Cyber Warfare 2014

Armi cibernetiche, sicurezza nazionale e difesa del business

a cura di Umberto Gori
e Serena Lisi

FrancoAngeli

Collana di Scienza Politica e Relazioni Internazionali, diretta da Umberto Gori

Il progresso delle scienze sociali è strettamente legato alla ricerca interdisciplinare. Tale indirizzo non ostacola però l'applicazione di un approccio e di un metodo rigorosamente unitari. L'approccio è quello dei sistemi, il metodo è quello della scienza politica più avanzata. L'uno e l'altro mirano a conoscere il reale nella sua complessità, a partire da dati e variabili fattuali, con l'ausilio, anche, di discipline diverse, teorie empiriche e quindi previsioni aventi valore probabilistico.
C'è una fortissima domanda, oggi, di strumenti aggiornati atti ad interpretare fenomeni complessi e talora privi di precedenti ed a consentirne la previsione, data l'accelerazione dei tempi storici.
A questa domanda la «Collana di Scienza Politica e Relazioni Internazionali» si propone, ambiziosamente, di rispondere, cercando anche di rimuovere, in misura progressiva, le resistenze, ancora vive nel nostro Paese, dovute al tradizionale convincimento che il campo sociale non sia coltivabile con gli strumenti euristici che hanno determinato lo sviluppo eccezionale delle scienze della natura.
La denominazione della collana si giustifica per due aspetti: primo, perché di solito quando si parla di scienza politica si pensa al quadro interno e qui invece si vuole accreditare la tesi che anche il sistema internazionale è analizzabile in tale prospettiva; secondo, perché anche per l'analisi corretta del sistema interno è ormai impensabile non fare un sistematico riferimento al contesto internazionale (e viceversa).
La collana svilupperà sia una parte di metodologia e di tecniche analitiche, sia una parte teorica e di ricerca sugli aspetti di sostanza del vasto campo preso in considerazione. Contribuiranno all'una e all'altra metodologi e scienziati politici, sociologi della politica e studiosi dell'amministrazione, comparatisti e cultori di relazioni internazionali.
La collana ha essenzialmente un taglio operativo. I suoi naturali destinatari saranno quindi, oltreché gli specialisti, anche tutti coloro che, ai diversi livelli, sono detentori di responsabilità decisionali. Scopo ultimo è infatti la progressiva «modernizzazione» dell'Italia nel campo della valutazione scientifica dei fatti politici, interni ed internazionali, che è premessa insieme di razionalizzazione dei processi decisionali e di un corretto funzionamento delle istituzioni e della vita democratica del Paese.

Cyber Warfare 2014

Armi cibernetiche, sicurezza nazionale e difesa del business

a cura di Umberto Gori
e Serena Lisi

FrancoAngeli

L'evento, articolato in due edizioni, ha avuto luogo l'11 giugno 2014 presso la Sala Gruppi della Camera dei Deputati e il 13 ottobre 2014 a Milano, presso l'Auditorium G. Testori Palazzo Lombardia. La Conferenza è stata ideata dal Centro Interdipartimentale Studi Strategici, Internazionali e Imprenditoriali (CSSII) dell'Università di Firenze, dall'Istituto per gli Studi di Previsione e le Ricerche Internazionali (ISPRI), dal Centro Studi Difesa e Sicurezza (CESTUDIS) e dal Centro di Ricerca di Cyber Intelligence and Information Security (CIS) de "La Sapienza" di Roma, d'intesa con Maglan Group – Information Defense and Technologies.

Si ringrazia Lorenzo Bonucci, studente dell'Università di Firenze,
per la collaborazione all'editing del volume.

Indice

Edizione di Roma – 11 Giugno 2014

L'inarrestabile sviluppo delle armi cibernetiche, di *Umberto Gori* pag. 11

Cyber Weapon – Offensive Observations for 2015-2017, di *Shai Blitzblau* » 19

Armi cibernetiche e strategie di difesa. Importanza della Societal Digital Security Culture, di *Antonio Colella* » 23

Cyber Defense, Cyber Intelligence e relative armi. Casi di collaborazione tra pubblica amministrazione, industria e ricerca finanziata dalla Commissione Europea, di *Alessandro Zanasi* » 39

Centro Intelligence Interforze. Il reparto SMD Operazioni e strumenti di intelligence nel cyberspace, di *Giandomenico Taricco* » 53

Cyber Electronic Warfare: la spinta dello Spettro Elettromagnetico nel 5° dominio, di *Daniela Pistoia* » 57

Cultural e Cyber Intelligence, la Nuova Alleanza? , di *Alessandro Zanasi* » 69

Edizione di Milano – 13 ottobre 2014

Dall'intelligence economica alla cyber intelligence: sfide e promesse per le imprese, di *Umberto Gori* » 85

La cyber intelligence nel contesto del quadro strategico, di *Luigi Ramponi* pag. 97

Maglan Cyber Intelligence (CyberINT) Gathering and Operations 2012-2014, di *Shai Blitzblau* » 106

La Cyber-security in ambiente bancario, di *Massimo Milanta* » 110

Cyber intelligence e successo del business: la nuova sfida manageriale per le PMI in uno scenario che cambia, di *Luciano Hinna* » 114

Darknet e Cyber Intelligence, di *Lino Buono* » 128

Digital Forensic Intelligence, di *Davide Gabrini* » 134

La tutela del mercato musicale e discografico tra Cyber Intelligence e tecnologia, di *Marco Signorelli* » 145

Commento agli interventi della sessione milanese, di *Giancarlo Grasso* » 153

Cyber Intelligence nelle grandi aree metropolitane: l'esperienza di Milano, di *Tullio Mastrangelo* e *Andrea Carobene* » 155

Postfazione, di *Ferdinando Sanfelice di Monteforte* » 161

Data Mining e Sociale Network Analysis: gli strumenti al servizio della cyber intelligence, di *Luigi Martino* e *Samuele Foni* » 165

Lista degli acronimi » 185

Riferimenti bibliografici » 187

Indice analitico » 191

Riconoscimenti

Adesione del Presidente della Repubblica

Patrocini

Senato della Repubblica
Presidenza del Consiglio dei Ministri
Ministero dell'Interno
Ministero della Difesa
Ministero dello Sviluppo Economico
Ministero delle Infrastrutture e dei Trasporti

Promotori

Centro interdipartimentale di Studi Strategici, Internazionali e Imprenditoriali dell'Università di Firenze (CSSII)

Centro Studi Difesa e Sicurezza (CESTUDIS)

Centre of Research of Cyber Intelligence and Information Security (CIS)

Istituto per gli Studi di Previsione (ISPRI)

Ideata d'intesa con Maglan – Information Defense & Intelligence

Con la sponsorship di FORTINET, Alenia Aermacchi

Medaglia di Rappresentanza, con firma del Presidente della Repubblica Giorgio Napolitano, inviata al Prof. Umberto Gori, direttore scientifico della Conferenza, in segno di apprezzamento per l'iniziativa.

Edizione di Roma

11 Giugno 2014

L'inarrestabile sviluppo delle armi cibernetiche

di *Umberto Gori*[*]

Autorità, Signore e Signori,

è questa la quinta volta che le nostre rispettive Istituzioni Vi invitano a riflettere sui problemi della sicurezza cibernetica al fine di far avere al nostro Paese una sempre maggiore consapevolezza sui rischi, minacce esfide che lo sviluppo tecnologico pone dinanzi alle nostre società e ad ognuno di noi.

Oggi Vi è stato consegnato il volume della Conferenza 2013, intitolato La protezione cibernetica delle infrastrutture nazionali, ultimo di una serie che comprende, dal più al meno recente, titoli come Armi cibernetiche e processo decisionale (2012), La sfida della cyber intelligence al sistema Italia: dalla sicurezza delle imprese alla sicurezza nazionale (2011), Le nuove sfide provenienti dal cyberspazio alla sicurezza nazionale italiana (2010). Titoli, questi ultimi, a loro volta preceduti da Invisible Threats: Financial and Information Technology Crimes and National Security e da Modelling Cyber Security: Approaches, Methodology, Strategies, risultato di iniziative svolte d'intesa con il Programma "Security through Science" della NATO.

La domanda a questo punto è: perché insistere ancora a parlare delle armi cibernetiche ? La risposta è molto semplice: minacce sempre più sofisticate e sempre più frequenti sono dirette nei confronti di molti Stati i quali, a loro volta, spendono sempre di più per lo sviluppo di nuove armi cyber, difensive ed offensive. Secondo stime di istituti internazionali specializzati (Market Info Group LLC), nel decennio 2014 – 2024, il mercato globale delle cyber weapons supererà la cifra astronomica di 4 trilioni di dollari, ossia 4.000 miliardi di dollari o 3000 miliardi di Euro (equivalenti

* Professore Emerito, Università degli Studi di Firenze. Presidente del CSSII., Direttore Istituto per gli Studi di Previsione e le Ricerche Internazionali ISPRI.

Il presente scritto è la riproduzione del discorso originale pronunciato dall'Autore alla Conferenza.

a poco meno di 6 milioni di miliardi di vecchie lire). Questa cifra è calcolata sulla base 1) del numero sempre crescente di minacce alle principali industrie e infrastrutture critiche, 2) dell'aumento delle spese per la difesa, 3) delle iniziative aziendali e 4) della preferenza sempre più netta accordata dai Governi alle armi cibernetiche offensive come strumenti bellici.

Attualmente, gli Stati che sono all'avanguardia nel settore sono, oltre agli Stati Uniti, la Cina e la Russia, anche le due Coree e l'Iran. Per quanto riguarda il futuro, ci aiuta una intelligente riflessione di una nota studiosa statunitense, Nazli Choucri, la quale, sulla base di ricerche effettuate dall'MIT, sostiene che per capire quali saranno gli Stati che nel futuro saranno protagonisti nel settore cyber, occorre considerare il peso, le interazioni, la collocazione e la dinamica di tre fattori: la popolazione, la tecnologia e le risorse. Una volta classificati gli attori statali in funzione di tali fattori, risultano sei profili che ci permettono di prevedere l'intensità della loro attività in campo cibernetico. I profili sono:

Profilo 1 : risorse, popolazione, tecnologia
Profilo 2 : popolazione, risorse, tecnologia
Profilo 3 : popolazione, tecnologia, risorse
Profilo 4 : risorse, tecnologia, popolazione
Profilo 5 : tecnologia, risorse, popolazione
Profilo 6 : tecnologia, popolazione, risorse.

Senza voler in questa sede perdere del tempo con un'analisi particolareggiata, basterà dire che gli Stati che vengono confermati o indicati come protagonisti nel settore sono, fra gli altri, USA, Cina, India, Austria, Francia, Danimarca, Finlandia, Norvegia, Polonia, Russia, Svezia, Australia, Messico. Stranamente, non viene citata la Germania.

La domanda ora è: in quale gruppo si situa l'Italia ?

A mio avviso, l'Italia si situa potenzialmente nel gruppo dei Paesi leader perché, anche se fortemente dipendente da importazione di risorse, è notevolmente dotata di tecnologia. Ne è dimostrazione, ad esempio, il programma NCIRC (Computer Incident Response Capability) di Selex ES in collaborazione con Northrop Grumman, scelto dalla NATO per la copertura della sicurezza di 50 siti NATO in 28 Paesi, nonché il nuovo Centro Selex ES per la sicurezza cibernetica di Chieti. Se il nostro Paese non è certo ai primi posti per capacità di difesa cibernetica è solo, in gran parte, per il fatto che solo da un anno o poco più l'Italia si è data uno strumento per la protezione delle infrastrutture critiche, (il DPCM 24 gennaio 2013) – di cui dobbiamo dar merito al qui presente Senatore Ramponi – seguìto, in quanto ivi previsti, dal Quadro strategico nazionale per la sicurezza dello spazio cibernetico e dal Piano nazionale per la protezione cibernetica e la sicurez-

za informatica, adottati ambedue in data 27 gennaio di quest'anno dal Governo Letta. Il primo di questi due documenti, elaborati dal CISR(Comitato interministeriale per la sicurezza della Repubblica) elenca le principali minacce informatiche, mentre il secondo indica le priorità e gli obiettivi, oltre a individuare i corsi d'azione necessari a dar concretezza al Quadro strategico. Da notare, fra l 'altro, che i cd 'soggetti economici', pubblici o privati che siano, hanno d'ora in poi l'obbligo di informare di ogni violazione informatica il CERT nazionale. Peccato che il Computer Emergency Response Team ancora non sia operativo presso il MISE. Il paradosso è che l'Italia ha avviato altri due progetti oltre a quello del CERT presso il MISE: 1) il CERT della Pubblica Amministrazione presso l'Agenzia per l'Italia Digitale; 2) il Nucleo di Sicurezza Cibernetica presso l'Ufficio del Consigliere Militare alla Presidenza del Consiglio dei Ministri. Comunque sia, mi sembra corretto il punto di vista di Andrea Rigoni, Direttore Generale del Global Cyber Security Center, il quale sostiene che l'esistenza di uno o più CERT non assicura la protezione dalle minacce. La Gran Bretagna ed Israele, ad esempio, Paesi avanzatissimi per ciò che concerne la protezione dalle minacce cyber, non dispongono di un CERT nazionale, ma hanno investito fior di miliardi in programmi di difesa cyber. La stessa Estonia, che nel 2007 disponeva già di un CERT, non è riuscita a salvarsi dall'ormai famoso attacco DDoS. Stupisce che qui si abbia la sensazione che con tre (e più) CERT si possa stare tranquilli. E ancor più stupisce l'idea che la difesa possa attuarsi "senza costi aggiuntivi" e con "fabbisogno finanziario annuo" uguale a zero.

Fra i Paesi sopra indicati, la Cina sembra avere la più grande possibilità di sviluppo. Secondo statistiche recenti, in Cina gli utilizzatori di Internet sono circa 400 milioni, pari a 1/3 della popolazione, con un aumento di 50 milioni di utenti per ogni anno, a fronte dei 250 milioni di utenti USA, pari all'80% della popolazione.

A livello globale, su una popolazione stimata al 2020 di 7,5 miliardi, si prevede che vi saranno 4,8 miliardi di internauti.

Questi numeri fanno ragionevolmente temere che il cyberspazio provocherà nuovi tipi di conflitto internazionale: un primo tipo di conflitto verterà su chi decide le regole del gioco, perché chi decide le regole controlla il gioco e chi controlla la Rete controlla il mondo. Qui si profila il grande scontro fra gli attualmente egemoni USA e la sfidante Cina. Un secondo tipo di conflitto sarà teso alla ricerca di vantaggi politici e di profitto, ivi incluso il controllo sui contenuti, sull'accesso, etc.

Il ricorso alle cyber weapons sarà sempre più importante anche a causa dei costi veramente minimi delle armi cibernetiche offensive rispetto a

quelle cinetiche. Mentre un aereo da caccia di quinta generazione costa da 80 a 120 milioni di dollari e un missile cruise da 1 a 2 milioni, un'arma cibernetica offensiva costa – si valuta – da 300 a 50.000 dollari USA. Oltre al basso costo, le cyber weapons sono a basso rischio, sono efficaci, lanciabili da qualsiasi parte del mondo, garantiscono, o quasi, l'anonimato anche perché dispongono di tecniche di mimetizzazione ben superiori a quelle possibili per le armi convenzionali. Devono di solito, inoltre, a differenza di molte armi tradizionali, essere prodotte rapidamente caso per caso e sono utilizzabili una sola volta perché debbono essere tarate su singoli obiettivi specifici. Le cyber weapons offensive sono di tre tipi: semplici, moderatamente complesse e complesse, e ciò in funzione della conoscenza ottenuta sui sistemi di controllo dell'obiettivo: nel primo caso si sfrutta direttamente la mancanza di autenticazione; nel secondo si procede preliminarmente a individuare il processo di controllo; e nel terzo il processo stesso viene furtivamente alterato con la conseguenza che il bersaglio non si rende conto del pericolo. (Per maggiori notizie si veda Dale Peterson, Offensive Cyber Weapons – Construction, Development, and Employment, in: "The Journal of Strategic Studies", febbraio, 2013). E dato che molte strutture sono isolate dal vettore Internet, vengono studiate altre soluzioni, fra le quali – a parte le chiavette USB – l'uso di segnali radio per inserire malware in remoto.

L'uso di armi cibernetiche presenta però anche dei delicati problemi. Ad esempio, può essere limitato in zone critiche al fine di evitare danni collaterali a strutture civili (ospedali, etc.) e anche perché un codice distruttivo, tramite tecniche di reverse engineering, può essere rimbalzato contro il mittente.

Le cyber weapons difensive sono invece estremamente più costose. Difendersi, in altre parole, ha un prezzo molto più alto. Ecco perché le difese dovrebbero sottostare al criterio del pooling and sharing.

Non sarà invece possibile, almeno per ora, difenderci nei confronti degli attacchi provenienti dalla cd 'Internet delle cose', e cioè – ad esempio – da tutti quegli apparecchi domestici tipo tv e frigoriferi etc. di ultima generazione capaci di interconnettersi con la Rete. L'impossibilità deriva dal fatto che le case costruttrici non hanno pensato a dotarli di dispositivi di protezione e che non è possibile dotarli di antivirus. Il problema è che possono fungere da botnet.

E veniamo adesso, rapidamente, al concetto di arma cibernetica di cui non vi è ancora una definizione accettata a livello internazionale. Chi Vi parla ha proposto, in una delle Conferenze precedenti, una definizione restrittiva del concetto. E cioè, molto semplicemente, uno strumento informatico costituisce una cyber weapon se, e soltanto se, ha una valenza almeno

potenzialmente letale, e cioè distruttiva di cose o persone. Solo questa caratteristica – la letalità – determina oggettivamente l'appartenenza dello strumento cibernetico (genus) alla species 'arma'. La presenza di altre condizioni non ha la stessa rilevanza. Pertanto, definizioni che includono strumenti come, ad esempio, il DDoS possono essere utili solo con riferimento alla categoria delle 'armi non letali'. D'altra parte, anche chi sostiene tali definizioni non può fare a meno di affermare che "unica vera cyber-arma attualmente conosciuta" è Stuxnet, l'unico software capace – almeno finora – di danneggiare fisicamente l'infrastruttura critica di una nazione sfruttando i sistemi informatici che la governano"(S. Mele, I princìpi strategici delle politiche di cybersecurity).

Definizione cyber arma di S. Mele: "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".

Prendiamo ad esempio i malware Stuxnet, Duku, Flame e Gauss, per citare solo questi. Secondo l'uso internazionale, tutti e tre sono definiti 'cyber weapons', ma – a rigore – solo Stuxnet, finora, ha dimostrato di avere capacità letali. Duku , Flame e anche Gauss, pur rassomigliando per certi aspetti a Stuxnet, tanto è vero che gli Stati che li hanno prodotti sono quasi certamente gli stessi, hanno finalità spionistiche, si attivano per rubare informazioni, talora prevalentemente specifiche e su determinate regioni del mondo, propedeutiche a possibili successivi attacchi cyber. Gauss, ad esempio, si concentra su istituzioni finanziarie del Libano e del Medio Oriente. Anche Flame, pur avendo una complessità 100 volte superiore a quella dei normali virus, non svolge che una attività di spionaggio. Gauss, però, presenta altre caratteristiche, alcune note, come la capacità di infettare ma anche di 'disinfettare' in certe occasioni e di incamerare informazioni in file nascosti; altre invece, sicuramente presenti, ma ancora inspiegabili, come informano i Laboratori Kasperski. Non è da escludere, quindi, che anch'esso possa esibire in futuro capacità letali. Il fatto che questi strumenti vengano spesso scoperti anni dopo rispetto alla loro entrata in funzione dimostra che non possiamo stare tranquilli su ciò che ci serba l'avvenire, tanto più che, come risulta ad InfoSec, almeno 140 Stati stanno più o meno segretamente lavorando sul settore. Gli Stati Uniti, tramite la DARPA (Defense Advanced Research Projects Agency), risulta stiano sviluppando un sistema capace di pre-programmare una cyber war automatica, senza cioè intervento umano (Piano X) al fine di velocizzare, fino ad annullare i tempi

di reazione, le procedure di attacco e di difesa. Ciò, ovviamente, pone problemi giuridici, etici e pratici di indubbia rilevanza. Si ripeterebbe qui il pericolo già evidenziato con il progetto di Strategic Defence Initiative di lasciare alle macchine il compito di scrivere il destino del genere umano.

Ovviamente, l'assenza di una definizione di cyber weapon concordata a livello internazionale ha come conseguenza il non poter stabilire un quadro giuridico capace di valutare oggettivamente la gravità della minaccia e le responsabilità dell'aggressore e lasciare tali valutazioni alla discrezionalità degli Stati, fatto – questo – che aumenta a dismisura i pericoli di escalation a livello cinetico. Un tentativo di risolvere problemi del genere è stato fatto con il Tallin Manual on the International Law Applicable to Cyber Warfare redatto da un gruppo internazionale di esperti indipendenti.

Nei Paesi più avanzati in tema di sicurezza cibernetica si è cominciato a riflettere se non sia il caso di passare da una difesa reattiva di tipo tattico ad una difesa di tipo strategico. È però la natura stessa dell'arma cyber che fa concludere a molti che non vi sia una significativa differenza fra l'uso tattico e quello strategico. L'interconnessione delle reti fa sì che gli effetti di un attacco concepito come tattico non possano essere comunque limitati. Inoltre, un bersaglio interessante dal punto di vista tattico potrebbe essere considerato più utile in prospettiva strategica. Questo, grosso modo, è il tipo di ragionamento che fa ritenere giusta ai più la tesi della indifferenziazione, o – più esattamente – la correttezza del solo uso strategico delle cyber weapons.

Qui emergono due altri problemi:

1) come si fa a decidere che un cyber attacco è una cyber war ?

2) è possibile una qualche forma di deterrenza in era cyber ?

una possibile risposta a questi due quesiti può essere molto rapida in quanto è stata già proposta dal sottoscritto nella terza conferenza, due anni fa. e cioè, in sintesi estrema, per ciò che concerne il primo quesito occorre valutare:

a) se dietro l'attacco non ci sia uno Stato (qui soccorre l'esame del contesto situazionale e strategico);

b) le conseguenze (tipo dei danni, quanto gravi, per quanto tempo);

c) la motivazione (l'attacco è politico ? risponde, cioè, a logiche di Realpolitik ?);

d) la complessità di pianificazione e di esecuzione. Alla seconda domanda rispondo, stante l'assoluta diversità del contesto nucleare nei confronti del contesto cibernetico, che la validità di una deterrenza by punishment declina con il diminuire del livello di organizzazione formale del potenziale attaccante. Resta invece possibile una cyber deterrenza by denial

che consiste nell'attivazione di strategie e tecnologie di difesa cyber atte ad impedire a potenziali avversari di colpire le nostre strutture che devono essere quanto più possibile resilienti e flessibili. Sarà comunque importante un approfondimento delle teorie sulla deterrenza in contesto cibernetico.

Infine – e chiudo – con i documenti cui abbiamo accennato, il Quadro strategico nazionale per la sicurezza dello spazio cibernetico e il Piano nazionale per la protezione cibernetica e la sicurezza informatica, l'Italia – vi si dice – "si dota di una strategia organica". A parte la stranezza di definire una strategia "organica" (una strategia o è tale o non è), la mia impressione è che si sia messo in moto un meccanismo che individua genericamente le varie minacce e alcune linee di azione (i cd 6 "indirizzi strategici") per attuare le quali vengono enunciati 11 "indirizzi operativi" specificati nel Piano e si attribuiscono specifici compiti ai diversi organi dello Stato che devono giustamente operare anche in collaborazione con il settore privato. Tutto ciò è indubbiamente molto utile. ma ancora, a mio avviso, l'Italia non ha ancora una vera strategia, se per strategia s'intende – come io credo – un piano d'azione completo nel senso che vengono esplorate tutte le possibili soluzioni di una certa situazione con tutte le loro relative conseguenze, attribuendo ad ogni soluzione possibile, e quindi ad ogni relativa conseguenza, un quantum di utilità. Questa mia interpretazione deriva direttamente dalla più precisa definizione del concetto di strategia elaborata da von Neumann e Morgenstern nel famoso libro Theory of Games and Economic Behaviour:

"Immaginiamo che il giocatore, anziché prendere una decisione quando ciò diventa necessario, rifletta in anticipo a tutte le eventualità concepibili, cioè che il giocatore cominci a giocare con un piano completo: un piano che determina la scelta che egli farà in ogni situazione possibile, e per ogni informazione di cui disporrà a quel momento (…). Un tale piano noi lo definiamo una strategia".

Ebbene, è questo 'piano' che ancora manca. E in un contesto dove la risposta deve essere immediata non è una mancanza da poco. La mia speranza è che questa mia conclusione sia frutto della mia non conoscenza di effettive strategie che di per sé debbono rimanere riservate.

Grazie.

Cyber Weapon - Offensive Observations for 2015-2017

di *Shai Blitzblau*[*]

Preface

The business dictionary[1] defines *Forecasting* as a planning tool that helps management and command layers in their attempts to cope with the uncertainty of the future, relying mainly on data from the past and present and analysis of trends. Forecasting starts by establishing certain assumptions based on the command cadre or management's experience, knowledge, and judgment. Forecasting is an essential tool for the global cyber weapons industry.

In fact, the global cyber weapons industry is driven by a combination of ever-increasing threats to essential industries and critical infrastructures, growing defense spending, corporate IT efforts, and the evolution of offensive Cyber Weapons as a preferred military weapon[2].

Cyber Weapons forecasting is highly complicated, since the cyber world is highly dynamic, rapidly developed and frequently changed, for example: every 48 hours a new computer malware is created, a mean of 25 IT and cyber vulnerabilities are found every 25 days and at least 5 million cyber-attacks occur monthly against the Italian governmental internet-networks.
IT and Cyber forecasting is broadly discussed by professional forecasters based on extensive research and mathematical models, while an enormous number of commercial IT and Cyber security companies publish glorified annual forecasts, mainly to achieve marketing objectives and promote their

* Maglan Information Defence Technologies Ltd.

Il presente contributo è tratto dalla sbobinatura dell'intervento originale dell'autore, con sua revisione.

[1] http://www.businessdictionary.com/definition/forecasting.html

[2] http://www.researchandmarkets.com/reports/2673398/offensive_and_defensive_cyber_weapons_for#description