ISTITUTO ITALIANO DI STUDI STRATEGICI

ITALIAN INSTITUTE OF STRATEGIC STUDIES

Niccolò Machiavelli

LA STRATEGIA ITALIANA IN MATERIA DI CYBER SECURITY

STEFANO MELE

HackInBo 2014 - Bologna

03 MAY 2014

@MeleStefano

- Avvocato specializzato in Diritto delle Tecnologie, Privacy, Sicurezza ed Intelligence.
- Dottore di ricerca presso l'Università degli Studi di Foggia
- Vivo e lavoro a Milano come "*of Counsel*" di Carnelutti Studio Legale Associato
- Collaboro presso le cattedre di Informatica Giuridica e Informatica Giuridica avanzata della Facoltà di Giurisprudenza dell'Università degli Studi di Milano
- Esperto di cyber-security, cyber-intelligence, cyber-terrorism e cyber-warfare:
  - Direttore di Ricerca su "*Cyber-security & Cyber-Intelligence*" del Ce.Mi.S.S. (Centro Militare di Studi Strategici)
  - Coordinatore dell'Osservatorio "InfoWarfare e Tecnologie emergenti" dell'Istituto Italiano di Studi Strategici 'Niccolò Machiavelli'
  - Consulente per organizzazioni nazionali ed estere, sia militari che civili
  - Docente presso Istituti di formazione e di ricerca del Ministero della Difesa italiano e della NATO

#Governo italiano e cyber-threat

#Governo italiano e cyber-threat

- ***Febbraio 2010 – DIS "Relazione sulla politica dell'informazione per la sicurezza 2009":***
  - «Con riferimento, poi, agli scenari di **potenziale incidenza sulla sicurezza economica** e sulla più generale architettura "di sistema" che sorregge il concreto funzionamento, le attività quotidiane e i programmi di sviluppo della Nazione, un fondamentale campo di sfida per l'intelligence sarà quello della cybersecurity. Ciò a cospetto di una minaccia che ha ormai assunto caratura strategica, tanto da essere considerata dai principali attori internazionali un fattore di rischio di prima grandezza, direttamente proporzionale al grado di sviluppo raggiunto dalle tecnologie dell'informazione».

- ***Febbraio 2011 – DIS "Relazione sulla politica dell'informazione per la sicurezza 2010":***
  - «**Di potenziale impatto sul sistema Paese e sulla stessa sicurezza nazionale**, la minaccia cibernetica si conferma una sfida crescente per le politiche di sicurezza degli Stati, e sollecita pertanto il diretto coinvolgimento degli apparati d'intelligence, la massima sinergia tra settori pubblici e privati e la più ampia collaborazione internazionale. […] Conclusivamente, è ragionevole ritenere che per l'immediato futuro la sfida più impegnativa sul piano della prevenzione e del contrasto sarà rappresentata proprio dalla minaccia cibernetica, che verosimilmente continuerà ad "evolvere", anche in relazione alla sua capacità di concretizzarsi in maniera efficace, selettiva, anonima, senza limiti di tempo e di distanza».

#Governo italiano e cyber-threat

- ***Luglio 2010 – "Cyber minacce e sicurezza. La relazione del COPASIR sulle possibili implicazioni e minacce per la sicurezza nazionale derivanti dallo spazio cibernetico":***
  - Pianificazione strategica in materia di contrasto alla minaccia cibernetica;
  - Dotarsi di un impianto strategico – organizzativo che assicuri una leadership adeguata e predisponga chiari linee politiche per il contrasto alle minacce e il coordinamento tra gli attori interessati;
  - Mappatura e classificazione delle infrastrutture critiche per la sicurezza nazionale, sia materiali che immateriali;
  - Predisporre un documento di sicurezza nazionale dedicato alla protezione delle infrastrutture critiche materiali e immateriali;
  - Redigere in stretto coordinamento con gli interlocutori istituzionali e privati, a cominciare dagli apparati di intelligence, le politiche strategiche di protezione, resilienza e sicurezza cibernetica;
  - Sviluppare la collaborazione pubblico – privato per migliorare l'azione di prevenzione e contrasto al cyber-crime e la cooperazione internazionale in ambito bilaterale e multilaterale;
  - Predisporre piani di *disaster recovery* per i dati di valore strategico per la sicurezza della Repubblica.

#Governo italiano e cyber-threat

- ***Febbraio 2012 – DIS "Relazione sulla politica dell'informazione per la sicurezza 2011":***
  - «L'attività di intelligence nel corso del 2011 ha considerato con **prioritaria attenzione la minaccia cibernetica** che, secondo valutazioni condivise anche in ambito di collaborazione internazionale, ha fatto registrare una crescita esponenziale. Il primo dato che emerge con evidenza da questa tendenza è quello dell'aumentata vulnerabilità di una moltitudine di attori, statuali e non, cui ha corrisposto il proliferare di sempre più sofisticate tipologie di attacchi informatici mirati. [...] Tra i nuovi strumenti di attacco informatico si annoverano, altresì, sofisticate forme di intrusione (*Advanced Persistent Threat* - APT), miranti alla sottrazione di informazioni sensibili e proprietà intellettuale di aziende e realtà pubbliche».

- ***Febbraio 2013 – DIS "Relazione sulla politica dell'informazione per la sicurezza 2012":***
  - «La minaccia cibernetica rappresenta, al momento, **la sfida più impegnativa per il sistema Paese** […]. La natura complessa, impalpabile e pervasiva della *cyberthreat* rende le soluzioni al problema di non facile individuazione ed applicazione poiché gli attori, i mezzi, le tecniche di attacco ed i bersagli mutano più velocemente delle contromisure».

#Governo italiano e cyber-threat

- ***Febbraio 2014 – DIS "Relazione sulla politica dell'informazione per la sicurezza 2013":***
  - «L'**elevato grado di priorità** annesso dall'intelligence al contrasto della minaccia cyber è correlato all'importanza che riveste lo spazio cibernetico per il benessere e per la sicurezza del Paese. Infatti, solo l'efficace tutela di tale spazio, che comprende tutte le attività digitali che si svolgono nella rete, **consente di garantire il normale funzionamento della vita collettiva sotto molteplici profili: politico, sociale, economico, tecnologico-industriale e culturale**».

#Governo italiano e cyber-threat

- ***Il DPCM 24 gennaio 2013 - "Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica aziendale"***
  - Lo scopo è quello di «definire in un contesto unitario e integrato l'**architettura istituzionale deputata alla tutela della sicurezza nazionale** relativamente alle infrastrutture critiche materiali e immateriali, con particolare riguardo alla protezione cibernetica e alla sicurezza informatica nazionali».

#La cyber-strategy italiana

#La cyber-strategy italiana

- ***Sei sono i pilastri strategici del "Quadro strategico nazionale per la sicurezza dello spazio cibernetico" su cui il nostro Governo ha deciso di incentrare la sua strategia:***

1. Il miglioramento delle **capacità tecnologiche, operative e di analisi** degli attori istituzionali interessati
2. Il potenziamento delle **capacità di difesa delle infrastrutture critiche nazionali e degli attori di rilevanza strategica** per il sistema-Paese
3. L'incentivazione della **cooperazione tra istituzioni e imprese nazionali**
4. La promozione e diffusione della **cultura della sicurezza**
5. Il rafforzamento delle capacità di contrasto alla diffusione di **attività e contenuti illegali on-line**
6. Il rafforzamento della **cooperazione internazionale** in materia di sicurezza cibernetica

#La cyber-strategy italiana

- ***Undici sono i punti operativi predisposti all'interno del "Piano nazionale per la protezione cibernetica e la sicurezza informatica":***

1. Potenziamento delle **capacità di intelligence, di Polizia e di difesa civile e militare**
2. Potenziamento dell'**organizzazione e delle modalità di coordinamento e di interazione** a livello nazionale tra soggetti pubblici e privati
3. Promozione e diffusione della **cultura della sicurezza informatica**. Formazione e addestramento
4. **Cooperazione internazionale** ed esercitazioni
5. **Operatività del CERT nazionale**, del CERT-PA e dei CERT dicasteri
6. **Interventi legislativi** e compliance con obblighi internazionali
7. Compliance a **standard e protocolli di sicurezza**
8. Supporto allo **sviluppo industriale e tecnologico**
9. **Comunicazione strategica**
10. **Ottimizzazione della spesa** nei settori della cyber-security e cyber-defence
11. Implementazione di un sistema di **information risk management** nazionale

#La cyber-strategy italiana

Il **Quadro Strategico italiano** mira «ad accrescere la capacità di risposta del Paese alle presenti e future sfide riguardanti il cyber-space, indirizzando gli sforzi nazionali verso obiettivi comuni e soluzioni condivise, nella consapevolezza che **la protezione dello spazio cibernetico è un processo più che un fine**, che la continua innovazione tecnologica introduce inevitabilmente nuove vulnerabilità, e che le caratteristiche stesse della minaccia cibernetica rendono **la difesa, per ora, di tipo prevalentemente – anche se non esclusivamente – reattivo**».

- La sicurezza come processo
- Approccio difensivo evidente e di *active defence* 'latente'

#La cyber-strategy italiana

Con il **Piano Nazionale italiano** «l'Italia si dota di una strategia organica, alla cui attuazione sono chiamati a concorrere non solo gli attori, pubblici e privati, richiamati nel Quadro Strategico Nazionale ma anche **tutti coloro che, su base quotidiana, fanno uso delle moderne tecnologie informatiche**, a partire dal singolo cittadino.
Tale strategia associa alla sua valenza organica un tratto di flessibilità, indispensabile a fronte delle rapide evoluzioni tecnologiche dello spazio cibernetico e delle relative sfide di sicurezza.
La necessità, in sostanza, **non è solo quella di essere "al passo con i tempi" ma anche di coglierne le "anticipazioni"**, così da prevenire le future minacce atte a minare lo sviluppo economico, sociale, scientifico e industriale, nonché la stabilità politico-militare del nostro Paese».

- Colma una lacuna presente nella maggior parte delle *cyber-strategy* degli altri Paesi
- Rilevanza della nascita di una cultura della sicurezza
- Rilevanza della cooperazione tra pubblico e privato
- Rilevanza dello sviluppo di capacità di analisi strategica e previsionale

#Profili di comparazione

#Profili di comparazione

- Mia ricerca pubblicata il **05 dicembre 2013** sul sito del nostro Sistema di Informazioni per la Sicurezza della Repubblica. **L'Italia non è ricompresa**.
- Solo **29 dei 196 Stati** generalmente riconosciuti sovrani a livello internazionale hanno reso pubblica una propria *cyber-strategy* (oggi il numero complessivo è leggermente maggiore, non fosse altro per la pubblicazione del nostro documento strategico).
- Al 05 dicembre del 2013, **15 dei 28 Stati membri dell'Unione Europea** avevano pubblicato una *cyber-strategy*.

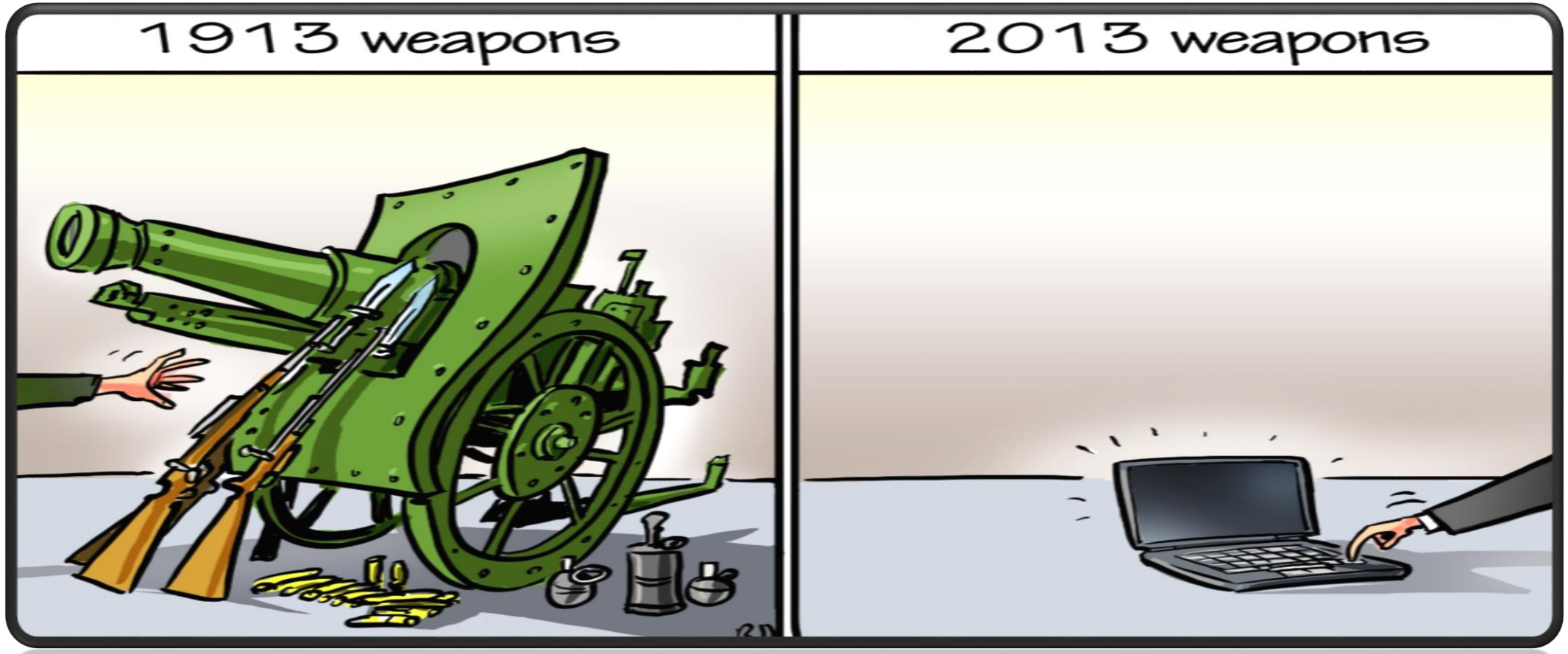
#Profili di comparazione

Dall'analisi del contenuto è possibile individuare alcuni **tratti comuni a tutte le *cyber-strategy* di matrice europea**. I principali pilastri strategici individuabili sono:

- **Stabilire trattati, leggi e regole** di condotta nazionali e/o internazionali ad hoc
- Sviluppare i **rapporti diplomatici e rafforzare le partnership internazionali**
- Focus sul **cyber-crime**
- Incrementare i livelli di **sicurezza, affidabilità e resilienza** delle reti e dei sistemi informatici
- Rafforzare la **condivisione delle informazioni** (anche tra pubblico e privato), l'*early warning* e le capacità di *incident response*

La strategia italiana, quindi, si **innesta perfettamente** e fa suoi tutti i principi comuni in ambito europeo.

#Conclusioni



DOMANDE..?

@MeleStefano s.mele@strategicstudies.it