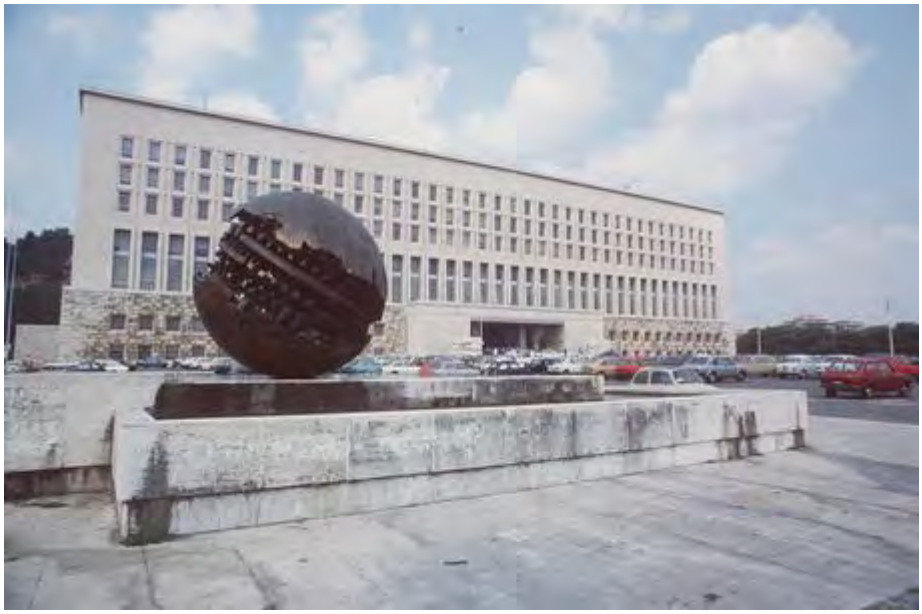
L'INSOSTENIBILE INADEGUATEZZA DEI VERTICI

Analisi Difesa

Gianandrea Gaiani



Tutte i commenti con cui gli esperti di cyber security hanno analizzato la notizia dell'attacco hacker al sistema informatico del Ministero degli Esteri italiano perdono significato di fronte allo scoop del quotidiano Il Mattino che ha scoperto come la protezione dei segreti della nostra politica estera siano stati affidati a società straniere, per di più facenti capo a due delle tre potenze mondiali più attive nel settore delle operazioni cyber, siano esse difensive o offensive.

Le valutazioni tecniche su come proteggere meglio gli accessi ai sistemi e le banche dati sono preziose così come le raccomandazioni di disporre di un valido sistema di allarme che rilevi la minaccia anche quando è già penetrata ed è attiva per impedire che sistemi informatici di portata strategica restino accessibili ad estranei senza che neppure ve ne sia la consapevolezza. Tutti aspetti fondamentali ma che divengono improvvisamente marginali di fronte all'insostenibile leggerezza di lasciare a compagnie straniere, russe e americane nella fattispecie, la gestione di sistemi informatici legati direttamente alla sicurezza, alla politica e agli interessi nazionali.

L'attuale ministro degli Esteri, Angelino Alfano, ha detto sabato che il governo "valuterà il da farsi solo dopo che avremo capito chi è il responsabile" dell'intrusione. Una risposta dilettantesca innanzitutto perché la minaccia cyber è furtiva per definizione, non lascia firme inequivocabili, come è già accaduto in passato un'attenta analisi potrà dirci che le intrusioni sono state effettuate dalla Russia o da altri Paesi ma non potrà attribuire al di là di ogni dubbio a uno Stato la responsabilità dell'azione.

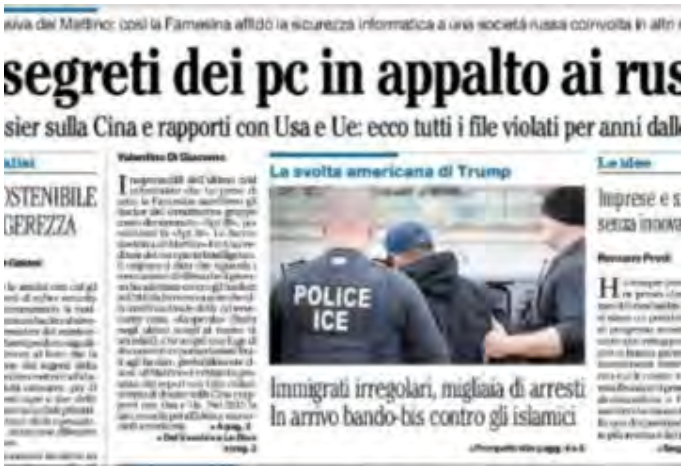
Non è inoltre possibile accusare nessuno, e non i propri vertici nazionali, se si affida a società straniere la sicurezza informatica delle proprie infrastrutture strategiche incluse quelle che gestiscono il nostro commercio estero.

Prima i russi della Kaspersky Lab, poi gli statunitensi della FireEye si sono accaparrati negli ultimi anni gli appalti milionari per la sicurezza informatica della Farnesina. Roba da repubblica delle banane! Ma in quale Stato con la S maiuscola si affidano a società straniere i dati del governo, della diplomazia e del commercio estero?

Persino gli sprovveduti sanno perfettamente che le società che operano nel settore cyber sono sempre legate, direttamente o meno, all'intelligence nazionale. Affidarsi a compagnie straniere per la sicurezza dei propri dati e comunicazioni significa avere la pressoché totale certezza che queste lavorino anche e soprattutto per gli interessi dei quei Paesi e che quindi dati e comunicazioni non siano al sicuro

Il caso Datagate ha dimostrato anche ai bambini che non ci sono amici e nemici, che le alleanze non escludono diffidenza e spionaggio, che tutti spiano tutti perché anche i Paesi amici sul piano politico o militare sono comunque rivali commerciali e perché in ogni caso conoscere i segreti degli altri aiuta ad anticiparne le mosse in tutti campi.

Edward Snowden era un contractor, un civile che lavorava per una società al servizio della NSA, agenzia che spia tutto il mondo e che subisce 300 mila tentativi d'intrusine informatica al giorno. Di società del genere ce ne sono molte in Usa ma anche in Gran Bretagna e Russia, sono composte per lo più da personale che in precedenza lavorava per l'intelligence e sono tutte strettamente collegate ai servizi segreti dei loro paesi che restano i loro più importanti clienti.



...iva del Maltino: così la Farnesina affidò la sicurezza informatica a una società russa coinvolta in altri ...

segreti dei pc in appalto ai rus

...sier sulla Cina e rapporti con Usa e Ue: ecco tutti i file violati per anni dall...

...STENIBILE
...GEREZZA

La svolta americana di Trump

Immigrati irregolari, migliaia di arresti
In arrivo bando-bis contro gli islamici

Le idee

Imprese e s...
senza mon...

Chi è lo sprovveduto che affiderebbe a russi e americani i segreti nazionali? Che affida a un gara d'appalto aperta a società straniere la sicurezza dei dati del Ministero degli Esteri di una delle prime 10 potenze economiche e delle prime 15 potenze militari mondiali qual è l'Italia?
E' chiaro che affidare a russi e americani la sicurezza della banca dati e delle comunicazioni della Farnesina equivale ad affidare a Diabolik la protezione degli accessi al caveau di Fort Knox.

Se degli USA sappiamo anche grazie al Datagate di non poterci fidare, circa la Russia occorre essere consapevoli che l'Italia le ha "dichiarato guerra" aderendo, pur controvoglia, alle sanzioni varate da USA e UE in seguito all'annessione della Crimea alla Russia.
Non si tratta di valutazioni di scarso peso. La Storia insegna che le privazioni economiche hanno spesso scatenato guerre.

Nel 1941 il Giappone decise di dare il via all'attacco alla base statunitense di Pearl Harbor per non veder soccombere la propria economia di fronte all'embargo petrolifero imposto da USA e alleati per l'annessione all'Impero del Sol Levante di parte del territorio cinese.

Più che normale quindi che a Mosca cerchino di spiare la nostra pur marginale e spesso inconsistente politica estera (soprattutto per capire cosa bolle in pentola negli scenari Ue, libici e nella penetrazione commerciale in mercati strategici come quelli asiatici) e infatti il portavoce del ministero degli Esteri russo, Maria Zakharova, si è limitata ad affermare che "non vi sono prove" del coinvolgimento russo nell'attacco alla Farnesina.

Non possiamo fidarci di alleati di cui siamo succubi come gli statunitensi (che sono nostri rivali in tutti i campi commerciali) e ancor meno di avversari cui imponiamo sanzioni come i russi. Perché allora affidare ad aziende di questi paesi i nostri segreti e le nostre banche dati?

La giustificazione che in Italia non esistono aziende in grado di operare in questo settore non regge. Basti pensare a CY4Gate fondata nel 2015 da Elettronica SpA (tra le più importanti aziende del mondo nella guerra elettronica,) e la modenese Expert System che opera nello sviluppo di tecnologie di cognitive computing per il supporto di intelligence e contrasto al crimine.

Abbiamo aziende che operano sul mercato strategico delle operazioni cyber con capacità difensive quanto offensive, società che hanno obblighi di riservatezza che possono e devono esser mantenuti e verificati costantemente perché concernono la sicurezza nazionale. Inoltre abbiamo servizi segreti che dovrebbero venire coinvolti nella protezione dei dati e dei sistemi di comunicazione criptati o meno degli apparati dello Stato.

"Errori" del genere non soni giustificabili né a livello politico né di dirigenza burocratica e possono essere motivati solo con una inaccettabile inadeguatezza dei vertici del governo (peraltro già gravemente emerso con l'annuncio dei nomi e dati personali degli agenti che a

Milano uccisero il terrorista dell'Isis, Anis Amri) o con il tradimento, termine sempre più desueto in un'epoca caratterizzata da continue cessioni di sovranità che a quanto pare riguardano anche la sicurezza nazionale.