compartimenti regionali e 80 sezioni provinciali, coordinati a livello centrale dal servizio Polizia delle Comunicazioni; ha un organico di circa 2.000 uomini. Dati su Polizia Postale e delle comunicazioni, *Attività e organizzazione*, 2010, http://www.poliziadistato.it/articolo/view/978/

[57] Polizia Postale e delle comunicazioni, *Attività e organizzazione*, 2010, http://www.poliziadistato.it/articolo/view/978/

[58] Ed anche l'utilizzo della rete per " danneggiare o per colpire […] obiettivi a essa correlati", Polizia Postale e delle comunicazioni, *Attività e organizzazione*, 2010, http://www.poliziadistato.it/articolo/view/978/

[59] Come indicato dal decreto del Ministro dell'Interno del 9 gennaio 2008

[60] Polizia delle Comunicazioni, *Unità di analisi sul crimine informatico* (*Computer crimes analysis unit),* 2010*,* http://www.poliziadistato.it/articolo/986-Unita_di_analisi_sul_crimine_informatico_Computer_Crime_Analysis_Unit/

criminalità informatica, e il Centro Nazionale per il Contrasto alla Pedopornografia su Internet (CNCPO)[61].

La Polizia di Stato collabora inoltre regolarmente con partner internazionali come l'Organizzazione per la Cooperazione e lo Sviluppo Economico (OCSE), il sottogruppo *high tech crime* del G8, Europol, Interpol, ed alcuni soggetti privati.[62] Dal 2009 la Polizia è il punto di contatto nazionale all'interno della rete di cooperazione istituita dai paesi firmatari della Convenzione sul *Cyber-crime* per facilitare la cooperazione e lo scambio di informazioni a livello internazionale.

Come visto in precedenza, una componente fondamentale dell'approccio europeo alla sicurezza informatica, su cui si concentrano le principali raccomandazioni delle istituzioni comunitarie, è la protezione delle infrastrutture critiche per l'informazione o CIIP. L'azione italiana si inserisce a pieno, seppure con qualche lentezza, nel contesto europeo. In ottemperanza al Programma Europeo per la Protezione delle Infrastrutture Critiche (*European Programme for Critical Infrastructure Protection*, EPCIP), dal 2007 è attivo presso l'Ufficio del Consigliere Militare del Presidente del Consiglio il "Tavolo PIC" (Protezione Infrastrutture Critiche), cui partecipano vari dipartimenti della Presidenza del Consiglio (PCM) e vari ministeri interessati.[63] Il Tavolo PIC è responsabile, tra le altre cose, di supervisionare l'attuazione della direttiva comunitaria sulle infrastrutture critiche, recepita nel nostro ordinamento nel gennaio 2011. Inoltre, dal 2009, l'Ordinanza del Presidente del Consiglio n. 3836 del 2009 ha creato la Segreteria di Coordinamento Interministeriale per le Infrastrutture Critiche (SCIIC), per assicurare coerenza e sinergia tra le attività delle amministrazione che si occupano di infrastrutture critiche.

---

[61] Polizia di Stato, *Centro Nazionale per il contrasto alla pedo-pornografia su internet*, 2006, http://www.poliziadistato.it/articolo/455-Centro_nazionale_per_il_contrasto_alla_pedo_pornografia_su_Internet/

[62] Ad esempio Il 23 novembre del 2010 è stato concluso un accordo con la società (privata) di sicurezza informatica Symantec, come su Polizia di Stato, *Commissariato di PS online*, http://www.commissariatodips.it/news/newsstanza.php?straidtip=5&strparent=10&strpercorso=12&strdoc=76

[63] Gli attori istituzionali coinvolti sono i seguenti: PCM - Dipartimento della Protezione Civile; PCM- Dipartimento per il Coordinamento delle Politiche Comunitarie; PCM - Dipartimento per l'Innovazione e le Tecnologie; PCM – Dipartimento per l'Informazione e l'Editoria; PCM - Dipartimento per gli Affari Giuridici e Legislativi; PCM – Dipartimento per le Risorse Strumentali; PCM - DigitPA (ex CNIPA); PCM – Dipartimento Informazioni per la Sicurezza: PCM – Agenzia per le Informazione per la Sicurezza Esterna; PCM - Agenzia per le Informazione per la Sicurezza Interna; Ministero degli Affari Esteri; Ministero dell'Interno; Ministero della Difesa;Ministero delle Infrastrutture e dei Trasporti; Ministero dello sviluppo Economico e Ministero della salute.
Luisa Franchina, *Infrastrutture critiche*, 2010, http://www.difesa.it/NR/rdonlyres/F5994928-BFA2-4BC6-A16E-197A2F5427D5/20694/05_Franchina.pdf, Luisa Franchina, *Infrastrutture critiche: lo stato dell'arte*, 2010, http://www.aipsi.org/wp-content/uploads/2010/11/IC-Franchina.pdf, *Ordinanza del Presidente del Consiglio dei Ministri, n. 3836 del 30 dicembre 2009: disposizioni urgenti in materia di protezione civile*, 2009, http://www.protezionecivile.it/jcms/it/view_leg.wp?contentId=LEG12453.

Fig. 2 L'assetto italiano attuale in materia di protezione delle infrastrutture critiche *(fonte http://www.aipsi.org/wp-content/uploads/2010/11/IC-Franchina.pdf, 2010)*

A livello operativo è interessante notare che la Polizia Postale si è vista attribuire competenze anche in materia di protezione delle infrastrutture per l'informazione critiche, che vanno ad aggiungersi a quelle relative al *cyber-crime* nel senso più stretto del termine. Dal 2009 la Polizia Postale gestisce infatti il Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche (CNAIPIC)[64], il cui compito è "la prevenzione e la repressione dei crimini informatici, di matrice comune, organizzata o terroristica, che hanno per obiettivo le infrastrutture informatizzate di natura critica e di rilevanza nazionale"[65]. Per perseguire i suoi scopi il CNAIPIC dispone di una sala operativa aperta 24 ore su 24 nonché di collegamenti esclusivi fra il Centro e le infrastrutture critiche. Specializzato anche in settori come il contrasto al *cyber-crime*, al *cyber*-terrorismo e allo spionaggio industriale, il CNAIPIC si articola in un settore operativo ed in uno tecnico.

Per un'efficace gestione delle emergenze informatiche, nonché per la protezione delle infrastrutture critiche informatizzate, è indispensabile disporre di una valida rete di CERT (cfr. capitolo 2), la cui creazione a livello nazionale ed europeo è stata più e più volte raccomandata da Bruxelles. L'Italia sembra aver raggiunto buoni risultati, potendo contare su nove CERT pubblici e privati. A livello istituzionale, sia la PCM che il Ministero della Difesa dispongono di un proprio CERT, che si occupa di assistere gli utenti riguardo alla protezione delle reti telematiche svolgendo

[64] Come indicato dall'articolo 3 del decreto del Ministro dell'Interno 9 gennaio 2008, su Polizia delle Comunicazioni, *CNAIPIC – Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche*, 2010, http://poliziadistato.it/articolo/18494/

[65] Polizia delle Comunicazioni, *CNAIPIC – Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche*, 2010, http://poliziadistato.it/articolo/18494/

nel contempo un ruolo di informazione nel campo della sicurezza informatica. Non mancano poi CERT regionali, di privati (Enel, Telecom) ed addirittura uno della Conferenza Episcopale Italiana.[66]

I privati, come università o associazioni, gestiscono iniziative più limitate, tra cui campagne di sensibilizzazione (anche di concerto con le istituzioni comunitarie).[67] Altri hanno un ruolo di maggiore rilievo, in qualità di gestori di infrastrutture critiche cruciali. Si pensi ad esempio al ruolo dell'Associazione Bancaria Italiana e della sua struttura ABI LAB in un settore critico e tra i più sensibili alle infiltrazioni delle reti criminali informatiche come quello bancario.[68] Altrettanto rilevante è il ruolo di Poste Italiane, protagonista tra l'altro di un'ambiziosa *partnership* pubblico-privato, che dimostra come anche in Italia questa strada stia venendo privilegiata per la protezione delle infrastrutture critiche. Si tratta in questo caso dell'accordo fra la Polizia Postale, Poste Italiane e il Secret Service[69] statunitense[70] che nel 2009 ha creato la *European Electronic Crime Task Force* (EECTF). Scopo di questa iniziativa è di migliorare il contrasto al *cyber-crime* grazie ad una interazione più stretta fra attori pubblici e privati. È la prima iniziativa italiana in questo campo, e, aspetto rilevante, aspira a coinvolgere altri partner europei.

[66] ENISA, *Italy country report,* 2010, http://www.enisa.europa.eu/act/sr/files/country-reports/Italy.pdf o Domenico Vulpiani, *La cyber threat alle infrastrutture critiche in Italia: punto di situazione ed azione di contrasto*, 2010, http://www.fondazioneicsa.it/UserFiles/File/Relazione%20Domenico%20Vulpiani.pdf

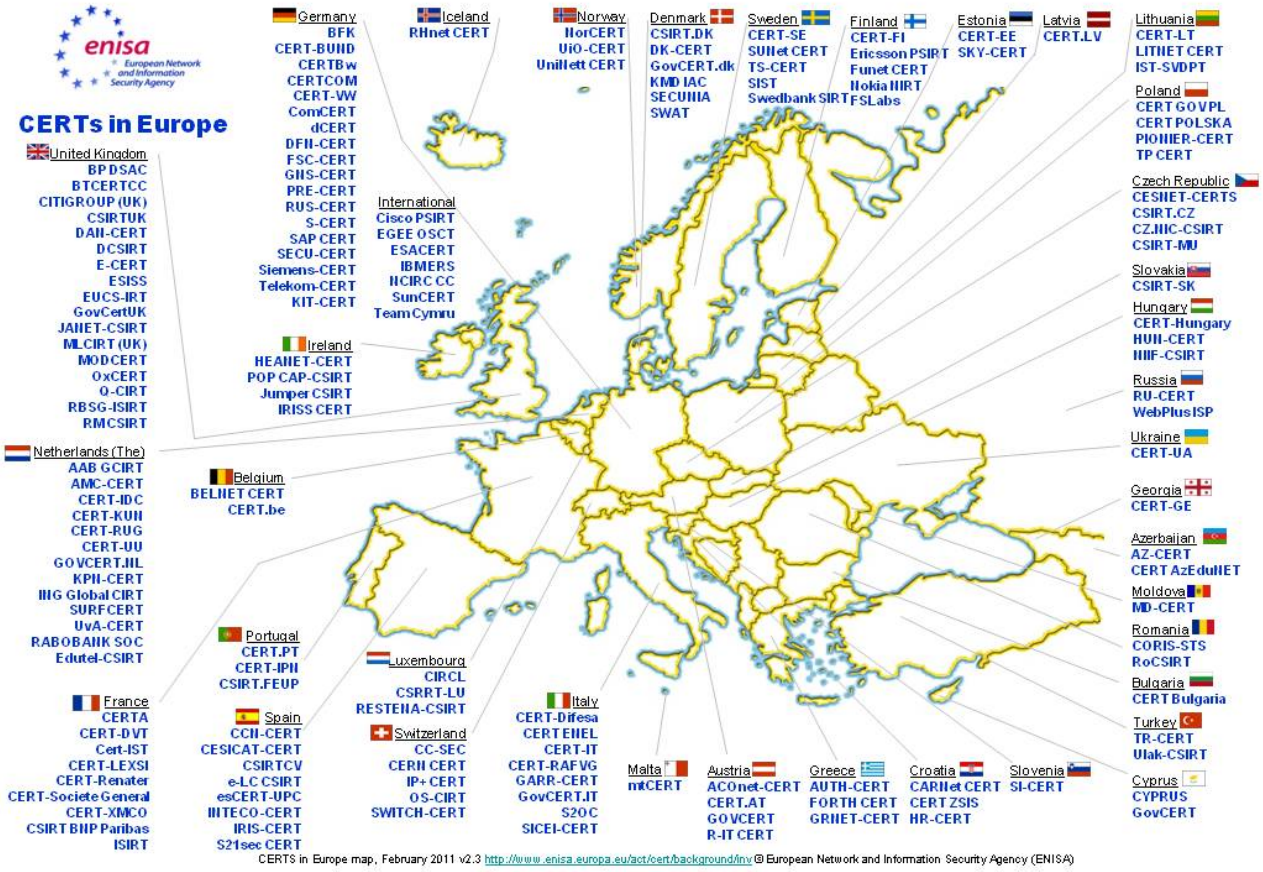
[67] Un esempio è EASY4, campagna di sensibilizzazione per un uso consapevole e sicuro di internet e dei cellulari da parte dei ragazzi. E' gestito da Adiconsum e Save the Children e finanziato dalla Commissione europea nell'ambito del programma Safer Internet.

[68] COPASIR, *Relazione sulle possibili implicazioni e minacce per la sicurezza nazionale derivanti dallo spazio cibernetico,* cit., pp. 78-82.

[69] Il Secret Service USA non è, contrariamente a quanto può far pensare il suo nome, un'agenzia di spionaggio. Si occupa invece della protezione del Presidente e Vice-Presidente e delle loro famiglie; di quella dei candidati alle presidenziali a partire da 120 giorni prima l'elezione; degli ex Presidenti (per un certo lasso di tempo); nonché dei Capi di Stato in visita negli USA. Il Secret Service è anche attivo nel contrasto alla frode valutaria, altre varietà di frodi e furti finanziari.

70 Poste Italiane, *Cybersecurity Internazionale*, http://salastampa.poste.it/uploaded_files/G8_cartellastampa04.pdf, United States Secret Service, *New task force to combat transnational cyber crime,* 2009, http://www.secretservice.gov/press/GPA05-09_EuropeanECTF.pdf

Fig. 3 I CERT nell'UE



Fonte:http://www.enisa.europa.eu/

Capitolo 4 – Raccomandazioni politiche e conclusioni

È molto difficile, se non impossibile, trarre delle conclusioni univoche per una problematica dai confini sfuggenti e in rapida evoluzione e che, allo stato attuale, sembra sollevare domande più che fornire risposte. Tuttavia iniziare a porsi in maniera condivisa gli interrogativi giusti è un punto di partenza.

Alla luce di quanto illustrato nei capitoli precedenti la cosa più utile sembra essere individuare alcune possibili vie di progresso per l'Italia, *in primis* nel contesto UE, ma anche sul piano bilaterale e internazionale, vista la natura transnazionale della dimensione *cyber*. Proprio questo carattere transnazionale per il quale le vulnerabilità non hanno confini geografici impone una cooperazione quanto più comprensiva ed internazionale possibile.

In ambito europeo va ricordato che, anche se l'azione UE è un chiaro valore aggiunto per tutti quegli aspetti che richiedono una *governance* di fenomeni transnazionali e di armonizzazione delle politiche nazionali, questa resta una competenza di natura sussidiaria. La responsabilità primaria nella gestione della problematica è affidata agli Stati.

Le forme di cooperazione tra le varie istituzioni e agenzie italiane e tra queste ultime e soggetti esteri devono svolgersi su diversi livelli:

a) urgenza particolarmente urgente è l'*aspetto terminologico e concettuale*. È necessaria un'armonizzazione in un settore che presenta numerosi vuoti, ambiguità, sovrapposizioni. Questo è vero a livello italiano, ma anche a livello europeo – proprio a causa dei diversi ordinamenti e culture nazionali – ed in tal senso l'UE deve effettuare uno sforzo maggiore rispetto, ad esempio, agli Stati Uniti, che sono avanti nella trattazione della materia al punto da influenzare, con la loro prevalenza in termini di fonti, lo stesso dibattito europeo relativo alla *cyber-security*.[71]

b) Il suddetto aspetto costituisce un'imprescindibile condizione per l'identificazione di *chiare fattispecie legali* e per la *produzione* e *sistematizzazione normativa,* ivi incluse le competenze dei vari attori coinvolti.

   b.1) La cooperazione tra agenzie di sicurezza è fondamentale, perché le giurisdizioni hanno confini territoriali che il *cyber*-spazio non ha. È difficile attribuire le responsabilità, sia per la difficile, se non impossibile, tracciabilità di eventi *cyber*, sia per la mancanza di paradigmi di riferimento per una chiara attribuzione delle responsabilità legali.

   A tale proposito bisogna ricordare che l'Italia è stata tra gli Stati che hanno ratificato la Convenzione del Consiglio d'Europa sul *Cyber-crime* (2001). Numerosi Stati europei vi aderiscono e il fatto che tra i suoi scopi preveda una "*common criminal policy*" conferma l'utilità dello strumento. Tuttavia esistono degli aspetti potenzialmente invalidanti. Non

[71] Secondo Europol, la preponderanza delle fonti statunitensi sta influenzando la prospettiva europea. Si veda Europol, *High Tech crimes within EU: old crimes new tools, new crimes new tools,* 2007, http://www.europol.europa.eu/publications/Serious_Crime_Overviews/HTCThreatAssessment2007.pdf.

sono parte della Convenzione Stati come Russia, Cina, India e Brasile, ed è improbabile che queste nazioni si decidano a cooperare in mancanza di chiari accordi sulle questioni militari e politiche nel *cyber*spazio.[72]

Per gli Stati europei, inclusa l'Italia, va riconosciuto il ruolo centrale di Europol, che nei prossimi anni dovrebbe venire rafforzato ulteriormente, ad esempio con la creazione del Centro Europeo per la *Cyber*-criminalità (cfr. capitolo 2).

Queste iniziative possono contare anche su una base legale rafforzata, introdotta dall'Art. 83 del Trattato di Lisbona, che dispone la possibilità di "stabilire norme minime relative alla definizione dei reati e delle sanzioni in sfere di criminalità particolarmente grave che presentano una dimensione transnazionale derivante dal carattere o dalle implicazioni di tali reati o da una particolare necessità di combatterli su basi comuni", includendo tra questi la criminalità informatica.

La scelta, anche italiana, di investire risorse sul *cyber-crime* appare opportuna se non obbligata, anche perché si tratta di contrastare le attività criminose che arrecano ingenti danni patrimoniali, e che statisticamente rappresentano la gran parte degli eventi aggressivi *cyber* e sono perciò maggiormente sentiti dai cittadini e dal settore privato.

b.2) In tale contesto, se si considerano situazioni in cui vi sia, potenzialmente, un coinvolgimento ostile da parte di Stati (cfr. capitolo 1), si devono indagare quali siano le condizioni che impongono il passaggio dalla sicurezza interna all'applicazione del diritto di guerra. Quale è la soglia di preoccupazione politica che rende equiparabile un attacco *cyber* ad un attacco armato? Le tradizionali categorie del diritto internazionale necessitano evidentemente di un aggiornamento, ma è difficile stabilire in che forma viste le incertezze che ancora permangono su tutto quello che ha che fare con la *cyber-security*. Si pone la questione di aggiornare lo stesso concetto di sovranità che nel contesto cyber non può essere legata alla territorialità (sovranità territoriale), ma, in maniera più adeguata, alle diverse "funzioni" che si espletano nel *cyber*-spazio. In altre parole si tratterebbe di "confini cibernetici funzionali", classificati cioè in base alle tipologie di attività svolte nel *cyber*-spazio: sovranità funzionale e giurisdizione funzionale per le quali però le possibilità di controllo appaiono incerte.

A questi interrogativi l'Italia sembra porre la giusta attenzione.

È da rilevare in particolare che lo Stato Maggiore della Difesa, III Reparto – Centro Innovazione Difesa (CID) si è con successo candidato a guidare la sezione relativa agli aspetti legali *cyber* nel quadro del *Multinational Experiment 7 – Access to the Global Commons* sponsorizzato dallo US JFCOM – J9. Quest'iniziativa, che durerà fino a tutto il 2012, rappresenta per il team italiano di ricerca un importante coinvolgimento

[72] James A. Lewis (CSIS), The international Context for Cybersecurity, Session on Cybersecurity, The Trilateral Commission, 2011 Washington Meeting – April 2011.

permanente di attori provenienti dalle forze armate e di polizia, dal settore privato e dal mondo accademico e della ricerca.

La relazione 2010 del Comitato Parlamentare per la Sicurezza della Repubblica (COPASIR) (2010)[73] raccomanda che l'Italia si faccia promotrice di "un'azione di costruzione del consenso internazionale, volta a promuovere nelle più alte sedi multilaterali la redazione di un primo testo per un Trattato per il Contrasto alle Minacce Cibernetiche Statuali".[74]. Ma se questa iniziativa avrebbe il merito di colmare un vuoto normativo, è da rilevare che, come visto, non corrisponde ad un problema quantitativamente preponderante (come quello del *cyber-crime*). Inoltre, secondo alcuni autorevoli commentatori un trattato, in particolare sul controllo delle armi, potrebbe avere oggi un impatto limitato.[75] Inoltre cos'è un'arma nel *cyber*-spazio? Un adolescente con capacità di *hacking*/intrusione? La verifica non sembra possibile.[76]

c) I due punti precedenti sull'armonizzazione terminologica e normativa sono tra i fattori che permettono ad uno Stato di potersi porre come un valido interlocutore sul piano internazionale. Lo stesso dicasi per l'Unione Europea dove invece – a fronte della nomina nel 2009 di un coordinatore per la *cyber-security* presso l'Ufficio Esecutivo del Presidente USA Barack Obama – l'opportunità di valutare la creazione di un omologo europeo, un "Mr. *Cyber-security*" come proposto dall'allora Commissario Europeo per la Società dell'Informazione e i Media (oggi "Agenda Digitale") Viviane Reding, non ha avuto seguito.[77]

   È però da rilevare che le recenti iniziative di potenziamento dell'ENISA (cfr. capitolo 2) potrebbero trasformarla nel punto di riferimento di Stati membri e istituzioni UE per tutte le questioni legate alla *cyber-security*, in particolare l'armonizzazione di iniziative nazionali a diversi livelli: terminologico, normativo, operativo.

d) Un altro aspetto importante è un'*attenzione permanente politico-istituzionale*. In Italia la Presidenza del Consiglio ha accentrato su di sé diverse responsabilità di *cyber-security* (cfr. capitolo 3). Una maggiore – e continua – attenzione a livello politico-istituzionale è necessaria anche sul piano internazionale. È un esempio incoraggiante in questo senso il fatto che negli ultimi vertici UE-USA alla *cyber-security* si sia dato sempre più spazio. Nel 2009 il vertice USA-UE ha per la prima volta si riconosciuto la *cyber-security* come sfida globale (non bilaterale, né regionale), segnalando nel contempo l'intento di: "rafforzare il

[73] COPASIR, *Relazione sulle possibili implicazioni e minacce per la sicurezza nazionale derivanti dallo spazio cibernetico,* cit.

[74] "(…) uno strumento sovranazionale, cioè, in grado di contrastare la proliferazione dei centri e delle modalità offensive e, senza intaccarne la libertà di utilizzo e di accesso, la possibilità di utilizzare la rete quale strumento militare non convenzionale. Tale obiettivo potrebbe essere raggiunto anche attraverso la creazione di un Centro internazionale per la repressione e il controllo della proliferazione degli strumenti cibernetici offensivi".

[75] James A. Lewis (CSIS), The international Context for Cybersecurity, Session on Cybersecurity, The Trilateral Commission, 2011 Washington Meeting – April 2011.

[76] *Ibidem*.

[77] Si veda *EU Commissioner Reding calls for preventive action to make the EU resilient against cyber attacks*, memo 09/199, 2009, http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/09/199.

[…] dialogo [USA-UE] per individuare e rendere prioritari i settori nei quali sia possibile intervenire congiuntamente per costruire un'infrastruttura che sia sicura, resistente e affidabile per il futuro".[78] Per quanto apprezzabili siano le intenzioni, esistono punti di contatto permanenti e dedicati a livello dei governi? Il vertice USA-UE 2010 ha creato un Gruppo di lavoro USA-UE sulla Sicurezza ed il Crimine Informatico, la cui composizione e i cui compiti sono però ancora sconosciuti. Valutare la sua reale efficacia richiederà tempo e la sua stessa denominazione, implicando la distinzione fra sicurezza e criminalità informatica come due differenti ambiti di attività, già desta alcune preoccupazioni sulla chiarezza e l'obiettivo del mandato. Il Gruppo di lavoro dovrebbe riferire sui risultati raggiunti al vertice USA-UE 2011. Probabilmente lo strumento potrebbe essere migliorato. Ad esempio perché non creare, a beneficio di quella attenzione politico-istituzionale di cui sopra, un Consiglio USA-UE sulla *Cyber-security* sul modello del Consiglio USA-UE sull'Energia pure stabilito a livello ministeriale nello stesso quadro istituzionale?[79]

e) Il livello *tecnico-operativo* è importante almeno quanto il livello politico-istituzionale.

e.1) Centrali in quest'ambito sono i CERT (cfr. capitoli 2 e 3). Pertanto andrebbe sostenuta l'armonizzazione ed elevazione degli standard dei CERT in Europa, e la creazione di una rete di tutti i CERT nazionali e i CERT delle istituzioni europee entro il 2012[80] con la graduale creazione di una governance UE-centrica dei CERT sotto responsabilità dell'ENISA[81]. Ciò senza dimenticare che la stessa ENISA sostiene la creazione di un CERT UE per gestire le minacce ICT che interessano l'Unione. Va ricordato che quasi tutti i CERT sono nazionali, mentre quelli internazionali sono molto pochi, con l'importante eccezione del *Forum of Incident Response and Security Teams* (FIRST).[82] I CERT hanno poi il valore aggiunto di includere insieme attori privati e pubblici (cfr oltre, lettera i)) e secondo una terminologia più recente sono indicati come *Computer Security and Incident Response Teams* (CSIRT). Ciò significa che oltre ai servizi di reazione (risposta agli incidenti), queste strutture di solito forniscono altri servizi di sicurezza per i loro utilizzatori, come l'allertamento, la consulenza e la formazione in materia di *cyber-security*. Nel corso degli anni i CERT/CSIRT si sono dunque sviluppati in fornitori di alta qualità di servizi di sicurezza.[83]

Anche sul fronte del *cyber*-crimine esistono iniziative valide, come l'italo-statunitense *European Electronic Crime Task Force* (EECTF) (cfr. capitolo 3) che, come visto, ha un punto di forza nella vocazione ad aprirsi ad altri membri europei.

---

[78] Libera traduzione da: *2009 EU-US Summit declaration*, 2009, http://eeas.europa.eu/us/sum11_09/docs/declaration_en.pdf

[79] *EU-U.S. Security Strategies: comparative scenarios and recommendations*, http://www.iai.it/pdf/Economia_difesa/EU-US-security-strategies.pdf

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

[81] Così riportando in un quadro istituzionale europeo alcune iniziative informali come lo European Government CERTs (EGC) group, 2011,http://www.egc-group.org/.

[82] Forum of Incident Response and Security Teams *What is FIRST?*, 2011,http://www.first.org/about/

[83] ENISA, *Cert factsheet,* http://www.enisa.europa.eu/act/cert/background/cert-factsheet

e.2) i CERT, come visto sopra, sono alla base del Sistema Europeo di Allerta e di Scambio di Informazioni (*European Information Sharing and Alert System*, EISAS) che l'ENISA progetta di sviluppare entro il 2013 (cfr. capitolo 2).

È importante ribadire che tutti gli aspetti tecnico-operativi fin qui menzionati o di altra o nuova iniziativa devono poter contare su quadri procedurali e legali adeguati pena la loro inefficacia.

f) Le *esercitazioni* costituiscono un fattore imprescindibile tanto a livello politico-istituzionale che tecnico-operativo (con coinvolgimento dei CERT) ed hanno un ruolo chiave a livello nazionale, europeo ed internazionale.

Si potrebbe valutare l'opportunità di incrementare e rendere permanenti gli scambi tra CERT europei e non (ad es. i CERT USA) con la condivisione di *lessons learned* così come rafforzando la spinta "dal basso" (*bottom-up*) che il settore tecnico-operativo può imprimere alla creazione di politiche condivise.

Per la stessa ragione le esercitazioni andrebbero tenute con maggiore regolarità e dovrebbero essere maggiormente valorizzate le lezioni apprese. Indicativo in questo senso è il rapporto conclusivo dell'ENISA sull'esercitazione *Cyber Europe 2010* (cfr. capitolo 2), che sottolinea innanzitutto la necessità di armonizzare le procedure operative dei vari Paesi membri. Potrebbe essere di aiuto in tal senso l'elaborazione di un piano europeo contro i *cyber*-incidenti, che dovrebbe essere completato entro il 2012. I privati, del tutto assenti in *Cyber Europe 2010*, dovrebbero essere coinvolti regolarmente nelle esercitazioni. Queste ultime dovrebbero poi essere ripetute nel breve-medio termine, e lo scambio delle lezioni apprese dovrebbe diventarne una parte integrante a tutti gli effetti.[84]

Cyber Europe 2010, che ha riguardato eventi che si ripercuotono sulla disponibilità di internet in diversi Stati europei[85], è stato la prima esercitazione pan-europea sulla protezione delle CII. Molto simili sono gli scenari di riferimento della serie di esercitazioni statunitensi *Cyber Storm* gestite dal Dipartimento per la Sicurezza Interna (*Department of Homeland Security*, DHS), la cui terza edizione (2010) ha simulato eventi *cyber* su larga scala e attacchi *cyber* contro il governo, le infrastrutture critiche nazionali e le risorse essenziali. Nonostante l'evidente compatibilità tra le due esercitazioni, al momento mancano esercitazioni congiunte ENISA-DHS sulla protezione delle CII.

g) Lo *sviluppo di sinergie* andrebbe ricercato e valorizzato. Ad esempio, l'attuale ruolo di ENISA – quindi al di là della prospettiva di allargarne il mandato ad esempio al *cyber-crime* (capitolo 2) – sembra limitato solo a garantire la continuità economica e commerciale. Tuttavia questa continuità ovviamente interessa infrastrutture pubbliche e private, e servizi

[84] Si veda ENISA *Cyber Europe 2010, Evaluation report*, 2011, http://www.enisa.europa.eu/act/res/cyber-europe-2010/cyber-europe-2010-report/at_download/file .

[85] Per ulteriori dettagli su Cyber Europe 2010, si veda ENISA*, Q&As on the first pan-European Cyber-security Exercise*, at http://www.enisa.europa.eu/media/news-items/faqs-cyber-europe-2010-final.

e funzioni che hanno un impatto diretto sui cittadini. In altre parole c'è una *sinergia fra le dimensioni "economiche" e "sociali"* della sicurezza delle reti e delle informazioni (*Network and Information Security*, NIS).

h) Gli investimenti nella ricerca e nello sviluppo (R&S) dovrebbero essere incrementati con un forte apporto dei privati. Ad esempio, se si considera l'ultimo bando in materia di sicurezza (2011) del 7mo Programma Quadro della Commissione Europea (il principale strumento di finanziamento della ricerca dell'UE), a fronte di oltre 220 milioni di euro da spendere su circa 50 tematiche, *solamente una* era relativa al *cyber* ("*Cyber*-attacchi contro le infrastrutture critiche").[86] Sempre a livello europeo esistono anche diversi finanziamenti per ricerche nell'ambito delle infrastrutture critiche (anche informatizzate) gestiti nel quadro del Programma Europeo per la Protezione delle Infrastrutture Critiche (*European Programme for Critical Infrastructure Protection*, EPCIP). È poi da considerare che molto spesso in ricerche formalmente dedicate a settori più generali (ad esempio finanziamenti sulla cooperazione transatlantica della Direzione Generale Relazioni Esterne[87], o altre tematiche come lo sviluppo del mercato della sicurezza) si finisce con il prendere in considerazione il settore *cyber*. Un'altra notazione nel campo della R&S è di nuovo sulla ricerca di sinergie in aree parzialmente sovrapposte. In particolare, sarebbe opportuna una più profonda riflessione sulle possibili sinergie tra tecnologie *cyber* civili, militari e di uso 'duale' (cioè sia militare sia civile).[88]

i) *Coinvolgimento degli* stakeholders *nella formulazione delle politiche* in tutti campi del settore *cyber*: monitoraggio, investimenti, contromisure, armonizzazione terminologica, normativa, etc. Almeno tre sono le categorie di *stakeholders* coinvolti: settore pubblico/governativo[89], settore privato/industria e società civile. In particolare, come più volte ripetuto, il settore privato è il motore di buona parte della ricerca e dello sviluppo nel settore delle ICT; dispone delle conoscenze più avanzate legate al funzionamento della tecnologia *hardware* e *software* che impiega; è il proprietario e/o l'operatore principale e/o l'amministratore di infrastrutture critiche; e ha un importante ruolo, anche di consulenza, nella preparazione e attuazione delle procedure ed i protocolli in materia informatica. Per tali ragioni i partenariati pubblico-privato sono tanto più necessari. Il settore privato deve essere sostenuto – tramite incentivi finanziari e quadri normativi adeguati – in modo da renderlo parte di in un'architettura strategica comprensiva in cui in ballo c'è la protezione della sicurezza dello Stato. La società civile è la più esposta alle

[86] Che conferma il giusto legame con le infrastrutture critiche e di nuovo una certa sovrapposizione di aree rispetto a quelle evidenziate nel Capitolo 2: infatti la tematica è inserita nell'area del "cyber-crime".

[87] Si veda ad esempio il progetto "EU-US Security Strategies: comparative scenarios and recommendations" (febbraio 2010 – marzo 2011) guidato dallo IAI nel quadro di un progetto pilota finanziato dalla Commissione Europea (http://www.iai.it/content.asp?langid=1&contentid=285). Il rapporto finale è disponibile al link http://www.iai.it/pdf/Economia_difesa/EU-US-security-strategies.pdf.

[88] Prendiamo per esempio la civilizzazione di alcune tecnologie per uso militare come l'utilizzo di i-phone che, con tecnologie civili, mostrano le cartine del teatro delle operazioni (una tendenza piuttosto europea e per soli usi tattici).

[89] Civile e militare.

minacce cibernetiche ed è opportuno incrementare la consapevolezza dei rischi *cyber* nei cittadini, che possono costituire l'anello debole della catena.[90]

Uno degli esempi più importanti in questo campo è la funzione dell'*International Telecommunication Union* (ITU), un'agenzia specializzata delle Nazioni Unite che si occupa di definizione di standard, di sviluppo e in particolare del potenziamento delle telecomunicazioni oltre che delle tematiche di sicurezza informatica. L'ITU, che conta 192 Stati parte e più di 700 membri ed associati[91], ha organizzato il *World Summit on the Information Society* (WSIS) che si è svolto a Ginevra nel 2003 e a Tunisi nel 2005[92], e che nel 2007 ha lanciato la *Global Cyber-security Agenda* (GCA)[93] come una cornice per la cooperazione internazionale mirata ad aumentare la fiducia e la sicurezza nella società dell'informazione. Vale la pena di citare anche l'*International Multilateral Partnership Against Cyber Threats* (IMPACT)[94], "iniziativa internazionale pubblico-privata" volta a migliorare le capacità della comunità internazionale di prevenire, difendersi e reagire agli attacchi informatici. IMPACT annovera una serie notevole di collaborazioni con il mondo accademico (circa 415), l'industria (18), le organizzazioni internazionali (4), le alleanze (18) e singoli paesi (53).[95] Inoltre, il *Global Response Center* (GRC) di IMPACT intende essere il principale centro risorse al mondo contro le minacce informatiche. Lavorando con i principali interessati del mondo accademico, dei governi e dell'industria, il GRC offre alla comunità internazionale un sistema aggregato di allerta rapida aggiornato in tempo reale attraverso il *Network Early Warning System* (NEWS) e la *Electronically Secure Collaboration Application Platform for Experts* (ESCAPE). L'*ITU Cyber-security Gateway*[96] è un altro esempio importante di iniziativa multilaterale nel settore della sicurezza informatica. Questo programma fornisce una piattaforma collaborativa per offrire e condividere informazioni tra le parti interessate nella società civile, il settore privato, le organizzazioni governative e internazionali che operano in diverse aree della sicurezza informatica.[97]

j) *Coordinamento*. Come già emerso, il coordinamento tra gli attori responsabili della *cyber-security* deve essere potenziato a tutti i livelli: internazionale; europeo tra istituzioni,

[90] Pensiamo per il settore privato e per i cittadini ad esempio ai sistemi cloud computing che permettono l'utilizzo di risorse hardware o software distribuite in remoto per l'archivio e la gestione dei dati ed alle collegate questioni di sicurezza dei dati.

[91] International Telecommunication Union (ITU), *About iTU,* http://www.itu.int/net/about/index.aspx.

[92] Ad entrambe le conferenze parteciparono circa 50 capi di Stato o di governo (o loro vice), 82 ministri e 26 vice-ministri di 175 Paesi, nonché importanti esponenti di organizzazioni internazionali, del settore privato, delle società civile ed infine circa 15.000 partecipanti; *World summit on the information society,* 2005*,* http://www.itu.int/wsis/basic/about.html.

[93] ITU, *Global Cybersecurity agenda*, http://www.itu.int/osg/csd/cyber-security/gca/.

[94] IMPACT, *International Multilateral Partnership Against Cyber Threats*, 2010, http://www.impact-alliance.org/home/index.html. ITU e IMPACT hanno firmato un memorandum d'intesa nel 2008.

[95] IMPACT, *Collaboration in critical times,* 2010*,* http://www.impact-alliance.org/partners/introduction.html e IMPACT, *Countries - Alphabetical list,* 2010, http://www.impact-alliance.org/countries/alphabetical-list.html.

[96] *ITU Cybersecurity Gateway,* http://groups.itu.int/Default.aspx?tabid=841.

[97] Il numero delle correnti iniziative ammonta a 3 per la società civile, a 6 per il settore privato, a 55 per i Governi ed a 76 per le Organizzazioni internazionali.

agenzie, e politiche dell'UE[98]; nazionale. Va infatti rilevato come anche nell'assetto nazionale, nonostante una positiva recente valutazione dell'ENISA sulla risposta italiana alle *cyber*-minacce[99], la mancanza di coordinamento può comportare spreco delle risorse finanziarie e inefficiente impiego delle risorse umane. Soprattutto, può venir inficiata l'efficacia della risposta che deve essere quanto più possibile rapida nell'applicazione di contromisure. Sono quindi per l'Italia condivisibili alcune raccomandazioni proposte dalla *Relazione sulle possibili implicazioni e minacce per la sicurezza nazionale derivanti dallo spazio cibernetico* del COPASIR, in particolare quella di definire un "impianto strategico-organizzativo che assicuri una *leadership* adeguata e predisponga chiare linee politiche per il contrasto alle minacce e il coordinamento tra gli attori interessati […] assegnando questi compiti ad una struttura di coordinamento presso il Presidente del Consiglio dei ministri [per] i seguenti compiti:

– definire compiutamente la minaccia e predisporre un documento di sicurezza nazionale dedicato alla protezione delle infrastrutture critiche materiali e immateriali;

– predisporre un piano d'intervento che definisca il perimetro della sicurezza cibernetica italiana, definendo i ruoli e le responsabilità di tutti i soggetti responsabili della sicurezza informatica nazionale."[100] Una pianificazione coordinata dunque, che introduca una forte componente preventiva.

Ma è evidente che con riguardo al primo punto, bisognerebbe avviare una più generale riflessione sull'opportunità, per l'Italia, di definire una Strategia di sicurezza nazionale che comprenda le dimensioni esterna ed interna della sicurezza, individuando gli interessi strategici italiani di medio e lungo termine e le direttive per la salvaguardia di questi nel contesto internazionale.[101]

[98] A tal proposito ad esempio, *La strategia di sicurezza interna dell'UE in azione: cinque tappe verso un'Europa più sicura*, COM(2010)673, si presenta come un'agenda congiunta tra gli Stati membri, il Parlamento europeo, la Commissione, il Consiglio, le Agenzie e altri, incluse la società civile e le autorità locali.

[99] ENISA, *Italy country report,* 2010, http://www.enisa.europa.eu/act/sr/files/country-reports/Italy.pdf

[100] "L'assenza di una revisione strategica del perimetro di sicurezza nazionale comporta, direttamente e indirettamente, un investimento non ottimale in termini politici e di tutela degli interessi nazionali." http://www.parlamento.it/service/PDF/PDFServer/DF/234494.pdf

[101] Federica Di Camillo e Lucia Marta, *Una strategia di sicurezza nazionale per l'Italia – Elementi di analisi*, IAI Quaderni, n.34, dicembre 2009.

Lista degli acronimi

AISE	Agenzia per l'Informazione e la Sicurezza Esterna
AISI	Agenzia per l'Informazione e la Sicurezza Interna
CCD CoE	*Cooperative Cyber Defence Centre of Excellence*
CDMA	*Cyber Defence Management Authority*
CERT	*Computer Emergency Response Teams* o.
CID	Centro Innovazione Difesa (Stato Maggiore della Difesa, III Reparto)
CIIs	*Critical Information Infrastructures* (infrastrutture critiche informatizzate)
CIIP	*Critical Information Infrastructure Protection* (protezione delle infrastrutture critiche informatizzate)
CNAIPIC	Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche
CNCPO	Centro Nazionale per il Contrasto alla Pedopornografia su Internet
	COPASIR: Comitato Parlamentare per la Sicurezza della Repubblica
CSIRT	*Computer Security and Incident Response Teams*
DDoS	*Distributed Denial of Service* (negazione diffusa di servizio)
DHS	*Department of Homeland Security* (Dipartimento della Sicurezza Interna)
DIS	Dipartimento per l'Informazione e la Sicurezza
EECTF	*European Electronic Crime Task Force*
EISAS	*European Information Sharing and Alert System* (Sistema Europeo di Allerta e di Scambio di Informazioni)
ENISA	*European Network and Information Security Agency* (Agenzia Europea per la Sicurezza delle Reti e dell'Informazione)
EP3R	*Partnership* Europea Pubblico-Privata per la Resilienza
EPCIP	*European Programme for Critical Infrastructure Protection* (Programma Europeo per la Protezione delle Infrastrutture Critiche)
ESCAPE	*Electronically Secure Collaboration Application Platform for Experts*
EU ETS	*European Union Emission Trading System* (Sistema Europeo di Scambio di Emissioni)
Europol	*European Police Office* (Ufficio di Polizia Europeo)
FIRST	*Forum of Incident Response and Security Teams*
GAT	Gruppo Anticrimine Tecnologico (*rectius* Nucleo Speciale Frodi Telematiche)

GCA	*Global Cyber-security Agenda*
GRC	*Global Response Center*
ICT	*Information and Communication Technology* (tecnologie per l'informazione e la comunicazione)
IMPACT	*International Multilateral Partnership Against Cyber Threats*
Interpol	*International Criminal Police Organization*
ITU	*International Telecommunication Union*
MITM	*Man-in-the-middle*
NATO	*North Atlantic Treaty Organization* (Organizzazione del Trattato dell'Atlantico del Nord)
NEWS	*Network Early Warning System*
NIS	*Network and Information Security* (sicurezza delle reti e delle informazioni)
OCSE	Organizzazione per la Cooperazione e lo Sviluppo Economico
PCM	Presidenza del Consiglio dei Ministri
PIC	Protezione Infrastrutture Critiche
R&S	Ricerca e sviluppo
SCADA	*Supervisory Control and Data Acquisition*
SCIIC	Segreteria di Coordinamento Interministeriale per le Infrastrutture Critiche
TIC	tecnologie dell'informazione e della comunicazione
UACI	Unità di Analisi sul Crimine Informatico
UE	Unione Europea
US JFCOM	*United States Joint Forces Command*
WSIS	*World Summit on the Information Society*

L'OSSERVATORIO DI POLITICA INTERNAZIONALE È UN PROGETTO DI COLLABORAZIONE TRA SENATO DELLA REPUBBLICA, CAMERA DEI DEPUTATI E MINISTERO DEGLI AFFARI ESTERI CON AUTOREVOLI CONTRIBUTI SCIENTIFICI.

L'OSSERVATORIO REALIZZA:

Rapporti
Analisi di scenario, a cadenza annuale, su temi di rilievo strategico per le relazioni internazionali.

Focus
Rassegne trimestrali di monitoraggio su aree geografiche e tematiche di interesse prioritario per la politica estera italiana.

Approfondimenti
Studi monografici su temi complessi dell'attualità internazionale.

Note
Brevi schede informative su temi legati all'agenda internazionale.

Approfondimenti già pubblicati:

11 - Il nuovo Concetto strategico della Nato: verso la quadratura del cerchio?, aprile 2010
12 - Nuove forme di antisemitismo e mezzi di contrasto, aprile 2010
13 - Il regime di non proliferazione nucleare alla vigilia dell'ottava Conferenza di Riesame del Trattato di Non Proliferazione Nucleare, maggio 2010
14 - Le relazioni sino-russe e il caso dell'Organizzazione per la Cooperazione di Shanghai, maggio 2010
15 - La formazione delle forze di sicurezza afghane, maggio 2010
16 - Cambiamenti climatici e governance della sicurezza: la rilevanza politica della nuova agenda Internazionale, maggio 2010
17 - Il Consiglio d'Europa e l'immigrazione, giugno 2010
18 - La nuova leadership Usa e le relazioni transatlantiche, settembre 2010
19 - Impatto delle sanzioni contro l'Iran, settembre 2010
20 - Nuovi paradigmi sulla sicurezza alimentare e la pace, settembre 2010
21 - Rom e sinti in Italia: condizione sociale e linee di politica pubblica, ottobre 2010
22 - Il Corno d'Africa, ottobre 2010
23 - La questione curda, ottobre 2010
24 - Il confronto internazionale nell'Artico, ottobre 2010
25 - Il nuovo governo della Colombia: le sfide e le opportunità, ottobre 2010
26- La crisi in Kirghizistan e le conseguenze per la stabilità regionale, novembre 2010
27- La riforma della governance economica europea, aprile 2011
28 - Le Assemblee legislative di Afghanistan e Pakistan, maggio 2011
29 - L'emergenza umanitaria al confine tra Tunisia e Libia.La situazione nel complesso di Ras Djir, maggio 2011
30 - La crisi dei Grandi Laghi, maggio 2011
31 - Cambiamento climatico. Il quadro dell'azione internazionale, maggio 2011

Coordinamento redazionale a cura del:
Senato della Repubblica
SERVIZIO STUDI
Tel. 06.67062629 - e-mail: studi1@senato.it
SERVIZIO AFFARI INTERNAZIONALI
Tel. 06.67062989 - e-mail: segreteriaAAII@senato.it