



IWC 2011

CYBER WARFARE & CYBER INTELLIGENCE NATO-EU: una sfida da affrontare insieme

Giancarlo Grasso
FINMECCANICA
Senior Advisor

“Cyber Security has become the hot issue both for the EU and for NATO and will remain such in the years to come”

Gilles de Kerchove d’Ousselghem
EU Counter –Terrorism Coordinator
ASD Conference, *Istanbul* Oct. 6, 2011

- Tutte le infrastrutture di una nazione possono essere danneggiate
- La distinzione tra militare e civile va sfumando
- I singoli domini, nell'ambito di una Nazione, devono inter-operare per essere poi totalmente integrati, soprattutto nella *cyber intelligence*
- Solo la collaborazione tra Nazioni può dare luogo ad una difesa efficace
- L'adesione alle iniziative delle Organizzazioni Internazionali (NATO, EU...) di cui facciamo parte è imprescindibile.

NATO

”Strategic Concept 2010”: *“develop further our ability to prevent, detect, defend against and recover from cyber-attacks...”.*

Amm. Di Paola

Chairman

NATO Military Committee :

“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.”

Il *North Atlantic Council (NAC)* ha avuto mandato dai Capi di Stato, meeting di Lisbona nel 2010, di rielaborare la “*NATO Cyber Defence Policy*”.

Il *Defence Policy and Planning Committee (DPPC)* ha emesso i documenti:

1. *NATO Cyber Defence Policy*
2. *Cyber Defence Action Plan*

entrambi sono stati approvati dal *NAC*, a livello di Ministri della Difesa, l'8 giugno 2011.

Principi

- Prevenzione e resilienza piuttosto che reazione
- Non duplicazione degli sforzi
- Condivisione dell'informazione e sicurezza

Governance

- Sviluppo delle capacità di *cyber defence* proprie della NATO definito dalle Autorità Militari in base alle decisioni prese dal *North Atlantic Council* secondo il *NATO Defence Planning Process*.
- Responsabilità diretta degli alleati sui CIS (*Communication Information System*) nazionali. NATO richiede che i medesimi siano affidabili e sicuri nelle loro connessioni con il proprio CIS NATO.
- Elaborazione dei requisiti minimi di *cyber defence* equivalenti e compatibili con quelli del CIS NATO in un processo di “*governance*” condiviso con gli Alleati.
- Certificazione NATO del raggiungimento dei requisiti minimi.

NATO ha istituito: *Cyber Defence Management Authority (NCDMA)/ Cyber Defence Management Board*

- pianificazione strategica, supervisione e guida dell'implementazione della politica cyber;
- coordinamento centralizzato di tutti i servizi *Cyber Defence* per il CIS NATO;
- gestione delle interazioni con gli Alleati.

NATO ha attribuito: alla *Consultation, Command and Control Agency (NC3A)*

- aspetti tecnici e implementativi della *cyber defence* dalla identificazione dei requisiti operativi e il relativo *procurement*.

NATO ha avviato: *Computer Incident Response Capability Technical Center (NCIRCTC)*

- responsabile della fornitura dei servizi di cyber security NATO. Opera direttamente in caso di incidenti e dissemina le informazioni relative ad essi ai gestori dei sistemi di sicurezza e loro utilizzatori

- NATO ha assegnato alla nuova** *Emerging Security Challenges Division (ESCD)*
il compito di coordinare gli approcci NATO al terrorismo e supportare gli Alleati nel loro sforzo teso a sviluppare politiche coerenti di risposta ad altre minacce trasversali quali i *cyber attack*, le minacce energetiche e la proliferazione delle armi di distruzione di massa
- NATO ha accreditato** il *Cooperative Cyber Defence* di Tallinn, Estonia, come Centro di Eccellenza con la missione di perseguire in un ambito di addestramento, ricerca e sviluppo, il miglioramento delle capacità e della cooperazione nonché lo scambio di informazioni ed esperienze tra gli alleati.

Forum europeo degli Stati membri (EFMS)

Promozione delle discussioni e degli scambi tra autorità competenti sulle “*best practices*” in materia di sicurezza e resilienza delle infrastrutture TIC per definire:

- l'insieme minimo di capacità e servizi di base e le relative raccomandazioni strategiche,
- la definizione di incentivi di natura economica e regolamentare, a favore della sicurezza e della resilienza,
- la valutazione della situazione della sicurezza informatica in Europa,
- l'organizzazione di esercitazioni paneuropee,
- l'esame delle priorità da trattare in un quadro internazionale in materia di sicurezza e resilienza.

Partenariato pubblico-privato europeo per la resilienza (EP3R)

Costituisce un quadro di *governance* europeo per la resilienza delle infrastrutture TIC che mira a incentivare la cooperazione tra il settore pubblico e il settore privato su questioni strategiche della politica dell'UE in materia di sicurezza e resilienza a minacce cyber.

Partenariati strategici di dimensione internazionale

Creazione, in occasione del vertice UE-USA del novembre 2010, di un gruppo di lavoro congiunto UE-USA sulla sicurezza e la criminalità informatica.

ENISA

European Network Information Security Agency

Creata nel 2004 e con sede a Creta è essenzialmente una piattaforma di scambio di informazioni e *best practices* tra le istituzioni UE, le autorità nazionali e le imprese. Può fornire pareri tecnici sia alle autorità degli Stati membri che alle istituzioni comunitarie.

EDA

European Defence Agency

A valle del documento EUMS:13537/09, *EU Concept for Computer Network Operations in EU-led Military Operations* (CNO) ha avviato iniziative per lo sviluppo delle *Cyber Defence Capabilities* e per il miglioramento delle attuali architetture includendo anche inputs provenienti dal mondo civile.

CERT

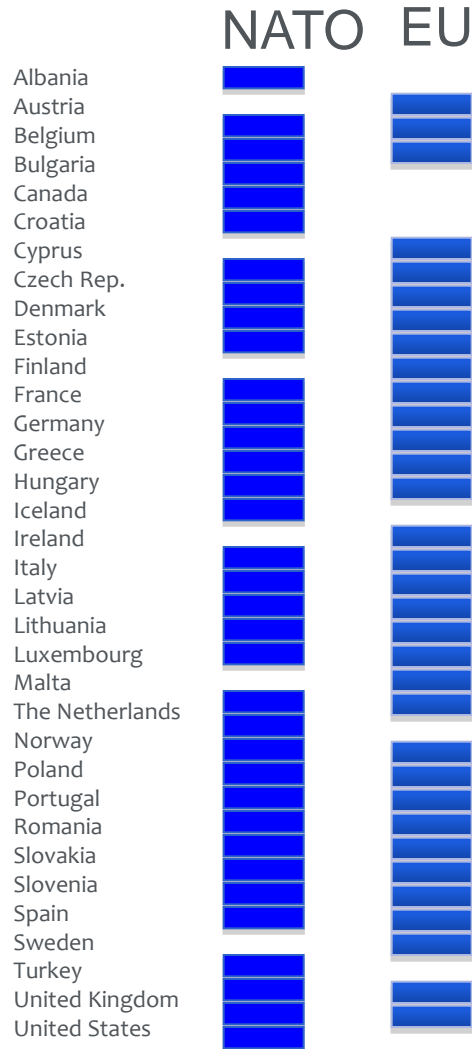
Computer Emergency Response Team

CERT delle istituzioni dell'UE e CERT in ogni Stato membro entro il 2012

EISAS

European Information Sharing and Alert System

Sistema europeo di condivisione della *cyber intelligence* informazioni e di allarme per il grande pubblico entro il 2013.



- 21 Stati Europei sono sia EU(27) che NATO(28).
- Non ha senso distinguere tra civile e militare.
- Le risorse sono quelle delle singole Nazioni.
- La minaccia deve essere affrontata in modo coordinato e cooperativo.
- La NATO ha dichiarato che intende per la *Cyber Defence* operare in coordinamento con le altre organizzazioni internazionali e in particolare ha l'obiettivo di concordare entro il 2011 una collaborazione con EU.

L'industria si aspetta che EU e NATO esercitino una *Governance* unificata nella definizione delle “regole” relative alla *cyber* degli Stati membri al fine di:

con l'obiettivo di:

per permettere alle industrie di:

- Facilitare il rapporto Domanda/Offerta in Partenariato
- Definire lo scenario ed evoluzione della minaccia
- Stabilire i livelli di protezione minima
- Imporre uno Standard e curare la Certificazione.

- Investire in prodotti rispondenti agli Standard Europei
- Introdurre nei prodotti la “*Built-In Cyber Security*”

- Sviluppare il mercato Europeo della *cyber security*