Osservatorio
Inforwarfare e
tecnologie emergenti

ISTITUTO ITALIANO
DI STUDI STRATEGICI
ITALIAN INSTITUTE
OF STRATEGIC STUDIES
Niccolò Machiavelli

CYBERWEAPONS
ASPETTI GIURIDICI E STRATEGICI

Stefano Mele

Aprile 2012

EDIZIONI MACHIAVELLI

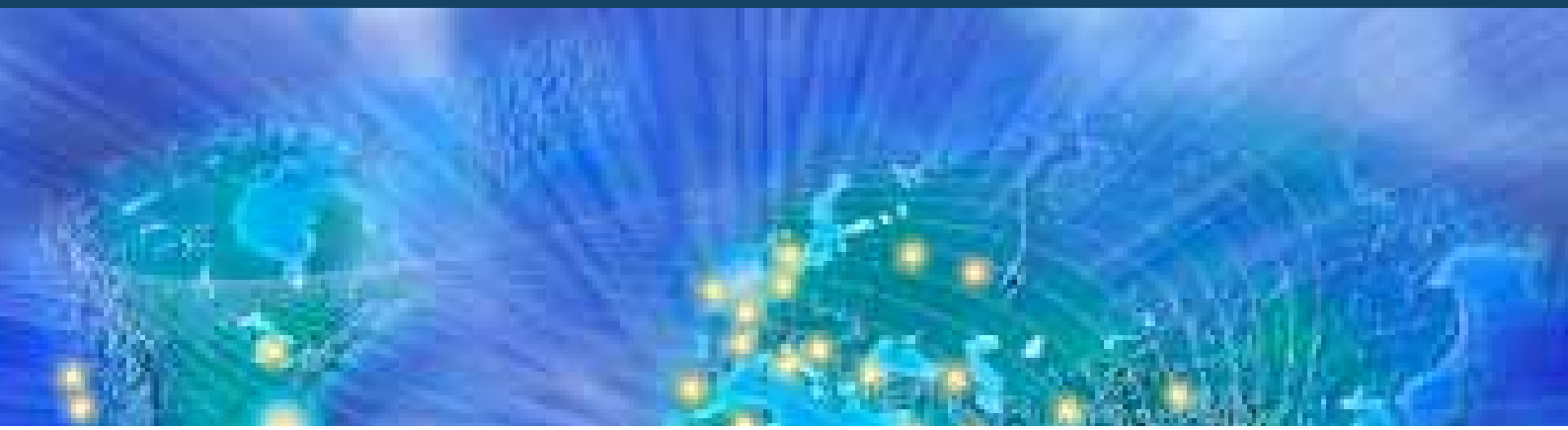
AUTORE

Stefano Mele

è Coordinatore dell'Osservatorio *Infowarfare* e Tecnologie Emergenti dell'Istituto Italiano di Studi Strategici "Niccolò Machiavelli".

Avvocato specializzato in Diritto delle Tecnologie, Privacy, Sicurezza ed Intelligence presso Carnelutti Studio Legale Associato.

E' esperto di *cyber-security* e *cyber-warfare* e direttore di ricerca del Centro Militare di Studi Strategici del Ministero della Difesa. Ha conseguito il Dottorato di ricerca presso l'Università degli Studi di Foggia.



1. Stuxnet

L'utilizzo del *worm* Stuxnet[1] per attaccare gli impianti nucleari di Bushehr[2] e Natanz[3] in Iran ha segnato un punto di svolta netto nel dibattito circa la possibilità, fino ad allora meramente teorica, di danneggiare un'infrastruttura critica di uno Stato penetrandola attraverso la rete Internet.

La prima variante del *worm* è apparsa nel giugno del 2009, ma quello che sarebbe poi stato ribattezzato con il nome di Stuxnet è stato rilevato per la prima volta a metà giugno 2010 dalla società bielorussa VirusBlokAda. Il *worm* ha come obiettivo i sistemi informatici industriali costruiti dalla società tedesca Siemens e, benché Stuxnet non sia il precursore degli attacchi informatici a questo genere di sistemi[4], vanta in assoluto di essere il primo *malware* appositamente progettato con l'intenzione di spiare, sabotare e riprogrammare in maniera del tutto autonoma il suo obiettivo[5].

Per quanto il principale veicolo d'infezione di Stuxnet siano i sistemi Microsoft Windows e, pertanto, il *malware* si sia diffuso e continuerà a diffondersi – fino al 24 giugno 2012, data in cui si auto-cancellerà – in maniera indiscriminata su ciascuna macchina che presenti determinate vulnerabilità (i c.d. "bug"), il software è programmato per "attivarsi" solo nel momento in cui arrivi ad infettare un sistema SCADA[6] WinCC7, PCS[7] o STEP7[8] della Siemens deputato alla gestione e al controllo di determinati processi industriali. Stuxnet, infatti, ha come obiettivo primario quello di arrivare ai PLC[9] (*Programmable Logic Controller*) dell'impianto SCADA, infettando l'applicazione "Step-7" utilizzata per la loro programmazione[10].

1- Per un'analisi completa ed esaustiva degli aspetti tecnici del worm Stuxnet, Marco De Falco, "Stuxnet Facts Report - A Technical and Strategic Analysis", Final draft version v.2.4, 2012.
2- Paul Woodward, "Iran confirms Stuxnet found at Bushehr nuclear power plant", 2010, in http://warincontext.org/2010/09/26/iran-confirms-stuxnet-found-at-bushehr-nuclear-power-plant/.
3- Foreign Policy, "6 mysteries about Stuxnet", 2010, in http://blog.foreignpolicy.com/posts/2010/09/27/6_mysteries_about_stuxnet.
4- Computer World, "Siemens: Stuxnet worm hit industrial systems", 2010, in http://www.computerworld.com/s/article/print/9185419/Siemens_Stuxnet_worm_hit_industrial_systems.
5- Per approfondire lo studio dell'argomento sotto i numerosi punti di vista posti dalla materia, Symantec, "W32 Stuxnet Dossier", 2011, in http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf; CSFI, "Stuxnet Report", 2010, in http://www.csfi.us/?page=stuxnet; Antiy CERT, "Report on the Worm Stuxnet Attack", 2010, in http://www.antiy.net/en/research/report_on_the_worm_stuxnet_attack.html; Eric Byres, "Analysis of the Siemens WinCC / PCS7 "Stuxnet" Malware for Industrial Control System Professionals", 2010, in http://www.tofinosecurity.com/professional/siemens-pcs7-wincc-malware; ESET, "Stuxnet Under the Microscope", 2010, in http://go.eset.com/us/resources/white-papers/Stuxnet_Under_the_Microscope.pdf; Ralph Langner, "How to Hijack a ControllerWhy Stuxnet Isn't Just About Siemens' PLCs", 2011, in http://www.controlglobal.com/articles/2011/IndustrialControllers1101.html.
6- In estrema sintesi, i sistemi SCADA (Supervisory Control And Data Acquisition), come dice l'acronimo, sono quei sistemi deputati al monitoraggio e controllo infrastrutturale o dei processi industriali.

Stando ai dati reperibili su fonti aperte, Stuxnet è riuscito a infettare ad oggi più di 100.000 *computer*, oltre la metà dei quali residenti fisicamente su territorio iraniano[11].

Paese	Percentuale d'infezione
Iran	58.85%
Indonesia	18.22%
India	8.31%
Azerbaijan	2.57%
Stati Uniti	1.56%
Pakistan	1.28%
Altri	9.2%

L'intera comunità internazionale di esperti, inoltre, è concorde nel valutare il processo che ha portato alla realizzazione di Stuxnet come un impegno di forza-lavoro[12] di molti mesi – tra sei[13] e dodici[14] – da parte di un team di programmatori specializzati in diverse discipline e capaci di avere una conoscenza diretta del funzionamento dei sistemi bersaglio e dei processi industriali gestiti[15].

Stuxnet, infatti, è un *worm* certamente complesso, ma comunque meno sofisticato di quanto la stampa abbia lasciato credere al grande pubblico[16]. Tuttavia, tutte le *security company* e gli esperti di sicurezza indipendenti sono sostanzialmente unanimi nell'assegnare la paternità del *worm* ad uno Stato dotato di notevoli fondi[17] e forti motivazioni politico-militari[18].
Israele[19] e gli Stai Uniti[20] sarebbero, allo stato attuale, i maggiori indiziati della sua realizzazione, laddove non è da escludere anche un ruolo della *cyber-criminalità* russa in una o più fasi della sua realizzazione[21].

Tuttavia, quello che a prima vista appare essere un dibattito strettamente riservato agli aspetti tecnico-tattici della materia, serba in sé aspetti strategici e giuridici di primaria importanza, nei confronti dei quali studiosi e decisori sono chiamati a dare con urgenza delle risposte.

7- Ralph Langner, "Ralph's Step-By-Step Guide to Get a Crack at Stuxnet Traffic and Behaviour", 2010, in http://www.langner.com/en/2010/09/14/ralphs-step-by-step-guide-to-get-a-crack-at-stuxnet-traffic-and-behavior/.
8- Nicolas Falliere, "Stuxnet Infection of Step 7 Projects", 2010, in http://www.symantec.com/connect/blogs/stuxnet-infection-step-7-projects.
9- Si tratta dei computer deputati all'esecuzione di un programma per l'elaborazione dei segnali digitali ed analogici provenienti da sensori e diretti agli attuatori presenti in un impianto industriale.
10- Steven Cherry and Ralph Langner, "How Stuxnet Is Rewriting the Cyberterrorism Playbook", 2010, in http://spectrum.ieee.org/podcast/telecom/security/how-stuxnet-is-rewriting-the-cyberterrorism-playbook.
11- Symantec, "W32 Stuxnet Dossier", 2011, cit..
12- Marco De Falco, "Stuxnet Facts Report - A Technical and Strategic Analysis", cit..
13- The Guardian, "Stuxnet worm is the 'work of a national government agency'", 2010, in http://www.guardian.co.uk/technology/2010/sep/24/stuxnet-worm-national-agency
14- Wired, "Blockbuster Worm Aimed for Infrastructure, But No Proof Iran Nukes Were Target", 2010, in http://www.wired.com/threatlevel/2010/09/stuxnet/
15- Computer World, "Is Stuxnet the 'best' malware ever?", 2010, in http://www.computerworld.com/s/article/9185919/Is_Stuxnet_the_best_malware_ever
16- Lukas Milevski, "Stuxnet and Strategy: A Space Operation in Cyberspace?", in JFQ (Joint Force Quarterly), issue 63, 4th quarter 2011.
17- NYTimes, "A Silent Attack, but Not a Subtle One", 2010, in http://www.nytimes.com/2010/09/27/technology/27virus.html.
18- BBC, "Stuxnet worm 'targeted high-value Iranian assets'", 2010, in http://www.bbc.co.uk/news/technology-11388018.
19- The Economist, "A cyber-missile aimed at Iran?", 2010, in http://www.economist.com/blogs/babbage/2010/09/stuxnet_worm
20- Ralph Langner, "Cracking Stuxnet, a 21st-century cyber weapon", 2011, in http://www.ted.com/talks/ralph_langner_cracking_stuxnet_a_21st_century_cyberweapon.html
21- The Diplomat, "Was Russia Behind Stuxnet?", 2011, in http://the-diplomat.com/2011/12/10/was-russia-behind-stuxnet/

L'aspetto strategicamente più rilevante di Stuxnet e che occorre in prima battuta evidenziare, allora, è quello relativo alla convergenza – per la prima volta – **tra azioni tipiche di cyber-crime e interessi statali**. Con Stuxnet, infatti, pare prendere forma "tangibile" quella linea dottrinale, sempre più consolidata, che vede gli Stati impegnati a capitalizzare il più possibile gli investimenti in materia di ricerca tecnica, tecnologica e di *know-how* sulla sicurezza informatica portati avanti principalmente da gruppi di ricercatori indipendenti e, soprattutto, da gruppi di criminali informatici. Occorre sottolineare, infatti, che quasi tutte le più significative azioni condotte attraverso il *cyber-spazio* dal 2006 ad oggi[22] sono intimamente legate al lavoro di ricerca, alle tecniche e ai codici di programmazione sviluppati dalla comunità internazionale dei *cyber-criminali*[23]. Peraltro, pare sempre più rafforzarsi l'idea[24] che siano proprio i gruppi di criminali informatici ad essere i destinatari privilegiati da parte di alcuni Governi[25] del sub-appalto di determinate azioni condotte nel *cyber-spazio* al di fuori della legalità.

Non può stupire, allora, come nel corso del tempo sia nato e si vada sempre più estendendo un vero e proprio "mercato nero" delle vulnerabilità informatiche presenti nei *software* più utilizzati e non ancora pubblicamente conosciute (i c.d. "*zero-day*" o "*0-day*").

Per avere chiaro un indice dei valori economici connessi a questo giro d'affari clandestino, indicativa può essere la seguente tabella, pubblicata all'esito di una recente indagine di Forbes[26] e riferita ad una forbice di prezzo indicativa per ogni singolo *zero-day* scoperto e posto in vendita.

ADOBE READER	$5,000–$30,000
MAC OSX	$20,000–$50,000
ANDROID	$30,000–$60,000
FLASH OR JAVA BROWSER PLUG-INS	$40,000–$100,000
MICROSOFT WORD	$50,000–$100,000
WINDOWS	$60,000–$120,000
FIREFOX OR SAFARI	$60,000–$150,000
CHROME OR INTERNET EXPLORER	$80,000–$200,000
IOS	$100,000–$250,000

22- CSIS (Center for Strategic and International Studies), "Significant Cyber Incidents", aggiornato al 16 marzo 2012, in http://csis.org/publication/cyber-events-2006
23- ames P. Farwell & Rafal Rohozinski, "Stuxnet and the Future of Cyber War", in Survival: Global Politics and Strategy, vol. 53, no. 1, February–March 2011.
24- Stefano Mele, "Cyber-warfare e danni ai cittadini", 2010, in http://www.stefanomele.it/publications/dettaglio.asp?id=168
25- Northrop Grumman Corp, "Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage", 2012, in http://www.uscc.gov/RFP/2012/USCC%20Report_Chinese_CapabilitiesforComputer_NetworkOperationsandCyberEspionage.pdf; US–China Economic and Security Review Commission, "2009 Report to Congress", 2009, in http://www.uscc.gov/annual_report/2009/annual_report_full_09.pdf; Alexander Klimburg, "Mobilising Cyber Power", in Survival: Global Politics and Strategy, vol. 53, no. 1, February–March 2011.
26- Forbes, "Shopping For Zero-Days: A Price List For Hackers' Secret Software Exploits", 2012, in http://www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits/

2. Riflessioni giuridiche sulle *cyber-weapon* e loro definizione

In via preliminare, inquadrare dal punto di vista giuridico il concetto di *cyber*-arma risulta ormai un sforzo di primaria importanza per avere la possibilità di valutare correttamente sia il livello di minaccia proveniente da un attacco informatico, che le eventuali responsabilità politiche e giuridiche ascrivibili a chi ha agito. Questo anche in considerazione del costo sopportato da un'azienda per ogni violazione della sicurezza dei suoi sistemi informatici, che, in un recentissimo studio americano[27], è stato stimato essere nel 2011 in media di 5.5 milioni di dollari, con un costo di 194 dollari per ogni singola informazione sottratta.

Sinteticamente, 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.

Contestualmente, 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, peraltro, si rileva a livello internazionale, dove le normative attualmente in vigore definiscono sempre e solo il concetto di arma, ma non quello di cyber-arma. Addirittura il *Dictionary of Military and Associated Terms*[28] del Dipartimento della Difesa americano, costituito da 550 pagine di definizioni rilevanti per il settore della Difesa, non contiene una **specifica definizione di arma**, né tantomeno quella di *cyber-arma*, limitandosi a definire esclusivamente le armi non letali[29].

27- Ponemon Institute and Symantec, "2011 Cost of Data Breach Study: United States", 2012, in http://www.symantec.com/content/en/us/about/media/pdfs/b-ponemon-2011-cost-of-data-breach-us.en-us.pdf
28- DoD Dictionary of Military and Associated Terms, in http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf
29- Definita come "a weapon that is explicitly designed and primarily employed so as to incapacitate personnel or materiel, while minimizing fatalities, permanent injury to personnel, and undesired damage to property and the environment".

Tuttavia, a **livello ontologico**, un'arma può essere anche un concetto puramente astratto e non per forza materiale (addirittura le parole, in alcuni contesti, possono essere usate come vere e proprie armi), ovvero, per ciò che rileva ai fini di questa ricerca condotta dall'Istituto Italiano di Studi Strategici "Niccolò Machiavelli", 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*. Pertanto, nonostante l'immaterialità di questo genere di armi, ciò su cui realmente occorre porre l'attenzione sono tre elementi: il **contesto**, lo **scopo** e il **soggetto/oggetto soccombente**; gli unici utili, nei fatti, a qualificare o meno – sempre a livello ontologico – questo genere di armi.

Se tutto ciò è vero, allora il Codice penale italiano può venirci davvero in aiuto per fondare una definizione di *cyber-arma* che abbia anche valenza giuridica. Infatti, mutuando quanto affermato dal legislatore nell'art. 615-*quinquies* in merito alla "*Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico*", nonché quanto previsto dalla Direttiva europea sulle infrastrutture critiche[30], possiamo arrivare a **definire giuridicamente una cyber-arma** 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.

Sulla base di questo assunto, allora, Stuxnet può essere certamente classificato come una *cyber-weapon*, in quanto rappresenta 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).

Stuxnet, inoltre, può essere considerato come una ***cyber*-arma "propria"**, poiché creata appositamente e in maniera premeditata con l'unico scopo di colpire e danneggiare esattamente 1. quel determinato sistema classificato come infrastruttura critica, 2. che è affetto da quegli specifici *bug* e 3. che utilizza un determinato tipo di *console* di gestione e programmazione.

Da un ulteriore punto di vista, inoltre, Stuxnet mantiene costante la sua qualità di *cyber-weapon* in considerazione della oggettiva difficoltà di riconfigurarlo ontologicamente come una "non arma", ovvero, riconvertirlo a comportamenti che contemplino esclusivamente funzioni che non arrechino danno.

Alla luce di ciò però, ai fini giuridici, persino un **generico *worm*** potrebbe assumere le caratteristiche di *cyber-arma*, nel momento in cui arrivasse a colpire – magari anche inavvertitamente – i sistemi informatici di un'infrastruttura critica. Questo finanche nel caso in cui il *worm* sia stato creato e programmato per avere una diffusione assolutamente indiscriminata.

30- La Direttiva del Consiglio 2008/114/CE dell'8 dicembre 2008, relativa all'individuazione e alla designazione delle infrastrutture critiche europee e alla valutazione della necessità di migliorarne la protezione, definisce come infrastruttura critica "un elemento, un sistema o parte di questo ubicato negli Stati membri che è essenziale per il mantenimento delle funzioni vitali della società, della salute, della sicurezza e del benessere economico e sociale dei cittadini ed il cui danneggiamento o la cui distruzione avrebbe un impatto significativo in uno Stato membro a causa dell'impossibilità di mantenere tali funzioni". Pertanto, sono certamente considerate come critiche le infrastrutture nazionali del sistema elettrico ed energetico, le varie reti di comunicazione, i circuiti economico-finanziari, le reti e le infrastrutture di trasporto persone e merci (aereo, navale, ferroviario e stradale), il sistema sanitario e quello per la gestione delle emergenze, nonché le reti a supporto del Governo, delle Regioni ed enti locali.

Pertanto, mantenendo inalterato il contesto e lo scopo, sarà fondamentale in questo caso verificare il soggetto/oggetto soccombente ed analizzare lo strato psicologico dell'intenzione, al fine di valutare a pieno il grado di colpa ascrivibile al soggetto agente e rilevare se ci si trovi dinanzi all'utilizzo di una *cyber-weapon*, ovvero semplicemente alla previsione di cui all'art. 615-*quinquies*[31] del codice penale.

Da ultimo, infine, le ***cyber-armi* "improprie"** possono essere rintracciate in tutte quelle *"apparecchiature, dispositivi ovvero qualsiasi insieme di istruzioni informatiche"* cosiddette *dual-use*, ad effetti indiretti o mediati. Numerosi, infatti, sono gli esempi di programmi creati per la gestione e l'*hardening* della sicurezza dei sistemi informatici che possono, altresì, essere utilizzati a scopi offensivi. Anche in questo caso, tuttavia, invariati il contesto e lo scopo, toccherà al soggetto/oggetto soccombente e alla valutazione dello strato psicologico inquadrare giuridicamente la corretta fattispecie.

31- Rubricato come "Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico", l'art. 615-quinquies enuncia che "chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le 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, si procura, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette a disposizione di altri apparecchiature, dispositivi o programmi informatici, è punito con la reclusione fino a due anni e con la multa sino a euro 10.329".

3. Riflessioni strategiche sulle *cyber-weapon*

Definito cosa si debba intendere per *cyber-arma*, l'analisi del *worm* Stuxnet ci permette di estrapolare alcuni rilevanti **concetti strategici** in merito alle *cyber-weapon*.

Il primo di essi è certamente quello del **danno causato** dalle *cyber-armi*. Così come affinché si possa parlare realmente di una *cyber-war*[32] occorre imprescindibilmente che gli atti posti in essere dai soggetti agenti attraverso il cyber-spazio causino dei danni reali "*off-line*"[33], sui cittadini o sulle infrastrutture (palazzi, strade, ponti, ecc.), ugualmente per parlare di *cyber-*armi occorrerà che esse creino direttamente dei danni tangibili o comunque significativamente rilevabili nei confronti del loro bersaglio. Difatti, il *software* utilizzato per un attacco che paralizza i sistemi informatici fino al riavvio delle macchine ovvero per un *Distributed Denial of Service* (DDoS), così come un programma utilizzato per effettuare il *defacement* di un sito, non potranno e non dovranno essere considerati come *cyber-weapon*, in quanto incapaci di creare in maniera diretta un livello di danno tangibile o significativamente rilevabile sul bersaglio.

Si verificheranno certamente dei danni causati dal malfunzionamento dei sistemi, dei danni alla reputazione pubblica del bersaglio, magari anche rilevanti perdite economiche a causa dell'interruzione nell'erogazione dei servizi, ma tutte queste voci di danno, così come molte altre ancora ipotizzabili, sono esclusivamente una conseguenza indiretta dell'attacco informatico e non il frutto dell'azione diretta di una *cyber-arma*.

Di contro, invece, il *worm* Stuxnet è stato programmato non solo per essere capace di penetrare i sistemi di sicurezza e di protezione di uno specifico sistema bersaglio, ma per mantenersi residente attraverso un *rootkit*[34] in questo sistema, rendendosi totalmente invisibile ai programmi di rilevamento, e per avere già in sé tutte le istruzioni informatiche utili affinché il bersaglio stesso si auto-danneggi, attraverso l'alterazione dei propri processi attivi, in maniera diretta e fisicamente rilevabile.

32- Cyber-war che, se correttamente inquadrata e definita, non risulta – almeno allo stato attuale – ancora mai avvenuta. Più correttamente, invece, si dovrebbe parlare di meri atti di cyber-warfare. Il Dipartimento della Difesa americano li definisce "the use of computers and the Internet in conducting warfare in cyberspace". Una non-definizione, pertanto. Forse più propriamente, con il termine cyber-warfare possono essere definiti quegli atti aventi come obiettivo la violazione non autorizzata da parte di, per conto di, oppure in sostegno a, un Governo nel computer di un altro Paese, nella sua rete o in qualsiasi altra attività interessata da un sistema informatico, al fine di aggiungere, modificare o falsificare i dati, ovvero causare l'interruzione o il danneggiamento, anche temporaneo, di uno o più computer, di uno o più dispositivi di rete, ovvero di qualsiasi altro oggetto controllato da un sistema informatico.
33- Stefano Mele, "Cyber-warfare e danni ai cittadini", cit..
34- Un rootkit è un tipo di software malevolo (malware), progettato per nascondere l'esistenza di alcuni processi o programmi dai normali metodi d'individuazione e rilevazione, abilitando e garantendo l'accesso continuato alla macchina bersaglio con i massimi privilegi di amministrazione possibili.

Non solo, come se ciò non bastasse, tutto questo è stato compiuto senza che gli operatori si accorgessero – neanche in tempo reale – dell'alterazione in atto dei processi di funzionamento, grazie alla ulteriore manomissione automatica dei sistemi di monitoraggio dei sensori, delle valvole e delle temperature degli impianti nucleari.

Da ciò possiamo delineare i seguenti **elementi tipici** di una *cyber-weapon*, ovvero che:

1. l'obiettivo sia mirato e che, pertanto, "*l'apparecchiatura, il dispositivo ovvero qualsiasi insieme di istruzioni informatiche*" non siano stati creati con lo scopo di avere la massima diffusione, come accade per i generici *worm* (salvo il caso della dissimulazione degli scopi reali dell'attacco);

2. l'obiettivo sia definibile come un'infrastruttura critica;

3. l'obiettivo sia di penetrare attivamente e con finalità malevoli i sistemi informatici del bersaglio (non di creare un semplice disservizio);

4. i sistemi informatici dell'obiettivo siano protetti;

5. si creino danni fisicamente tangibili o significativamente rilevabili.

Il livello di sofisticazione di Stuxnet, inoltre, pone in evidenza due ulteriori questioni. La prima, relativa alla capacità di **autonomia d'azione** del *worm*, che, avendo come obiettivo dei sistemi informatici disconnessi dalla rete Internet, è stato già a monte programmato per avere in sé tutto "l'arsenale" utile a portare a termine la sua missione. La seconda, è la quasi totale mancanza di danni **collaterali**[35].

Come si è già detto, infatti, il *worm* è stato programmato per "attivarsi" esclusivamente nel momento in cui fosse arrivato ad infettare un sistema SCADA WinCC , PCS7 o STEP7 della Siemens deputato alla gestione e al controllo di determinati processi industriali. Alcun danno è stato rilevato sui sistemi informatici che Stuxnet ha infettato prima e dopo l'attacco.

Per quanto detto finora, appare importante anche sottolineare come il rilevante tecnicismo delle *cyber*-armi, la loro estrema sofisticazione, l'elevata '*targettizzazione*' richiesta, nonché l'alto potenziale di danno che devono portare con sé, richieda per la loro realizzazione un notevole quantitativo di **risorse economiche**, di **tempo** e di **forza-lavoro** altamente specializzata. E' proprio la razionalizzazione di questi tre elementi che potrebbe indurre a pensare ad una sorta di "unione delle forze" tra uno o più Stati e gruppi di *cyber*-criminali. I primi necessari per la parte economica e di finanziamento della ricerca, l'*intelligence* sull'obiettivo e l'eventuale iniezione della *cyber*-arma in caso di sistemi non direttamente connessi alla rete Internet (com'è avvenuto per Stuxnet), mentre i secondi utili per la risorsa tempo e l'impiego di forza-lavoro specializzata. Per di più, appare sempre più plausibile che la realizzazione di Stuxnet sia stata delegata a più soggetti non-governativi, ognuno deputato a sviluppare un "pezzo" del *worm* all'oscuro dell'obiettivo finale[36], ovvero creare un worm capace di colpire e danneggiare i sistemi informatici di un'infrastruttura critica ben precisa.

35- Thomas Rid e Peter McBurney, "Cyber-weapons", in RUSI Journal, vol. 157, no. 1, 2012.
36- Alexander Klimburg, "Mobilising Cyber Power", in Survival: Global Politics and Strategy, vol. 53, no. 1, February–March 2011.

Tuttavia, a differenza delle armi convenzionali, che hanno un eccellente ritorno sia in termini di efficacia che, soprattutto, in termini di resistenza della produttività dell'investimento al trascorrere del tempo, quelli nel settore delle *cyber-weapon* funzionano, di contro, in maniera totalmente diversa e hanno un **arco temporale di utilizzazione** decisamente molto più compresso. Basandosi, infatti, su una o più vulnerabilità del sistema bersaglio, spesso tra l'altro coordinate tra loro e tutte necessarie per il raggiungimento dell'obiettivo, le *cyber*-armi possono sfruttare una linea temporale di utilizzazione ("*U*") decisamente molto breve, proporzionalmente decrescente con il trascorrere del tempo ("*T*") (i programmi vulnerabili, infatti, possono essere corretti o sostituiti con altri), moltiplicato per il numero di *bug* "V" da sfruttare contemporaneamente per portare a termine con successo l'attacco. Pertanto, il fattore di **produttività dell'investimento** per le *cyber-weapon* ("*P*") è espresso dalla seguente formula:

$$P^{(\text{produttività})} = U^{(\text{utilizzazione})} - (T^{(\text{tempo})} * V^{(\text{vulnerabilità})})$$

Infine, occorre evidenziare che la configurazione dei sistemi da violare potrà essere così specifica che una *cyber*-arma, realmente programmata per massimizzare i danni, presumibilmente riuscirà con estrema difficoltà a **colpire ulteriori bersagli** con la stessa intensità ed efficacia, risultando inadeguata per le successive operazioni. E' questo il caso, ad esempio, in cui l'operazione andata a buon fine venga resa pubblica, così come pubblici vengano resi i metodi e le vulnerabilità utilizzate per penetrare i sistemi. In questo caso, pertanto, i produttori del *software* rilasceranno a stretto giro di tempo una c.d. patch di correzione delle vulnerabilità, chiudendo definitivamente quella "strada di accesso". Di conseguenza, è verosimile che una *cyber*-arma possa essere utilizzata una volta soltanto verso un determinato bersaglio, ovvero possa tornare utile per una sola ondata di attacchi, purché realizzati in un arco temporale molto ristretto. Questo soprattutto nel caso in cui l'attacco vada a segno e produca i suoi effetti dannosi, allertando così gli addetti alla sicurezza dei sistemi colpiti, che correranno immediatamente ai ripari (ancor prima che le *patch* di correzione delle vulnerabilità siano rilasciate dai produttori).

Mettendo a sistema e schematizzando queste riflessioni, si può evincere che la realizzazione di una *cyber*-arma richieda:

- ingenti risorse economiche e d'*intelligence*, professionalità non comuni, notevoli tempi di realizzazione e di *testing*; ma che, di converso,

> questi sforzi abbiano un arco temporale di utilizzazione molto ristretto, direttamente proporzionale – con valore decrescente – al trascorrere del tempo necessario all'utilizzazione della *cyber-weapon*, alla sua complessità di assemblaggio e, ovviamente, alla sicurezza dei sistemi da penetrare;

> la *cyber*-arma, una volta colpito il suo bersaglio, difficilmente potrà essere riutilizzata per successive operazioni, anche verso sistemi differenti, a causa della alta visibilità sui mass media che allo stato attuale questo genere di attacchi hanno;

- le *cyber*-armi (o presunte tali) finora analizzate hanno la capacità di **sabotare temporaneamente** il sistema informatico dell'infrastruttura critica della nazione bersaglio e non di distruggerlo completamente, come potrebbe avvenire, ad esempio, in conseguenza di un attacco missilistico.

Gli alti costi, le alte variabili di rischio sulla loro realizzazione ed efficacia, nonché i risultati "limitati" e comunque temporanei, portano a far ritenere attualmente le attività di ricerca e sviluppo nel settore delle *cyber*-armi come **strategicamente non convenienti**, a meno che non sia possibile un'*escalation* (comunque prevedibile e, anzi, già da alcuni preannunciata[37]) nelle capacità di questi *software* di innalzare il livello di danno e/o di estenderne quanto più possibile l'arco di durata degli effetti. Pertanto, siamo di fronte certamente ad una minaccia, ma essa deve essere urgentemente inquadrata in maniera corretta e ponderata, lontano dai titoli "ad effetto" dei principali organi di comunicazione.

Resta ferma già oggi, comunque, la possibilità e l'impareggiabile efficacia di sfruttare gli attacchi elettronici come mezzi utili ad **agevolare gli attacchi fisici**[38].

Discorso diametralmente opposto deve essere effettuato per i **crimini informatici**, anche nel caso in cui vengano eseguiti, come sempre più spesso accade[39], verso quegli obiettivi elettronici di uno Stato, anche sensibili, ma che non abbiano, però, le caratteristiche d'infrastruttura critica.

In questo caso, infatti, le risorse economiche, le informazioni d'*intelligence*, la forza-lavoro e la fase di *testing* degli *exploit* da impiegare sono spesso ampiamente ridotte e alla portata sia della quasi totalità dei maggiori gruppi di criminali informatici che degli Stati. Molto spesso, anzi, le informazioni necessarie e gli opportuni *exploit*[40] sono agevolmente rintracciabili direttamente in Rete o acquistabili sul mercato nero, ovvero, a strettissimo giro di tempo, disponibili liberamente e gratuitamente come "moduli" di noti programmi per la scansione delle vulnerabilità (i *software Metasploit*[41] e *Nessus*, per tutti). Tuttavia, anche per gli *exploit* il trascorrere del tempo gioca a sfavore del loro utilizzo verso il sistema bersaglio, ma con un coefficiente di riduzione decisamene minore rispetto a quello di una *cyber*-arma. Occorre rilevare, infine, come un *exploit*, a differenza di una *cyber*-arma, spesso possa essere agevolmente riutilizzato per successive operazioni, soprattutto verso sistemi bersaglio differenziati.

Per quanto detto finora, i crimini informatici, soprattutto quelli orientati allo **spionaggio elettronico e al furto d'informazioni riservate**[42], restano e resteranno – almeno nel breve periodo – la principale minaccia[43], sia per le società private che gravitano nell'orbita governativa che direttamente per i sistemi informatici degli Stati.

37- Stefano Mele, "Cyber-warfare e danni ai cittadini", cit..
38- Come potrebbe essere avvenuto nel 2007 per il bombardamento di Damasco da parte di aerei israeliani, effettuato dopo aver disattivato i sistemi di controllo aereo siriani. Per approfondire, Richard Clarke and Robert Knake, "Cyber War. The next threat to national security and what to do about it", Harper Collins, 2010.
39- Andrea Zapparoli Manzoni, "Panoramica degli eventi di cyber-crime e incidenti informatici più significativi del 2011 e tendenze per il 2012", in Rapporto CLUSIT 2012, 2012; Paolo Passeri, "2012 Cyber Attacks Timeline Master Index", 2012, in http://hackmageddon.com/2012-cyber-attacks-timeline-master-index/
40- Un exploit è un termine usato per identificare un insieme di informazioni elettroniche che, sfruttando un bug o una vulnerabilità, porta all'acquisizione di privilegi o al denial of service di un computer.
41- Tra tutti, si prenda come esempio il 'Project Basecamp', che mira a fornire pubblicamente e in maniera totalmente gratuita dei moduli preconfezionati utili a colpire i sistemi PLC delle infrastrutture critiche. Maggiori dettagli su http://www.digitalbond.com/tools/basecamp/metasploit-modules/.

Non è un caso, infatti, che anche il cosiddetto potenziale "successore" di Stuxnet, denominato Duqu[44], in realtà, allo stato attuale del suo sviluppo, si limiti esclusivamente a propagarsi e ad infettare i suoi bersagli con l'unico scopo di raccogliere informazioni sui sistemi di controllo industriali, forse per un (probabile) successivo attacco mirato. Siamo di fronte, pertanto, ad attività di spionaggio elettronico orientate a raccogliere informazioni d'*intelligence* sui potenziali bersagli.

Si può prevedere, allora, che quelli che attualmente risultano essere gli attori principali nel settore dello spionaggio elettronico e del furto d'informazioni, **Russia** e **Cina**, continueranno ad essere i protagonisti indiscussi del settore dei crimini informatici, continuando così ad influenzare il quadro geopolitico internazionale. La prima, grazie alla collusione tra personaggi politici di spicco[45], servizi segreti[46] e gruppi di *cyber*-criminali[47] / *hacker patriots*[48].

La seconda, grazie alle capacità di controllo del Governo sul pensiero e sulle azioni della popolazione, sia in maniera diretta, attraverso propaganda, censura e collusione, che indiretta, attraverso il reclutamento di cittadini e *patriot hackers*.

Questo stato di cose, peraltro, può far presumere con discreta certezza che sia il Governo russo che quello cinese, proprio per le ragioni appena analizzate, siano[49] e probabilmente sempre più saranno i due Stati maggiormente attivi in ambito *cyber-warfare*[50], svolgendo un ruolo primario anche nell'ideazione, sviluppo, realizzazione ed uso delle prossime generazioni di *cyber*-armi.

42- L'ultima operazione balza agli onori della cronaca è stata quella denominata "Luckycat". Resa pubblica dalla società di sicurezza Trend Micro, questa operazione ha avuto come obiettivo 233 computer nel corso di 90 attacchi portati nei confronti di enti e società "sensibili" in Giappone, India e Tibet. L'intero report, dal titolo "Luckycat Redux. Inside an APT Campaign with Multiple Targets in India and Japan", è reperibile su http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_luckycat_redux.pdf. Indicativa può essere anche l'info-grafica relativa alle principali operazioni di esfiltrazione di dati sensibili e riservati attualmente conosciute, reperibile qui http://blog.trendmicro.com/global-targets-infographic/

43- Richard Clarke, "China has hacked every major US company", 2012, in http://www.zdnet.com/blog/security/richard-clarke-china-has-hacked-every-major-us-company/11125

44- Symantec, "W32.Duqu", 2011, in http://www.symantec.com/security_response/writeup.jsp?docid=2011-101814-1119-99; Symantec, "W32.Duqu: The Precursor to the Next Stuxnet", 2011, in http://www.symantec.com/connect/w32_duqu_precursor_next_stuxnet; Laboratory of Cryptography of Systems Security (CrySyS), "Duqu: A Stuxnet-like malware found in the wild, technical report", 2011, in http://www.crysys.hu/publications/files/bencsathPBF11duqu.pdf

45- Alexander Klimburg, "Mobilising Cyber Power", cit..

46- Basti pensare che nel 2006 più del 78% dei 1.016 leader politici russi era stato in precedenza al servizio in organizzazioni affiliate al KGB e all'FSB. Per approfondire, Evgenia Albats, "Siloviks in power: fears or reality?", interview with Olga Kryshtanovskaya, in Echo of Moscow, 2006.

47- Uno tra tutti, il Russian Business Network (RBN). Per approfondire, David Bizeul, "Russian Business Network study", 2007, in http://www.bizeul.org/files/RBN_study.pdf; The Economists, "A walk on the dark side", 2007, in http://www.economist.com/node/9723768?story_id=9723768

48- Soggetti con elevate capacità tecniche motivati politicamente ad agire al fianco e nell'interesse del proprio Stato.

49- Northrop Grumman Corp, "Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage", cit.; US–China Economic and Security Review Commission, "2009 Report to Congress", cit..

50- In mancanza di una definizione giuridica universalmente accettata, con il termine cyber-warfare possono essere definiti quegli "atti aventi come obiettivo la violazione non autorizzata da parte di, per conto di, oppure in sostegno a, un Governo nel computer di un altro Paese, nella sua rete o in qualsiasi altra attività interessata da un sistema informatico, al fine di aggiungere, modificare o falsificare i dati, ovvero causare l'interruzione o il danneggiamento, anche temporaneo, di uno o più computer, di uno o più dispositivi di rete, ovvero di qualsiasi altro oggetto controllato da un sistema informatico", in Stefano Mele, "Cyber-warfare e danni ai cittadini", cit..

Da ultimo, volgendo lo sguardo al medio periodo, un ruolo molto simile a quello attualmente svolto da Russia e Cina sarà interpretato anche dalla **Corea del Nord** e dall'**Iran**, che guardano a questi settori con sempre maggiore interesse, destinando sempre più risorse economiche, sforzi organizzativi[51] e capitale umano[52].

51- Tra i numerosi articoli e le più recenti news, Trend, "Iran establishes supreme cyberspace council", 2012, in http://en.trend.az/regions/iran/2001057.html; Fars News Agency, "Iran Warns: West Using Internet for Spying", 2012, in http://english.farsnews.com/newstext.php?nn=9012151817; Press TV, "Iran cyber defense headquarters makes local mail servers", 2012, in http://www.presstv.ir/detail/232105.html; Fox News, "Iran is Recruiting Hacker Warriors for its Cyber Army to Fight 'Enemies' ", 2011, in http://www.foxnews.com/world/2011/03/14/iran-recruiting-hacker-warriors-cyber-army/; The Green Voice of Freedom, "Who are the 'Iranian Cyber Army'?", 2010, in http://en.irangreenvoice.com/article/2010/feb/19/1236

52- Infosec Island, "North Korea's Cyber War Forces", 2012, in http://infosecisland.com/blogview/20532-North-Koreas-Cyber-War-Forces.html; The Korea Herald, "North Korea has 30,000 electronic warfare agents", 2011, in http://www.koreaherald.com/national/Detail.jsp?newsMLId=20110518000723; Al-Jazeera, "North Korea recruits hackers at school", 2011, in http://www.aljazeera.com/indepth/features/2011/06/201162081543573839.html; Fox News, "North Korea's Cyber Army Gets Increasingly Sophisticated", 2011, in http://www.foxnews.com/world/2011/05/17/north-koreas-cyber-army-gets-increasingly-sophisticated/

4. Riflessioni conclusive

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 di informazioni sensibili e/o classificate dei Governi, 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.

Inquadrare correttamente il concetto di *cyber*-arma, quindi, dandone una definizione anche a livello giuridico, risulta un passaggio urgente e imprescindibile – uno dei tanti, in realtà, che mancano in questo settore – per avere la possibilità sia di valutare il livello di minaccia proveniente da un attacco informatico, che le conseguenti responsabilità politiche e giuridiche ascrivibili a chi ha agito. Questo, ovviamente, sempre ammesso che si riesca a rintracciare l'autore dell'attacco e ad attribuirgli giuridicamente la responsabilità delle azioni. Cosa allo stato attuale tra le più complesse nel *cyber*-spazio.

Tuttavia, soltanto consolidando questo genere di definizioni e creando un substrato d'informazioni comunemente accettato si potrà cominciare a rispondere a quelle domande che, in maniera sempre più pressante, richiedono concretezza. Soprattutto ora che, mancando risposte tecniche (tracciabilità degli attacchi) e giuridiche (responsabilità degli attacchi), alcuni Governi cercano di accelerare al massimo il processo innovativo proprio nel settore delle *cyber-weapon*, al fine di colpire e distruggere le reti militari nemiche anche nel caso in cui non siano connesse alla rete Internet[53].
Le sfide che la Difesa, le Forze Armate e, più in generale, le Istituzioni della sicurezza nazionale sono e saranno sempre più chiamate ad affrontare nel settore della *cyber-security* e della *cyber-intelligence* sono certamente tanto complesse quanto affascinanti. Le *cyber-weapon*, come si è visto, impongono comportamenti adattivi e di reazione che tagliano trasversalmente sia il settore della ricerca tecnica e tecnologica, che quello strategico, tattico ed operativo, i quali per la prima volta, proprio attraverso Internet e la tecnologia, stanno vedendo svanire la loro tipica compartimentazione settoriale.

53- E. Nakashima, "U.S. accelerating cyberweapon research", in Washington Post, 2012, http://www.washingtonpost.com/world/national-security/us-accelerating-cyberweapon-research/2012/03/13/gIQAMRGVLS_story.html

Definire con certezza quando un attacco informatico alle infrastrutture critiche possa essere qualificato come uso della forza, ovvero assuma il carattere di un vero e proprio attacco armato, rappresenta ormai – in un mondo occidentale totalmente interconnesso e che basa il suo intero substrato sociale sulle tecnologie informatiche – anche una nostra priorità.

A maggior ragione ora che il Congresso americano si è visto costretto ad autorizzare il proprio Dipartimento della Difesa[54] a condurre operazioni militari di offesa nel cyber-spazio[55], lasciando intravedere un futuro tutt'altro che roseo in tema di attacchi informatici[56].

54- Department Of Defense, "Strategy for Operating in Cyberspace", 2011, in http://www.defense.gov/news/d20110714cyber.pdf
55- United States Congress, National Defense Authorization Act For Fiscal Year 2012, "Military Activities in Cyberspace", Sec. 954, in http://www.fas.org/irp/congress/2011_cr/cyberwar.html
56- SC Magazine, "Duqu variant uncovered", 2012, in http://www.scmagazine.com/duqu-variant-uncovered/article/233385/

Editing e realizzazione grafica a cura di:

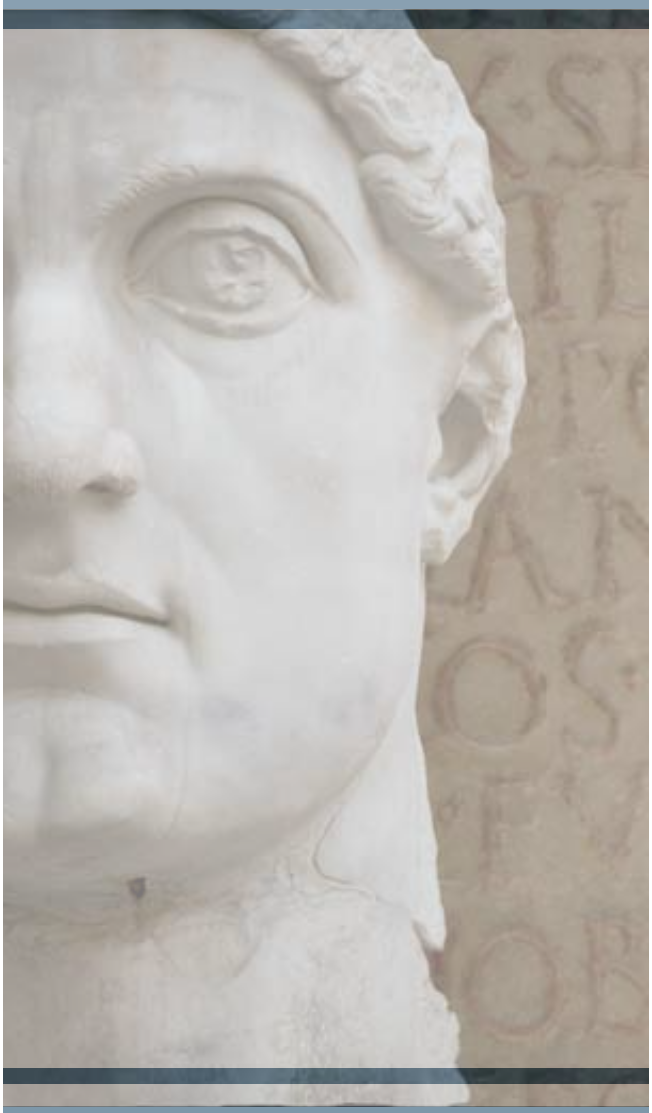
Leader in Digital Brand Management

Famebridge è partner del Think Tank
“Niccolò Machiavelli”.

Fondata e guidata da un executive manager che proviene da aziende quali Procter & Gamble, Johnson & Johnson e Adidas, FameBridge è una realtà Leader nel Digital Brand Management.

FameBridge ha di fatto una expertise unica nella realizzazione delle strategie digitali di Celebrities nazionali e internazionali di tutti i settori (Sport, Cinema, Giornalismo, Moda, Tv, Politica ecc). Questa expertise, unita alle solide competenze nei Social Media, parte integrante della strategia di business, rende FameBridge una società particolarmente efficace nel monitorare e influenzare i Consumatori, gli Utenti e la Pubblica Opinione per scopi di marketing.

www.famebridge.com



ISTITUTO ITALIANO
DI STUDI STRATEGICI

ITALIAN INSTITUTE
OF STRATEGIC STUDIES

Niccolò Machiavelli

L'Istituto Italiano di Studi Strategici "*Niccolò Machiavelli*" è un'associazione culturale senza scopo di lucro costituita a Roma nel 2010.

L'Istituto, think tank indipendente, nasce dall'iniziativa di un gruppo internazionale di personalità del mondo economico, accademico ed istituzionale civile e militare, con l'obiettivo di contribuire alla rinascita del pensiero strategico italiano.

La complessità e l'ampiezza delle sfide che attendono il Paese nel XXI secolo richiede conoscenza, consapevolezza e capacità prospettiche. L'Istituto Machiavelli, anche grazie al proprio network globale, promuove l'interscambio culturale tra il decisore italiano ed internazionale, pubblico e privato, e svolge attività di ricerca finalizzate ad elevare il livello di competitività globale del "Sistema Paese".

L'Istituto Machiavelli, autonomamente o in collaborazione con istituzioni, organizzazioni ed aziende nazionali ed estere, realizza studi ed analisi strategiche *policy-oriented*, organizza briefing, seminari e workshop, cura corsi di alta formazione per i *leader*.

Per ulteriori informazioni:

Istituto Italiano di Studi Strategici "Niccolò Machiavelli"
Via di San Basilio, 64
00187 – Roma
Tel.: (+39) 06 45422952
Fax.: (+39) 06 97259168
email: info@strategicstudies.it
http://www.strategicstudies.it