Sicurezza informatica

'Fusion Cell' una struttura per la Cyber Defence

ANTONIO TETI

A fine marzo scorso, il ministro del Cabinet Office britannico, Francis Maude, ha annunciato l'attivazione del 'Fusion Cell', una struttura ubicata in una località segreta in cui convoglieranno i maggiori esperti di sicurezza informatica del Paese. Il costo del cyber crime nel Paese di Sua Maestà, ha raggiunto la ragguardevole vetta di 27 miliardi di sterline annue. Solo la collaborazione tra istituzioni governative, aziende private e strutture accademiche, può consentire di produrre una risposta efficace ad una criminalità informativa, in continua evoluzione, che agisce su scala planetaria. Tuttavia c'è chi pensa ad una maggiore integrazione, anche psicofisica, con le tecnologie digitali…

Un nuovo modello di sicurezza

La notizia risale a fine marzo scorso ed è il ministro del Cabinet Office britannico, Francis Maude, a comunicarla ai media: sarà attivato un nuovo centro di sicurezza informatica per contrastare, a vantaggio di imprese pubbliche e private e del governo, le future minacce informatiche. Fortemente voluta dal GCHQ[1] e dall'MI5[2], la struttura sarà realizzata nell'ambito del programma Cyber Security Information Sharing Partnership (CISP) e raccoglierà le migliori menti informatiche di aziende pubbliche, private e di strutture governative, particolarmente formate nel settore della sicurezza informatica.

Sono circa 160, finora, le aziende coinvolte nel progetto. Il nome della struttura sarà *Fusion Cell* (cella di fusione), nome non poco evocativo di un

[1] GCHQ. Acronimo di 'Government Communications Head Quarter', è l'Agenzia governativa che si occupa della sicurezza, nonché dello spionaggio e controspionaggio, nell'ambito delle comunicazioni; attività tecnicamente nota come SIGINT (SIGnal INTelligence). La sede principale è ubicata a Cheltenham, in Gran Bretagna.

[2] MI5 (Military Intelligence, Sezione 5). Corrisponde al Security Service, l'Agenzia per la sicurezza e il controspionaggio interno del Paese. Le attività sono indirizzate alla protezione dalle minacce che possano mettere a rischio la sicurezza nazionale, la democrazia parlamentare, gli interessi economici britannici, oltre alla lotta a forme di grave criminalità, al separatismo, al terrorismo e allo spionaggio nel Regno Unito. L'MI6 (Military Intelligence, Sezione 6) si occupa invece della sicurezza esterna.

programma che vuole tendere alla raccolta e alla 'fusione' dei migliori cervelli informatici del Regno Unito. In una recente intervista, Maude ha dichiarato '*Sappiamo che i cyber attacchi si stanno diffondendo nel settore industriale, e le imprese sono di gran lunga le più grandi vittime in termini di spionaggio industriale, oltre al furto di proprietà intellettuale. Il tutto genera perdite per l'economia del Regno Unito equivalenti a miliardi di sterline all'anno*'. Il CISP si doterà anche di un portale web, che sarà munito di complessi sistemi di sicurezza per consentire a qualsiasi cittadino del Paese di condividere informazioni, in tempo reale, sulle minacce rilevate durante la navigazione nel Cyberspazio. Di particolare interesse, nel sito web, sarà la presenza di applicazioni (programmi software) che mirano alla costruzione di un rapporto di fiducia intersettoriale (soprattutto per le aziende private) per sostenere la condivisione delle informazioni.

Secondo un recentissimo rapporto del National Audit Office, il costo del Cybercrime, nel Regno Unito, ha raggiunto la ragguardevole somma di 27 miliardi di sterline annue, e le azioni criminose sono soprattutto riconducibili allo spionaggio industriale e al furto di proprietà intellettuale.

Anche da questi elementi sorge la convinzione, da parte dei vertici istituzionali britannici, che solo attraverso la collaborazione tra strutture governative e private, si potrà fornire un contrasto efficace alle azioni criminose che si consumano nel Cyberspazio. Dall'altro capo dell'oceano, se ne è convinto anche Michael Welch, della Divisione Cyber dell'FBI, che asserisce '*La strategia di difesa richiede una maggiore collaborazione tra settore pubblico e privato nel garantire gli interessi di un Paese on line*'. Tuttavia, sulla questione della collaborazione tra pubblico e privato, un problema lo pone Troels Oerting, vicedirettore della divisione Cyber Crime di Europol: quanto sono disposte le aziende che operano nell'IT Security a condividere il proprio *Know-how* con aziende governative e istituzionali? Sembra rispondergli a distanza un portavoce del GCHQ, che in un'intervista sul quotidiano 'The Guardian' asserisce '*Ci possono essere cose sviluppate dal GCHQ che potrebbero essere utilizzate per scopi commerciali*'. Potremmo essere giunti a una svolta epocale: un sistema di difesa nazionale basato sul rapporto sinergico pubblico-privato?

Origini del progetto: condivisione di esperienze per rafforzare la difesa

L'idea di realizzare questo progetto nasce in verità da un'iniziativa del 2011, rappresentata dallo studio realizzato dal National Cyber Security Strategy, pubblicato nello stesso anno, a cui collaborarono il Cyber Security e Information Assurance (OCSIA) e il Cyber Security Operation Centre (CSOC) di Cheltenham. Secondo alcune notizie diffuse dai media, fu Owen Pengelly, vice direttore di Ocsia, a porre la questione, in una conferenza sul Cyberspazio tenutasi il 2 novembre scorso a Londra (a cui fu rigorosamen-

te vietato l'ingresso a giornalisti e ai non invitati), sulla scelta delle possibili strategie da adottare per combattere l'inarrestabile crescita della Cybercrime. Anche se ben poco è trapelato sui temi trattati durante la conferenza, un partecipante ha sintetizzato così le conclusioni a cui sono giunti: '*Durante tale riunione è emerso che nessuna singola entità o organizzazione ha piena visibilità di ciò che sta accadendo nel Cyberspazio a livello di minacce*'. Alle aziende che parteciparono all'evento, tuttavia fu chiesto di aderire a quella che fu definita come 'uncomfortable partnership', per condividere le conoscenze sulle cyber-minacce circolanti in Rete. Non furono certamente pochi gli scetticismi derivanti dalla richiesta di condivisione delle informazioni possedute dalle singole aziende sulle problematiche esposte, soprattutto per le preoccupazioni delle stesse a rivelare ad altri dati e notizie accumulate dalle esperienze conseguite nel corso degli anni, la cui diffusione ad altri *competitor* avrebbe potuto produrre una perdita di competitività o addirittura il danneggiamento dell'immagine dell'azienda. Il progetto di 'collaborazione scomoda', prevedeva anche il coinvolgimento di altre strutture del Paese, come le banche e la Polizia. In sostanza, l'architettura di questa Task Force si sarebbe dovuta basare sulla predisposizione di 'cyber hub and nodes' in grado di raccogliere, analizzare e classificare tutti gli eventi riconducibili agli attacchi informatici. In tal senso, la Metropolitan Police e Crime Unit, unità delle Forze di polizia specializzata in crimini informatici, ha aderito al progetto mettendo a disposizione le informazioni in proprio possesso, su alcuni particolari crimini come il furto on line delle credenziali finanziarie condotte verso banche nazionali che hanno filiali all'estero. Sembra che questa attività di condivisione dati sia stata attivata anche con strutture di paesi amici, come il Federal Bureau of Investigation (FBI).

L'attenzione dei britannici sulla questione della lotta al cyber crime era già ai massimi livelli, come dimostrato dall'attivazione, nel 2010, del CSOC che ha permesso di coordinare le attività di contrasto al cyber crime per quanto concerne i sistemi informativi del governo, e del Centre for the Protection of National Infrastructure (CPNI) che si occupa del controllo e monitoraggio dei rischi informatici, oltre che della tutela della sicurezza fisica dei sistemi informativi nel settore privato.

Risulta evidente che il governo di Sua Maestà, attraverso la guerra alla criminalità informatica mira, soprattutto, a tutelare interessi economici del Paese, grazie anche all'implementazione di una strategia di sicurezza in Rete che dia l'immagine del Regno Unito come un luogo sicuro dove fare commercio on line. Le crescenti preoccupazioni circa il possibile impatto economico derivante dal cyber crime, sono state motivate anche dai recenti attacchi subiti dai sistemi britannici, che a ottobre del 2010 avevano raggiunto soglie di pericolosità così consistenti da portate a 'livello 1' la soglia di allarme nelle agenzie governative.

Ciò nondimeno, l'idea sposata dagli inglesi per contrastare il fenomeno della criminalità in Rete, non è quella di censurare, limitare o restringere il

numero o le tipologie di attività gestibili nel Cyberspazio, ma di creare una sorta di circuito collaborativo, ad ampio spettro, nel paese, per trasformare la lotta al Cybercrime come un'azione della collettività a difesa della nazione. In questo senso va la decisione di migliorare anche le competenze sull'IT Security, in particolare nel settore pubblico, con delle azioni specifiche come ad esempio quella di chiedere al CESG[3], il braccio operativo di reperimento delle informazioni del GCHQ, di verificare che i *professional skill* del personale operante in queste strutture, siano allineati e aggiornati in funzione delle continue evoluzioni delle tecnologie digitali. Per ottenere ciò è stata attivata una collaborazione diretta con organizzazioni che operano nel settore delle certificazioni informatiche, come BCS[4], IISP[5] e CREST[6], per attuare un piano di formazione continua al fine di migliorare le competenze degli specialisti chiamati a fronteggiare i continui attacchi che provengono dalla Rete.

Per la verità, *Fusion Cell* non è la diretta conseguenza dell'innalzamento del numero degli attacchi informatici a livello mondiale. Esso ha origini più antiche. Ed è lo stesso Maude ad ammetterlo. È una copia del modello di collaborazione tra governo e aziende, sviluppato e adottato dall'Estonia, in funzione degli attacchi informatici subiti nella prima metà del 2007[7], che vide il piccolo paese baltico oggetto di un'ondata di attacchi informatici condotti nel giro di sole tre settimane. Essendo dal 2004 integrato nel sistema di difesa NATO, il problema fu esaminato con la massima urgenza da buona parte delle strutture di cyber defence dei paesi aderenti al Patto Atlantico. Inizialmente si pensò ad una ritorsione russa riconducibile alla decisione del governo di Tallin di rimuovere alcune statue di bronzo del periodo Sovietico in un cimitero di guerra. Ma l'ampiezza dell'attacco, condotto contro i siti web di ministeri, partiti politici, quotidiani, banche e imprese operanti nel settore della comunicazione, lasciavamo presagire che il *cyber-attack* fosse stato condotto per ben altre finalità: la sperimentazione di un modello di attacco cibernetico ad ampio spettro. E forse fu per questo che la NATO inviò sul posto i migliori esperti di cyber-terrorismo per indagare sull'accaduto e aiutare gli estoni a fortificare il proprio sistema di difesa cibernetico. L'Estonia è un paese di circa 1,4 milioni di persone, tra cui una grande minoranza russa, ed è uno dei paesi più cablati d'Europa, oltre ad essere 'pioniere' nello sviluppo dell'e-Government. Pertanto, essendo uno dei paesi al mondo più dipendente dalle moderne tecnologie di comunicazione e trasmissione dati, risulta il bersaglio perfetto per sperimentare le

[3] *http://www.gchq.gov.uk/AboutUs/Pages/CESG.aspx* .

[4] BCS - British Computer Society (www.bcs.org).

[5] IISP - The Institute of Information Security Professional *(https://www.iisp.org/imis15).*

[6] CREST - Council for Registered Ethical Security Testers *(http://www.crest-approved.org/).*

[7] *http://www.guardian.co.uk/world/2007/may/17/topstories3.russia* .

conseguenze di un attacco informatico finalizzato alla paralisi dei sistemi delle infrastrutture critiche della nazione. Per l'esattezza, sono stati attaccati i sistemi:

- della Presidenza Estone e il Parlamento;
- di quasi tutti i ministeri;
- dei partiti politici;
- dei tre più importanti media-network del paese;
- delle due più grandi banche del paese;
- di buona parte delle aziende specializzate nel settore delle comunicazioni.

Non è stato possibile stabilire l'entità dei danni prodotti dai cyberattacchi, anche in funzione della rapida reazione dei sistemi di difesa estoni che hanno immediatamente disattivato tutti gli accessi, provenienti da Internet, ai propri sistemi. Anche in funzione di questi eventi, nel 2008 viene attivato il CCDCOE[8] (NATO Cooperative Cyber Defence Centre of Excellence), la cui mission è quella di adoperarsi in ogni modo possibile per contrastare gli attacchi provenienti da Internet. All'accordo iniziale hanno aderito Estonia, Germania, Italia, Lettonia, Lituania, Slovacchia, Spagna a cui si sono aggiunti successivamente Polonia, Turchia e Regno Unito. La sede generale è ubicata a Tallin.

La sperimentazione: il progetto 'Auburn'

Nel 2011, su pressione del CISP, David Cameron sigla un accordo con un gruppo di aziende che darà vita ad un piano di sperimentazione meglio conosciuto come programma 'Auburn'. Vengono coinvolte circa 80 aziende, operanti nel settore della difesa, farmaceutico, telecomunicazioni, finanza ed energia, ivi compresi i fornitori di tecnologie e servizi per le infrastrutture critiche nazionali. La vera sperimentazione consiste nella verifica della possibilità di mettere insieme, concretamente, le esperienze, le metodologie, le strategie e le tecnologie di rafforzamento della sicurezza informatica. I risultati del programma si rivelano molto soddisfacenti, al punto tale che un responsabile del progetto asserisce '*Quello che stiamo cercando di fare è di ottenere la migliore rappresentazione dell'intelligenza presente nell'industria, in modo da consentire ad essa di muoversi in un contesto di azione*'[9]. Tuttavia durante lo sviluppo del programma Auburn, si manifesta, soprattutto da parte di aziende private operanti nel settore dell'Infor-

[8] *https://www.ccdcoe.org/* .

[9] *http://www.guardian.co.uk/technology/2013/mar/27/mi5-industry-join-forces-cyber-crime* .

mation Technology, un atteggiamento rivolto al protezionismo e alla tutela delle proprie competenze e tecnologie. Ma Wieland Adge, General Manager del settore Europe, Middle East & Africa di Barracuda Networks, cerca di smorzare le tensioni, asserendo che '*Le proteste delle imprese, innescate dal nervosismo sulla possibilità di rivelare pubblicamente informazioni riservate sugli attacchi subiti e sui segreti riconducibili ai rispettivi sistemi di sicurezza implementati, sono sostanzialmente infondate*', e poi aggiunge che '*Concentrandosi sulla loro reputazione, che è solo un elemento di valore sul mercato, dimenticano ciò che è maggiormente in gioco, la perdita dei dati dei loro clienti*'. Il CISP, nel tentativo di rassicurare gli animi e raffreddare i bollori, si affretta a garantire che i nomi delle organizzazioni coinvolte, così come le informazioni che saranno condivise, saranno classificate tutte come 'confidenziali'. Saranno accessibili solo da pochi e con le dovute autorizzazioni condivise. Il modello si rivela vincente e l'idea di unire le competenze e le conoscenze di strutture governative con quelle private, raccoglie consensi anche in altre nazioni, ma una in particolare, accoglie il suggerimento con grande convinzione: gli Stati Uniti.

Ed è lo stesso Barack Obama a decidere di sposare l'idea, al punto tale che a febbraio scorso sigla addirittura un ordine esecutivo in cui si richiede alle agenzie federali di attivare delle forme di condivisione delle informazioni con le aziende private operanti nel settore. Un'unica mission: combattere le crescenti minacce provenienti dal Cyberspazio. L'executive order, fortemente sostenuto da Janet Napolitano, segretario della Homeland Security e da Howard Schmidt, Cyber Security Chief della Casa Bianca, giunge in risposta al blocco del disegno di legge sulla Cyber Security, che era rimasto impantanato da tempo al Congresso, dove i repubblicani sostenevano che la legge poteva rivelarsi particolarmente gravosa, in termini di privacy, per le reti aziendali del Paese. Schmidt, asserendo che un ordine esecutivo poteva fungere da elemento di stimolo per le aziende ad aggiornare la sicurezza dei propri sistemi informativi, ha affermato '*Se ci sono cose che questo Congresso non è disposto a fare, il Presidente ha alcune opzioni che gli possono consentire di farle da solo*'. Anche se l'adesione delle aziende private è su base volontaria, per alcune di esse, e per l'esattezza per tutte quelle che gestiscono infrastrutture critiche, la partecipazione al processo di condivisione delle informazioni, dovrà essere effettuato obbligatoriamente. Obama ha anche sostenuto che i nemici degli Stati Uniti sono sempre più orientati alla conduzione di azioni di sabotaggio della rete elettrica, delle reti finanziarie e dei sistemi di controllo del traffico aereo del paese, insomma di quelle che vengono identificate con il termine di infrastrutture critiche. Stranamente, anche l'American Civil Liberties Union, sempre pronta a scendere in campo a difesa delle libertà dei cittadini e della loro privacy, è d'accordo con l'approccio di Obama all'adozione di questi sistemi di accrescimento della sicurezza del paese.

Saltando nuovamente dall'altra parte dell'oceano, in Europa, a febbraio 2013 è stato pubblicato l'EU Cyber security Plan[10], nella cui sezione 30 '*Establish a European cybercrime platform*' si legge testualmente '*Europol, in collaborazione con la Commissione Europea, è stato invitato a integrare tutte le piattaforme nazionali pertinenti in un'unica piattaforma allarme criminalità informatica (European Cybercrime Platform). La piattaforma europea di allerta funzionerebbe come un centro per la raccolta e la conservazione di informazioni sui reati connessi a Internet e per la compilazione di relazioni periodiche statistiche sulla criminalità informatica. La piattaforma di criminalità informatica europea dovrebbe essere un elemento importante dell'European Cyber Crime Centre (EC3)'*. Per il 2013 la Commissione prevede di '*avviare l'European Cybercrime Centre per fornire canali più efficienti per gli Stati membri per la condivisione delle informazioni relative al cyber crime*'. È il primo passo verso l'unificazione delle forze nazionali per il contrasto alla criminalità informatica verso un'unica struttura di difesa transnazionale? Vedremo…

'Fusion Cell': organizzazione e funzioni gestite dalle agenzie di intelligence

Secondo il Cabinet Office, *Fusion Cell* rappresenterà l'elemento 'chiave' per l'intera strategia di difesa della nazione dagli attacchi provenienti dal Cyberspazio, ampliando il progetto iniziale del CISP. Il finanziamento stanziato dal Governo per il progetto è di 650 milioni di sterline, per una durata di cinque anni. Per quanto concerne l'organico, esso si baserà sulla 'fusione' di un gruppo di specialisti che andranno a formare una 'cella di menti' specializzate in Cyberwar. Inizialmente il gruppo sarà basato su di una cellula di circa 15-16 persone. Una decina di 'menti' dovranno provenire dai ranghi degli ufficiali dell'MI5, GCHA e MI6, gli altri saranno indicati dalle più grandi aziende del Regno Unito e dovranno rappresentare il meglio che il paese può esprimere in termini di professionalità, esperienze e competenze acquisite nella lotta alla criminalità informatica.

Una fonte governativa inglese, ha asserito che l'idea di miscelare le diverse professionalità, era generata dalla '*… consapevolezza che nessuna singola organizzazione era abbastanza grande da sorvegliare il cyberspazio. Per questo motivo è stata presa la decisione di riunire i settori commerciali e le Agenzie di Intelligence*'[11]. La stessa fonte dichiara che '*Fusion Cell ci permetterà di tracciare geograficamente dove sono diretti gli attacchi e quali sono i settori di interesse*'.

Ma ciò che risalta rapidamente agli occhi, anche del lettore meno attento, risiede nella composizione del gruppo di menti, più esattamente nella

[10] *http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security* .

[11] *http://news.sky.com/story/1070111/cyber-threat-spies-and-big-firms-join-forces* .

massiccia presenza di personale proveniente dagli ambienti di Intelligence. E non è certamente un caso. Lo scopo che presumibilmente il Governo inglese intende perseguire, è quello di creare una struttura dedicata al contrasto degli attacchi informatici, quindi particolarmente ricca di quelle competenze, capacità, esperienze e tecnologie che solo le aziende private operanti nel settore possono offrire, ma al tempo stesso coordinata da professionisti dell'intelligence, che avranno il compito di fornire precise indicazioni su '*cosa*' e '*chi*' combattere. Un altro obiettivo che la struttura dovrà perseguire, sarà quello di garantire la funzione di collettore tra diverse aziende che operano nel settore dell'ICT[12], per garantire e uniformare le tecniche di Cyber security.

Risulta, quindi, evidente la connotazione di un nuovo concetto di difesa delle aziende e dell'intera nazione, basato sul modello 'struttura-paese'. Ad esempio, se consideriamo che un attacco informatico ad una società commerciale o industriale può esercitare un forte condizionamento sul prezzo delle sue azioni, il danno che ne deriverebbe non sarebbe solo riconducibile alla sola azienda, ma si estenderebbe anche all'immagine del paese in cui l'azienda risiede, e di conseguenza sul livello del Prodotto Interno Lordo (PIL). In uno scenario come quello descritto, la tutela dei sistemi informativi delle aziende assume la connotazione di un'azione esercitata per la salvaguardia dell'economia nazionale, pertanto ha una rilevanza assoluta proprio per le agenzie di intelligence.

Per questo motivo, fonti governative affermano che le informazioni inerenti ad un attacco condotto contro un'azienda, saranno condivise con le altre solo se la vittima che ha subito l'attacco lo autorizzerà esplicitamente. I civili, per l'accesso alle informazioni condivise, avranno un'autorizzazione di tipo 'mid-level', contrariamente ai funzionari dell'Intelligence che avranno autorizzazioni di più alto livello. Il distacco del personale civile alla nuova struttura, sarà su base volontaria e gli specialisti dovranno rimanere nel sito segreto di Fusion Cell per almeno sei-nove mesi.

Parallelamente, l'MI5 è coinvolto anche in un altro programma di 'outreach' (testualmente traducibile in 'raggiungere fuori'), in cui si impegna ad assistere alcune delle aziende incluse nel FTSE 100 Index[13] del Regno Unito. L'assistenza, anche in questo caso, è riferita all'aspetto della cyber security e della protezione delle infrastrutture legate al mondo della finanza. Nell'ambito del programma CISP, va ad inserirsi anche l'avvertimento lanciato da Sir Jonathan Evans, ex direttore generale dell'MI5, alle università inglesi, sull'importanza della tutela dei segreti commerciali. La comuni-

12 Information and Communication Technology.

13 FTSE 100 Index. Meglio conosciuto come indice FTSE 100, è un indice di riferimento delle 100 aziende con la più alta capitalizzazione di mercato quotate al London Stock Exchange. Rappresenta uno degli indici azionari di maggiore riferimento, ed è visto come un indicatore di valore rappresentativo del livello di business delle aziende del Regno Unito.

cazione, che risale ad aprile scorso, è stata inviata ai *vice chancellors* di tutte le università inglesi e comprende una serie di raccomandazioni sul problema della protezione delle proprietà intellettuali possedute da tutte le realtà accademiche del Regno. L'interazione esistente da decenni tra i Servizi di Intelligence britannici e le università inglesi, testimonia la corretta intuizione degli inglesi sui vantaggi che possono scaturire tra strutture dedicate alla salvaguardia della nazione e quelle che operano nel settore della formazione e della ricerca. È per questo motivo che la raccomandazione di Sir Evans è stata immediatamente accolta dalle università britanniche, come testimoniato dal Professor Eric Thomas, accademico inglese, che ha confermato in un'intervista al Financial Times[14], che le strutture accademiche e di ricerca del paese sono in 'allarme'.

Ma le 'celle di fusione di menti' non bastano…

L'idea di realizzare una 'cella' in cui concentrare i migliori cervelli informatici del paese, è certamente un'idea vincente. Ma l'idea di 'fondere' competenze ed esperienze possedute dai migliori esperti del paese, forse potrebbe non essere sufficiente per contrastare, se non addirittura sconfiggere le forze del male che imperversano nel Cyberspazio. Occorrono anche le migliori e più innovative tecnologie disponibili. È proprio su questa linea che sempre l'MI5 ha deciso di attivare nuove attività. In un articolo pubblicato sul quotidiano Daily Mail[15], è riportata la notizia che il servizio di intelligence inglese sarebbe intenzionato ad installare delle 'black box' (dispositivo attivo di rete in grado di filtrare ed esaminare il traffico dei pacchetti dati che viaggiano in Rete), per verificare il contenuto dei messaggi che viaggiano in Internet. Il sistema di controllo si basa sulla tecnologia *Deep Packet Inspection*[16], che consente di analizzare qualsiasi dato che viaggia in Rete, che si tratti di una mail o di un post inserito su un social network Facebook. Anche se ci sono state reazioni di indignazione da parte dei movimenti per le libertà civili e degli attivisti della privacy, criticando una violazione della stessa in funzione dell'utilizzo di questo dispositivo di 'spionaggio', una relazione presentata in Parlamento, a febbraio del 2013, dal Security Committee, evidenzia come sia diventata improcrastinabile l'adozione di sistemi di controllo in Rete finalizzati all'attivazione di azioni di contrasto nel caso si verifichino degli attacchi informatici. Non è solo il Gover-

14 *http://www.publicservice.co.uk/news_story.asp?id=22677* .

15 *http://www.dailymail.co.uk/sciencetech/article-2274388/MI5-install-black-box-spy-devices-monitor-UK-internet-traffic.html#ixzz2SEA9Hgf9* .

16 Deep Packet Inspection. È un sistema di packet filtering (filtraggio dei pacchetti) fruibile in Rete. Fa una verifica su tutti i dati che compongono un pacchetto che viaggia tra i nodi della rete. È possibile decidere se il pacchetto può circolare o se deve essere bloccato.

no di Sua Maestà a sostenere che l'accesso immediato alle comunicazioni in Rete sia fondamentale per la lotta al terrorismo ed altri crimini similari, anche l'attuale direttore dell'MI5, Jonathan Evans, lo ribadisce sostenendo '*L'accesso alle comunicazioni di qualsiasi tipo è molto importante. Rappresenta la spina dorsale del modo in cui affrontiamo le indagini. Penso che si possa affermare che non esistono indagini significative che non si basino sulla comunicazione di dati, in funzione del fatto che le stesse ci possono consentire di dirvi dove e quando saranno condotte azioni contro quali bersagli specifici*'.

Naturalmente siamo ancora allo stadio della proposta. L'installazione di questi dispositivi potrà essere autorizzata solo in funzione dell'approvazione di un apposito provvedimento legislativo. Inoltre con le black box le informazioni a cui i Servizi di Intelligence potrebbero accedere sarebbero limitate, ad esempio, ai soli dati del mittente e del destinatario di una email. Infatti, per l'accesso al contenuto del messaggio, in funzione delle leggi in vigore nel Regno Unito, sarebbe indispensabile un'autorizzazione del Tribunale di competenza.

Senza alcun dubbio, la creazione di strutture in cui possano convogliare le migliori menti del paese, rappresenta, a qualsiasi livello e per qualunque settore, un elemento di grande valore per una nazione. Lo è ancor di più se parliamo di sicurezza nazionale. Pertanto *Fusion Cell* rappresenta un esempio di trasformazione culturale che deve condurci a profonde riflessioni: la prima è data dalla consapevolezza che il problema della difesa di un paese deve costituire una preoccupazione che deve essere condivisa dall'intera collettività. In funzione di ciò ogni individuo deve sentirsi responsabile, quindi coinvolto, nel processo di strutturazione di un modello di protezione delle aziende, pubbliche e private che siano e, soprattutto, delle infrastrutture 'critiche' da cui dipende la stessa sopravvivenza di una nazione. In secondo luogo, risulta improcrastinabile l'attivazione di un piano di formazione nazionale dei cittadini sull'utilizzo delle tecnologie informatiche. Non basta più sapere cos'è un virus informatico o come proteggere i dati contenuti nel proprio profilo su Facebook (anche se sono ancora molti coloro che non lo sanno!). Bisogna innalzare il livello di conoscenza dell'utilizzo degli strumenti informatici a tutti i livelli, dal cittadino all'azienda, per consentire di combattere il peggiore di tutti i codici maligni: il costo dell'ignoranza informatica.

E Obama lancia il programma 'BRAIN Initiative'

Questo è il nome del progetto che il Presidente Barack Obama ha deciso di varare allo scopo di riuscire a mappare il cervello dell'uomo. Lo ha annunciato ad aprile scorso, confermando che nel bilancio fiscale 2014 l'attivazione del progetto peserà per un importo iniziale di 100 milioni di dollari. La durata del progetto è stimata in 10 anni, e dovrebbe raggiungere il co-

sto globale di circa 3 miliardi di dollari. Lo scopo è di arrivare a comprendere il funzionamento del cervello umano per scoprire delle nuove metodologie di cura per tutte quelle patologie che interessano l'apparato cerebrale umano, come l'autismo, l'epilessia, i traumi cerebrali, la schizofrenia e il morbo di Alzheimer. La tecnologia giocherà un ruolo determinante nel progetto (non è un caso che il termine BRAIN si riferisca all'acronimo Brain Research through AdvancIng Neurotechnologies), e il costo dell'intero programma sembra non spaventare il governo statunitense più di tanto, anche perché, secondo stime di organismi governativi, le malattie del cervello costano al sistema sanitario statunitense qualcosa come 500 miliardi di dollari all'anno. D'altronde anche il 'Progetto Genoma Umano' varato nel 1990 e conclusosi nel 2000 dal National Institutes of Health (NIH) per mappare tutti i geni del DNA umano, ha prodotto scoperte e vantaggi di portata incalcolabile. Va inoltre ricordato che tra i vari organismi studiati all'interno del progetto, ne troviamo anche uno (quello del batterio Escherichia Coli), che ha portato nel 2011 alla realizzazione di SPAM (Steganography by Printed Arrays of Microbes) un sistema di codifica dei batteri per la trasmissione di messaggi cifrati[17].

Anche il progetto BRAIN Initiative nasce all'interno del NIH, struttura che può vantare una strettissima collaborazione ultradecennale con DARPA (Defense Advanced Research Projects Agency), per lo sviluppo di progetti avanzati nel settore della difesa. Tra questi, poco pubblicizzato, è il '*chip to screen for safe and effective drugs*'[18] varato nel 2011 con la collaborazione del Food and Drug Administration, che prevede lo sviluppo di un microprocessore per la valutazione degli effetti dei farmaci sugli esseri umani. Anche se il chip sarà innestato su 'sistemi cellulari' simili al corpo umano, non si esclude la sperimentazione sugli individui. Il costo per i cinque anni di sperimentazione, ammonta a 70 milioni di dollari e DARPA si è impegnata a sostenere una parte corposa dell'investimento. Per quanto concerne BRAIN Initiative, l'apporto finanziario di DARPA si basa, per il solo anno 2014, su una somma di 50 milioni di dollari. L'obiettivo, come dichiarato dal direttore dell'agenzia, Arati Prabhakar, è di '*… comprendere le funzioni dinamiche del cervello e di dimostrare di poter sviluppare nuove applicazioni basate su queste intuizioni*'[19]. Egli ha inoltre dichiarato che '*L'iniziativa del Presidente rafforza l'importanza della comprensione di come i record del cervello, processano, utilizzano, memorizzano e recuperano grandi quantità di informazioni. Queste conoscenze delle funzionalità del cervello, potrebbero ispirare la progettazione di una nuova generazione di sistemi di elaborazione delle informazioni; condurre a intuizioni sulle lesioni cerebrali e sui meccanismi di recupero per permette-*

[17] A. Teti, *Il messaggio in codice viaggia con il batterio*, GNOSIS n. 4/2011 *(http://gnosis.aisi.gov.it/Gnosis/Rivista29.nsf/servnavig/13).*

[18] *http://www.nih.gov/news/health/sep2011/od-16.htm .*

[19] *http://www.medicalnewstoday.com/articles/258641.php .*

re nuove diagnosi, terapie e sviluppo di dispositivi in grado di riparare le lesioni traumatiche'. Ma nel contempo potrebbero consentire di sviluppare nuovi sistemi di interazione/comunicazione con il sistema nervoso centrale; la possibilità di colloquiare con il cervello dell'uomo grazie all'utilizzo di tecnologie wireless e processori RFID.

E le conferme su come le tecnologie possano interagire, se non addirittura integrarsi, con il sistema nervoso dell'uomo, non mancano di certo. In uno studio pubblicato lo scorso anno su Neuron[20], si cita il Brain Activity Map Project e gli autori spiegano come sia possibile realizzare delle piccole macchine molecolari capaci di funzionare come sensori, a livello cellulare, per monitorare l'attività dei neuroni. Gli scienziati spiegano che sebbene attualmente sia possibile avere una visione d'insieme delle attività cerebrali grazie alla magnetoencefalografia e alla risonanza magnetica funzionale, queste tecniche mancano di specificità cellulare e di risoluzione temporale. In altri termini non consentono di fotografare la singola attività neuronale in dato istante. E nonostante l'utilizzo del *calcium imaging* e del *voltage imaging* (che usano rispettivamente il calcio e i cambiamenti di voltaggio per monitorare l'attività elettrica dei neuroni), permane la necessità di aumentare l'efficacia dei sensori e della loro risoluzione temporale. Sarà attraverso l'utilizzo di nano particelle e nano diamanti, molto sensibili ai campi magnetici, che si potranno ottenere dei sistemi di monitoraggio e comprensione delle comunicazioni neuronali. Abbinando il tutto a sistemi ottici (come obiettivi, telecamere e algoritmi) che permetteranno di analizzare grandi zone del cervello, sarà finalmente possibile, grazie anche alle tecnologie wireless, colloquiare e interagire direttamente con il cervello umano.

Il progetto BRAIN Initiative consentirà, come ammesso dagli stessi responsabili, di spianare anche la strada ai progressi nel settore dell'intelligenza artificiale. Vale la pena di ricordare che da almeno cinque anni, grazie ai finanziamenti del Dipartimento della Difesa statunitense, il Centro Bioelectronics, Biosensors and Biochips (C3B) dell'Università di Clemson, sta sperimentando l'innesto di un microprocessore all'interno del cervello umano[21]. Ultima nota degna di riflessione sul progetto BRAIN Intiative, ci giunge da una riunione tenutasi lo scorso 17 gennaio. È stato organizzato un incontro presso il California Institute of Technology, a cui hanno partecipato NIH, DARPA e National Science Foundation oltre ai rappresentanti di Google, Microsoft e Qualcomm. Obiettivo: stabilire se esistono infrastrutture informatiche in grado di catturare e analizzare tutti i dati che giungeranno dal progetto. La conclusione è stata positiva[22].

20 *http://arep.med.harvard.edu/pdf/Alivisatos_BAM_12.pdf* .

21 A. Teti, *Microchip nel cervello. Privacy a rischio*, GNOSIS n. 4/2008 (http://gnosis.aisi.gov.it/Gnosis/Rivista17.nsf/servnavig/17).

22 *http://www.nytimes.com/2013/02/18/science/project-seeks-to-build-map-of-human-brain.html?pagewanted=all&_r=1&* .

Russian Human Genome Project: il DNA riprogrammato da Internet

I russi non stanno a guardare. E se lo fanno, per qualche breve periodo, è per carpire insegnamenti che possano essere utilizzati a loro vantaggio. Anche loro hanno varato un Progetto Genoma Umano che ha condotto ad una interessante teoria dai riscontri applicativi che potrebbero rivoluzionare il concetto stesso di riprogrammazione del DNA[23]. In un documento elaborato da Grazyna Fosar e Franz Bludorf (Vernetzte Intelligenz), sulle recenti scoperte sul DNA condotte in Russia, si spiega come il DNA possa essere 'influenzato e riprogrammato da parole e frequenze', in altri termini, sembrerebbe che le informazioni genetiche contenute nell'acido desossiribonucleico, oltre ad essere il responsabile della costruzione del nostro corpo, sia anche in grado di comunicare e archiviare dati. Gli scienziati russi, in collaborazione con dei linguisti, avrebbero trovato un codice genetico capace di 'seguire le stesse regole di tutte le lingue umane'. In effetti, se ci riflettiamo per un istante, il linguaggio umano non è altro che un riflesso del nostro DNA. Gli scienziati russi ritengono che la vita dei cromosomi funzioni proprio come un computer olografico, utilizzando radiazioni laser interne del DNA. Sarebbero quindi riusciti a modulare alcuni modelli di frequenze (suoni) attraverso un raggio laser in grado di influenzare la frequenza del DNA e di conseguenza l'informazione genetica stessa. Dato che la struttura di base delle coppie alcaline del DNA e la lingua parlata hanno la stessa struttura, la decodifica del DNA non sarebbe necessaria. Teoricamente, si potrebbero utilizzare le stesse parole del linguaggio umano (che sarebbero trasformate in frequenze finalizzate alla modifica delle informazioni del DNA) per riprogrammare il DNA di un essere umano. Naturalmente, non è dato sapere quali siano stati i reali risultati conseguiti dalle sperimentazioni in atto, tuttavia sembra che le stesse abbiano prodotto esiti molto incoraggianti. Se queste sperimentazioni dovessero dimostrare che è possibile interagire con il DNA, la portata della scoperta sarebbe a dir poco sensazionale. Facciamo un esempio: sappiamo bene che l'ipnosi è un fenomeno psicosomatico che coinvolge sia la dimensione fisica che quella psicologica del soggetto. Ed è stato ampiamente dimostrato che essa è una condizione particolare di funzionamento dell'individuo che gli consente di influire sulle proprie condizioni sia fisiche, sia psichiche e sia di comportamento. La ricerca russa potrebbe fornire un ulteriore contributo, in termini di spiegazione scientifica, sul perché le tecniche di ipnosi possano funzionare così bene in molteplici casi. Seguendo la linea delle possibilità offerte dalla ricerca russa, si potrebbe quindi ipotizzare l'utilizzo di strumenti tecnologici interconnessi in Rete (smartphone, tablet, netbook), per la trasmissione di frequenze utili alla modificazione delle informazioni contenute del DNA.

[23] *http://www.thinkaboutitdocs.com/russian-human-genome-project-discovers-extraterrestrial-abilities-to-modify-dna-through-a-biological-internet/* .

Di ciò ne è assolutamente convinto il professor Kevin Warwick, autorevole studioso di intelligenza artificiale e ingegneria biomedica dell'Università di Reading. Nel 1998 decise di impiantarsi un chip sottocutaneo a radiofrequenza (RFID) per dimostrare che poteva automaticamente aprire la porta del proprio ufficio, attivare il riscaldamento, accendere le luci nei locali in cui sostava, e a gestire tutti i dispositivi elettronici, computer compreso. Esperimento perfettamente riuscito. Il 14 marzo del 2002, si spinge oltre e decide di farsi impiantare nel suo braccio destro, un elettrodo array, forte di 100 elettrodi interconnessi direttamente al suo sistema nervoso, per governare, a distanza mediante la rete Internet, un braccio artificiale e una sedia a rotelle. Lo scienziato riuscì effettivamente a pilotarli dalla Columbia University, mentre il braccio e la sedia a rotelle erano ubicati presso l'Università di Reading. Esperimento anch'esso perfettamente riuscito. Ma Warwick non si arrese e decise di coinvolgere anche sua moglie in queste avveniristiche sperimentazioni. Adottando la stessa tecnica chirurgica, nel 2002, fece impiantare nel braccio di sua moglie un dispositivo analogo, con lo scopo di stabilire un canale comunicativo (quasi telepatico) tra loro. I rispettivi sistemi nervosi entrarono effettivamente in comunicazione, consentendo però solo l'interscambio di messaggi elementari (ad esempio quando la moglie dello scienziato muoveva il braccio, il movimento veniva avvertito dal marito). Lo stesso Warwick è convinto che nel futuro la società mondiale sarà popolata da forme di vita ibride, a metà tra l'essere umano e le macchine. Potremmo essere muniti di GPS integrato a livello cutaneo, o di un microchip in grado di monitorare i valori corporei (pressione, temperatura corporea, valori del sangue, ecc.) o, semplicemente, di un tag RFID in grado di autenticarci ogni volta che transitiamo negli aeroporti, in ufficio o in strutture pubbliche. Il prossimo obiettivo di Warwick, per i quali ha fissato un intervallo temporale di circa sette anni, si basa su di un progetto di comunicazione telepatica che consentirebbe la trasmissione di informazioni complesse come immagini o sensazioni.

La penetrazione della mente dell'uomo, in qualunque modo, sembra rappresentare uno degli obiettivi strategici del terzo millennio. Una dimostrazione di ciò è data dalla corposità dei finanziamenti che sono destinati a questo scopo. Le agenzie che operano nel settore dell'intelligence e della difesa, sono le protagoniste di questa sfida. Il Cyberspazio, le tecnologie di trasmissione dati avanzate, le nanotecnologie, le applicazioni software avanzate, sembrano fondersi in un unico coacervo tecnologico che mira al reperimento di ciò che più conta al mondo: le informazioni, di qualsiasi tipo e a qualsiasi livello. Il loro valore è incommensurabile e la sfida per assimilarne il maggior numero possibile e alla massima velocità realizzabile, rappresenta la vera sfida del terzo millennio. Si tratta solo di capire chi raggiungerà per primo questo risultato…

Bibliografia

- *http://www.medicalnewstoday.com/articles/258641.php*

- *http://www.nytimes.com/2013/02/18/science/project-seeks-to-build-map-of-human-brain.html?pagewanted=all&_r=0*

- *http://www.bibliotecapleyades.net/scalar_tech/esp_scalartech12.htm*

- *http://www.guardian.co.uk/uk/defence-and-security-blog/2013/mar/27/uk security-terrorism*

-*http://News.Techworld.com/security/3437386/Fusion-Cell-Cyber-Unit-will-defend-UK-business-from-Cyber-Attack-Government-Announces/*

- *http://www.dailymail.co.uk/sciencetech/article-2274388/MI5-install-black-box-spy-devices-monitor-UK-internet-traffic.html*

- *http://www.livescience.com/28354-obama-announces-brain-mapping-project.html*

- *http://en.wikipedia.org/wiki/BRAIN_Initiative*

- *http://www.thinkaboutitdocs.com/russian-human-genome-project-discovers-extraterrestrial-abilities-to-modify-dna-through-a-biological-internet/*

La riproduzione totale o parziale dell'articolo pubblicato non è ammessa senza preventiva autorizzazione scritta della Direzione.