NICOLA PEDDE

Cybersecurity Strategy of the European Union

La cultura dell'Intelligence è lo strumento attraverso il quale comprendere il ruolo e l'operato dei moderni Servizi di informazione e sicurezza. Strumento dato dall'approfondimento degli studi e delle analisi dei principali think tank, centri di ricerca, università italiane e straniere.
La cultura dell'Intelligence intende, quindi, selezionare e presentare periodicamente i più significativi studi sulle tematiche relative alle strutture di intelligence, o a queste direttamente connesse, agevolando la comprensione della storia, delle metodologie e delle funzioni delle più moderne strutture di settore.
Un contributo per sfatare i tanti miti e luoghi comuni che da sempre accompagnano l'immagine dei Servizi segreti di tutto il mondo e per acquisirne, al contrario, consapevolezza del ruolo e dell'operato.

Cybersecurity Strategy of the European Union:
An Open, Safe and Secure Cyberspace

Joint Communication of the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions European Commission
Documento
Brussels, 7 febbraio 2013
http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security

Iran's Ministry of Intelligence and Security: a Profile
Federal Research Division, Library of Congress
Washington, Dicembre 2012
http://www.fas.org/irp/world/iran/mois-loc.pdf

Interessante quanto originale documento prodotto dal Dipartimento di Studi della Biblioteca del Congresso USA, che illustra la struttura e le competenze dell'apparato di intelligence della Repubblica Islamica dell'Iran.
Un documento ricco di immagini e tabelle, che traccia un quadro generale del MOIS partendo da una prospettiva storica e terminando con una valutazione complessiva della capacità operativa odierna all'interno del paese e a livello internazionale.

Administration Strategy on Mitigating the Theft of U.S. Trade Secret
Defense Security Service
Washington, Febbraio 2013
http://www.whitehouse.gov//sites/default/files/omb/IPEC/admin_strategy_on_mitigating_the_theft_of_u.s._trade_secrets.pdf

Vero e proprio manuale introduttivo, ad uso della pubblica amministrazione statunitense, per favorire l'adozione di politiche volte alla mitigazione del rischio relativo al trafugamento di segreti commerciali. Questo documento è stato realizzato attraverso una collaborazione tra la DSS e numerosi altri enti governativi, direttamente coinvolti sull'argomento, come il Dipartimento del Commercio, il Dipartimento della Difesa, la Homeland Security, il Dipartimento della Giustizia, il Dipartimento di Stato, l'Ufficio del Direttore dell'Intelligence Nazionale e l'Ufficio della Rappresentanza di Commercio degli Stati Uniti.

Cybersecurity Strategy of the European Union

Lungamente atteso, questo documento della Commissione Europea pone le basi per la strategia comunitaria di intervento in materia di sicurezza nel cyberspazio, affrontando in modo completo ed organico l'insieme delle esigenze dell'Unione per la gestione libera e sicura della Rete e delle informazioni in transito su questa.

L'obiettivo del documento, quindi, è quello di delineare il quadro concettuale nell'ambito del quale l'Unione Europea dovrà definire la propria strategia di sicurezza cibernetica favorendo, da un lato, le garanzie di accessibilità e liberta della rete e, dall'altro, i profili di sicurezza per la protezione delle informazioni su questa scambiate.

Il documento parte dal presupposto di come la cyber-criminalità sia un'evidenza di portata ed ampiezza non più trascurabile, i cui costi ed i relativi effetti sulla stabilità dei sistemi tendono a divenire esponenziali. A questa forma di minaccia è, quindi, necessario rispondere con una adeguata azione di cyber-sicurezza, volta a tutelare gli interessi degli individui, delle imprese e delle istituzioni comunitarie.

Con il termine di cyber-security viene, quindi, indicata dal documento l'azione volta alla salvaguardia dell'ambiente digitale, sia civile che militare, dalle minacce che possono compromettere l'interdipendenza dei network e le infrastrutture informatiche. Il ruolo della cyber-security è, quindi, quello di garantire e preservare l'accessibilità e l'integrità dei network e delle infrastrutture, e la confidenzialità delle informazioni da questi processate.

Viene, invece, denominata come cyber-crime l'azione criminale in cui il computer rappresenta il mezzo per delinquere, o l'obiettivo del crimine. La tipologia di reato comprende una vasta gamma di fattispecie, come quelle tradizionali (ad esempio la frode, la falsificazione, il furto di identità, ecc.), quelle relative ai contenuti (come, ad esempio, il traffico di materiali pedopornografici), e quelle relative all'utilizzo dei sistemi informativi (virus, malaware, ecc.).

Lo spirito del documento è, quindi, quello di sancire una estensione della tutela dei valori fondamentali riconosciuti dall'Unione Europea anche al settore digitale, ed in particolare:

a) Protezione dei diritti fondamentali, della libertà di espressione, dei dati personali e del diritto alla privacy.
b) Accessibilità per tutti.
c) Governance multipla democratica ed efficiente.
d) Responsabilità condivisa a garanzia della sicurezza.

Nel definire le priorità strategiche e le azioni necessarie per garantire la sicurezza dei sistemi informativi, il documento individua nei singoli Stati membri la responsabilità di base della cyber-security. L'obiettivo comune dell'Unione Europea per il settore, quindi, è quello di garantire una efficace ed omogenea adozione di provvedimenti a livello di singole entità governative, al fine di assicurare il conseguimento di cinque priorità strategiche.

La prima è quella inerente il conseguimento della 'cyber-resilienza', e quindi, della capacità di resistenza dei cyber-sistemi attraverso il conseguimento di una capacità di interazione, integrazione e coordinamento dei sistemi a livello europeo. Per fronteggiare e resistere alle emergenze e garantire la continuità di funzionamento dei sistemi comunitari e la loro sicurezza.

L'Europa resterà vulnerabile senza uno sforzo sostanziale per incrementare le capacità pubbliche e private, le risorse e i processi per prevenire, individuare e gestire la cyber-sicurezza. Per questo è stata sviluppata dalla Commissione una politica di Network e Information Security (NIS), attraverso la creazione nel 2004 dell'ENISA (European Network and Information Security Agency).

Nonostante i poderosi progressi conseguiti, deve essere oggi definita una nuova strategia di gestione del settore, attraverso la definizione di una puntuale e rispondente legislazione, e sviluppando dei livelli operativi minimi comuni nell'adozione della NIS a livello locale.

Ulteriore priorità dell'azione di resilienza è quella dell'incremento della consapevolezza del rischio ad ogni livello della vita pubblica e privata in ogni singolo paese membro dell'Unione Europea, attraverso un concreto ruolo in tale ambito da parte della Commissione.

La seconda priorità strategica è quella relativa alla necessità di ridurre drasticamente la cyber-criminalità, attraverso un'azione combinata sul piano legislativo (finalizzato ad individuare e definire con precisione le fatti-specie di reato e le modalità di prevenzione e contrasto) e su quello della sicurezza infrastrutturale, creando in tal modo una barriera fisica di ostacolo alla penetrazione degli operatori criminali nella rete dei paesi membri dell'Unione.

Anche in questo caso, la Commissione si farà promotrice di un ruolo centrale favorendo, soprattutto, il raccordo dei singoli Stati membri in un processo di cooperazione efficace e funzionale.

La terza priorità strategica è invece dedicata allo sviluppo della politica e della capacità di cyber-difesa, nell'ambito dei margini della politica comune di sicurezza e difesa (CSDP), soprattutto al fine di incrementare ed implementare le strategie di sicurezza dei sistemi di comunicazione e informazione dei singoli apparati nazionali di Difesa e Sicurezza Nazionale.

In questo ambito, la Commissione auspica una sempre maggiore cooperazione dei settori civili e militari, soprattutto attraverso un nuovo e più vigoroso impulso sulla ricerca e sullo sviluppo in ambito tecnologico e una più efficace collaborazione sia a livello governativo, che industriale e accademico.

La Commissione ritiene, peraltro, esplicitamente necessaria una formula di cooperazione tra l'Unione Europea e la NATO, stante la stretta correlazione tra le due organizzazioni e la gestione in larga misura dei medesimi rischi sulle medesime aree geografiche di interesse primario.

La quarta priorità strategica si riferisce allo sviluppo di risorse industriali per la cyber-sicurezza, partendo dalla consapevolezza che la maggior parte dei migliori e più innovativi produttori di tecnologia ICT risieda al di fuori dei confini dell'Unione. Questo deve, quindi, spingere in direzione di uno sforzo non solo per la realizzazione di poli di sviluppo industriale di settore sul territorio dell'Unione ma, anche, e soprattutto la creazione e la promozione di un singolo mercato dei prodotti per la cyber-sicurezza. Gli organi e le istituzioni pubbliche, le imprese e le attività industriali, ma anche i singoli cittadini, devono comprendere il valore e la rilevanza del fattore sicurezza, implementando, aggiornando e rendendo sicuro il modo in cui i propri dati e le proprie comunicazioni vengono gestite a livello tecnologico, investendo costantemente sull'*upgrade hardware e software* della sicurezza, e dando quindi luogo ad un mercato europeo della sicurezza capace di alimentare lo sviluppo di prodotti e componenti all'avanguardia.

Sarà anche in questo caso la Commissione a favorire il potenziamento delle sinergie nel settore della Ricerca e dello Sviluppo, agevolando in tal modo la creazione di un polo europeo di eccellenza di settore.

La quinta e ultima priorità strategica sarà invece quella di stabilire una politica internazionale del cyber-spazio coerente a livello europeo, promuovendo i valori cardine del sistema dell'Unione e dando quindi vita ad un modello squisitamente autoctono di definizione delle linee di intervento normativo.

Questo processo può essere ottenuto solo attraverso la definizione di una più significativa e corposa azione di cooperazione a livello internazionale, cercando di integrare nel processo relazionale tutti gli organi ed organismi internazionali a vario titolo coinvolti nell'azione comune di garantire la cyber-sicurezza ed il perseguimento delle fenomenologie criminali in quest'ambito collocate.

Il documento si conclude con una descrizione di quelli che dovranno essere i ruoli e le responsabilità degli attori coinvolti, esplicitamente escludendo una supervisione centrale degli organi europei a vantaggio, invece, di una localizzazione delle responsabilità nell'ambito delle singole realtà degli Stati membri.

Questo per assicurare una più diretta, mirata, puntuale ed efficace forma di individuazione e gestione del processo di gestione della cyber-sicurezza, attraverso una capacità di intervento mirata alla soluzione nel 'punto di ingresso' della minaccia.

Il coordinamento delle autorità con competenza NIS costituisce ovviamente una priorità assoluta, sia a livello comunitario che, più in generale, a livello internazionale.