Presi nella Rete
(analisi e contrasto della criminalità informatica)

Collegio Ghislieri *Pavia, 23 novembre 2012*

Dal crimine informatico al cyber-warfare
Analisi dell'evoluzione della minaccia a difesa dello Stato

AVV. STEFANO MELE

Dal crimine informatico al cyber-warfare

- Lo scenario attuale in materia di *cyber-warfare*

E' una **minaccia reale**?

- Incremento esponenziale del numero degli attacchi
- Incremento degli "attori"

Cyber-attack come:

- Spionaggio elettronico
- Facilitatore di attacchi armati
- *Cyber-weapon*

Dal crimine informatico al cyber-warfare

- Reazione a livello internazionale

✓ Incremento del *budget* per il settore
✓ Creazione di strutture statali *ad hoc*
✓ Pianificazione strategica e *cyber-strategies*

Dal crimine informatico al cyber-warfare

- Reazione Italiana

In Italia ad un appena accettabile livello di consapevolezza della minaccia fa eco, almeno per quanto è dato sapere a livello di fonti aperte:

- ✓ la mancanza di pianificazione strategica;
- ✓ la mancanza di una dottrina nazionale;
- ✓ la mancanza di un centro decisionale integrato di livello strategico.

Dal crimine informatico al cyber-warfare

- Principali questioni strategiche

- ✓ Supremazia dell'attacco sulla difesa
- ✓ Tracciabilità degli attacchi
- ✓ Attribuzione delle responsabilità
- ✓ Mancanza di deterrenza
- ✓ Mancanza di leggi *ad hoc*
- ✓ *Cyber-weapons* e danni da "fuoco amico"
- ✓ Mancanza di *information sharing* tra settore pubblico e privato

Dal crimine informatico al cyber-warfare

- Principali questioni giuridiche

- ✓ Mancanza delle definizioni giuridiche che regolano la materia
- ✓ Preparazione del “campo di battaglia” in tempo di pace
- ✓ Regole d’ingaggio
- ✓ Quando un *cyber-attack* equivale ad un attacco armato
- ✓ Proporzionalità della risposta rispetto all’attacco
- ✓ *Systems as proxies*
- ✓ Danni collaterali
- ✓ ecc..

Dal crimine informatico al cyber-warfare

Focus sulle *cyber-weapon*

- In maniera molto semplicistica e diretta, le armi sono strumenti attraverso cui, all'interno di uno specifico contesto, un soggetto può **recare un danno** ad un altro soggetto o ad un oggetto, ovvero difendersi da un'aggressione.

- Il Codice penale, agli artt. 585 e 704, definisce come armi:

1. quelle **da sparo** e tutte le altre la cui destinazione naturale è l'**offesa alla persona**;
2. tutti gli strumenti atti ad offendere, dei quali è dalla legge vietato il **porto in modo assoluto**, ovvero senza giustificato motivo;
3. le **bombe**, qualsiasi macchina o involucro contenente **materie esplodenti**, e i gas asfissianti o accecanti, assimilati alle armi.

Dal crimine informatico al cyber-warfare

Focus sulle *cyber-weapon*

- Per armi improprie s'intendono quegli strumenti atti ad offendere, ma che non nascono per adempiere questo **specifico scopo**, come ad esempio coltelli, mazze, catene, martelli, ecc.
- Appare evidente, allora, come la **normativa italiana** non definisca ancora in maniera chiara e diretta cosa debba intendersi per *cyber-weapon*
- Medesima situazione si rileva a **livello internazionale** (*Dictionary of Military and Associated Terms*)

Dal crimine informatico al cyber-warfare

Focus sulle *cyber-weapon*

- A **livello ontologico**, un'arma può essere anche un concetto puramente astratto e non per forza materiale, ovvero può certamente essere considerato come arma un **insieme di istruzioni informatiche**, come ad esempio un programma, un algoritmo, una parte di codice e così via, che, utilizzate in determinati contesti con lo scopo di colpire e danneggiare specifici soggetti e/o oggetti, possono assumere la caratteristica di cyber-armi.

Dal crimine informatico al cyber-warfare

Focus sulle *cyber-weapon*

- Nonostante l'immaterialità di questo genere di armi, ciò su cui realmente occorre porre l'attenzione sono tre elementi:

1. il **contesto**,
2. lo **scopo**, e
3. il **soggetto/oggetto soccombente**

Gli unici elementi utili, nei fatti, a qualificare o meno – sempre a livello ontologico – questo genere di armi.

Dal crimine informatico al cyber-warfare

Focus sulle *cyber-weapon*

- Il Codice penale italiano può venirci in aiuto per provare a dare una definizione di *cyber*-arma che abbia anche **valenza giuridica**, mutuando l'art. 615-*quinquies* in materia di "*Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico*" e il contenuto di alcuni concetti della Direttiva europea sulle infrastrutture critiche.

Dal crimine informatico al cyber-warfare

Focus sulle *cyber-weapon*

- Una ***cyber*-arma** può essere definita come:

"un'apparecchiatura, un dispositivo ovvero qualsiasi insieme di istruzioni informatiche dirette a danneggiare illecitamente un sistema informatico o telematico avente carattere di infrastruttura critica, le sue informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti, ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento".

Dal crimine informatico al cyber-warfare

Focus sulle *cyber-weapon*

Sulla base di questo assunto, **Stuxnet** è certamente una ***cyber-weapon*** in quanto è:

- un insieme di **istruzioni informatiche**, sotto forma di programma eseguibile/*worm*,
- creato appositamente per alterare illecitamente il funzionamento (**scopo**)
- di un'infrastruttura critica (**oggetto soccombente**)
- attraverso un attacco informatico (**contesto**).

Riflessioni conclusive

Le *cyber-weapon*, come si è visto, **impongono comportamenti adattivi e di reazione** che tagliano trasversalmente sia i settori della ricerca tecnica e tecnologica, che quelli **strategico, tattici ed operativi**, i quali per la prima volta, proprio attraverso Internet e la tecnologia, stanno vedendo **svanire la loro tipica compartimentazione settoriale**.

Che ci si trovi di fronte ad una "*cyber-war*", ovvero a singoli atti di *cyber-warfare*, come ancora ad azioni tese ad impadronirsi esclusivamente delle informazioni sensibili e/o classificate di un Governo, la priorità resta e deve restare sempre la **protezione degli *asset* strategici – anche immateriali – della nostra nazione**, che oggi possono essere messi a rischio quasi istantaneamente attraverso un attacco informatico.

Collegio Ghislieri

Dal crimine informatico al cyber-warfare

Analisi dell'evoluzione della minaccia a difesa dello Stato

.. grazie per l'attenzione..

AVV. STEFANO MELE

http://www.stefanomele.it avv.stefanomele@gmail.com