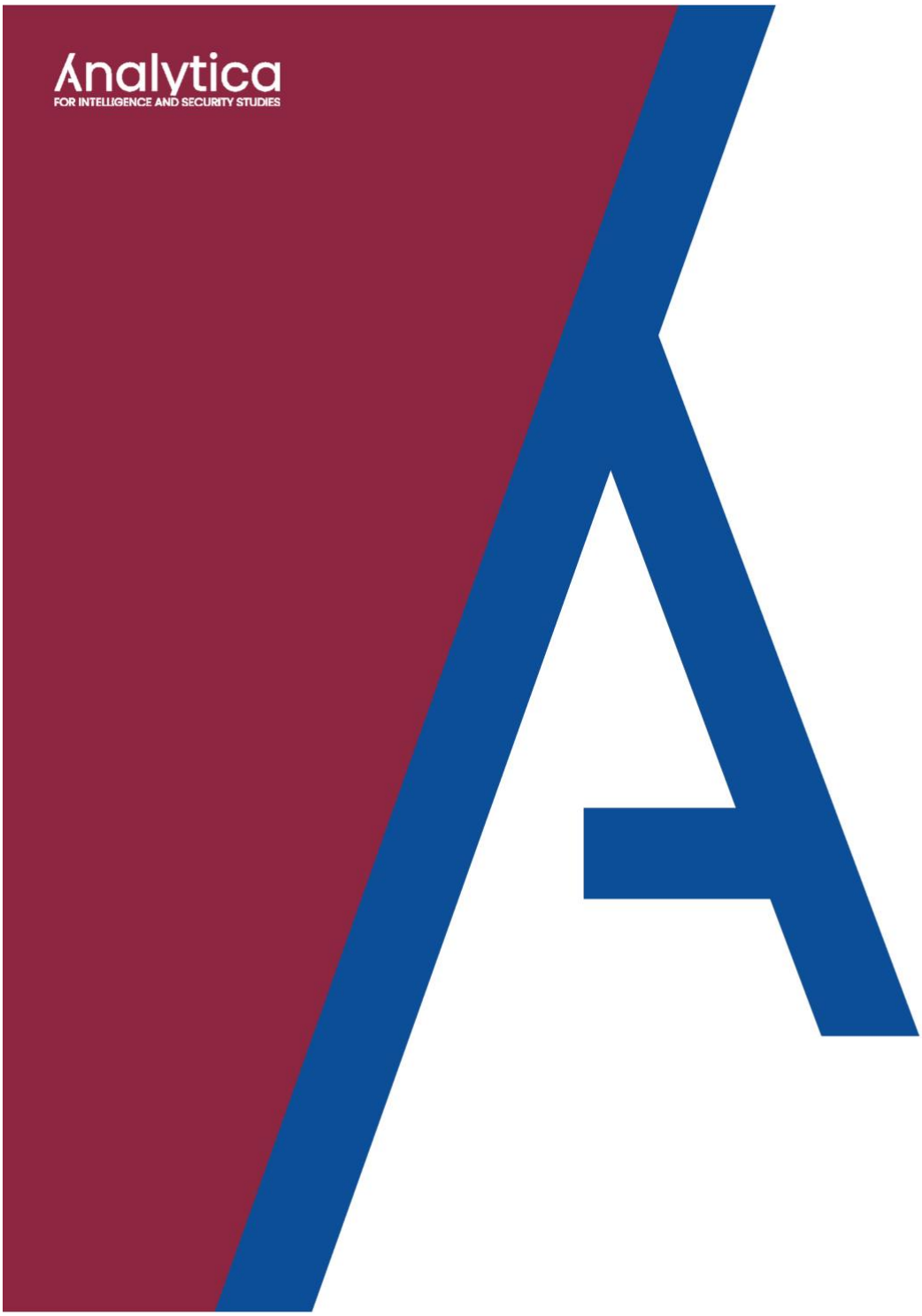

Dal caso Stuxnet all’analisi del panorama cibernetico italiano.

Francesca Caravita
Anaïs Michelle Cornolti - Viktoria Karanets - Lorenzo Noro
Lorenzo Pedullà - Sonia Tiralongo

Analytica for intelligence and security studies

Paper Cyber-Security

ISSN: 2784-8779

Dal caso Stuxnet all'analisi del panorama cibernetico italiano.

Francesca Caravita
Anaïs Michelle Cornolti - Viktoria Karanets - Lorenzo Noro - Lorenzo Pedullà
Sonia Tiralongo

Correzioni e revisioni a cura del Dottor SPELTA Maurizio

Direttore del Dipartimento Cyber - Security

Torino, giugno 2021

Il presente paper ha l'obiettivo di capire se, alla luce del caso Stuxnet analizzato, l'architettura cibernetica ed informatica attuale del nostro paese sarebbe in grado di fronteggiare un eventuale futuro attacco cyber della portata di Stuxnet. Per rispondere a questa domanda è stato diviso il lavoro in due parti: nella prima parte si è analizzato il caso Stuxnet in sé e per sé portando alla luce diversi aspetti, da quello geopolitico e delle relazioni internazionali a quello più tecnico e strategico; nella seconda parte invece sono stati delineati i punti di forza e di debolezza del nostro sistema in modo da valutare lo stato dell'arte attuale dell'Italia in ambito cyber.

Analisi di Stuxnet

Considerando che il caso Stuxnet è ritenuto un evento di rilevanza sia a livello tecnologico che geopolitico, nel presente capitolo si è analizzato lo stesso sotto diversi punti di vista; in una prima parte si è fornita un'analisi circa il contesto geopolitico dell'Iran con un focus sulla questione nucleare, in una seconda parte, invece, si è analizzato l'attacco informatico dal punto di vista fattuale e tecnico.

1.1 Il Contesto geopolitico

1.1.1 Non Proliferation Treaty

Basato su tre principi quali il disarmo, la non proliferazione e l'uso pacifico dell'energia nucleare, esso stabilisce il quadro di riferimento per regolare il commercio internazionale di materiali, tecnologie, impianti destinati alle applicazioni pacifiche dell'energia nucleare, e per assicurare controlli e salvaguardie atti a evitare la proliferazione nucleare "orizzontale", ossia l'aumento del numero di paesi dotati di capacità nucleari militari, e la proliferazione "verticale" ovvero lo stop alla corsa agli armamenti e la riduzione degli arsenali esistenti per i paesi definiti "potenze nucleari". Il TNP riconosce come tali Stati Uniti, Russia, Regno Unito, Francia e Cina poiché firmatari dell'accordo e che alla sua entrata in vigore avevano già acquisito una capacità nucleare militare[1].

L'Iran ha firmato il TNP nel 1968 e lo ha ratificato nel 1970.

[1] Per approfondire: https://www.un.org/en/conf/npt/2015/pdf/text%20of%20the%20treaty.pdf e https://www.armscontrol.org/factsheets/nptfact

1.1.2 Il programma nucleare iraniano

Il programma nucleare iraniano trova il suo fondamento nel quadro del progetto inaugurato dal Presidente americano Dwight Eisenhower nel 1953[2], nato dal suo discorso all'Assemblea Generale delle Nazioni Unite conosciuto come "Atoms for Peace", e inizia ufficialmente nel 1957 quando lo shāh Mohammed Reza Pahlavi e gli Stati Uniti siglano l'"Agreement for Cooperation Concerning Civil Uses of Atomic Energy", dopo due anni di negoziati[3].

Il programma nucleare iraniano, simbolo del processo di modernizzazione del Paese voluto dallo shāh, partì nel 1959 con l'apertura del Centro di Ricerca nucleare dell'Università di Teheran e fino al 1972 avrà come obiettivo solo quello della ricerca. Infatti, nel 1972 venne annunciata l'intenzione di costruire i primi reattori nucleari per la produzione energetica, ampliando inoltre la propria partnership per l'espansione delle infrastrutture nucleari con la firma di contratti con la Francia e la Germania dell'Ovest, e nel 1974 venne fondata l'Atomic Energy Organization of Iran (AEOI), affinché collaborasse in armonia con le agenzie internazionali preposte allo sviluppo pacifico dell'energia nucleare[4].

Il Programma nucleare iraniano e tutta l'impalcatura degli scambi commerciali e tecnologici con gli Stati Uniti e i paesi europei che si era andata a formare si interruppe bruscamente nel febbraio del 1979 quando la rivoluzione islamica prese il sopravvento.

Inizialmente vessato e rifiutato dalla visione anti-modernista del Khomeinismo, durante il conflitto con l'Iraq, iniziato nel settembre del 1980, la neonata Repubblica Islamica decise di riprendere lo sviluppo del programma nucleare intuendone le potenzialità in chiave militare, e quindi, in un'ottica di deterrenza: il solo possesso di quella tecnologia, magari proprio delle armi nucleari, avrebbe potuto far desistere Baghdad nell'aggressione contro l'Iran.

Dal 1987 Teheran riavviò il proprio programma cercando nuovi investitori esteri dopo il rifiuto dei precedenti accordi da parte di Germania e Francia, in particolare per la costruzione della centrale elettronucleare di Bushehr.

---

[2] Passato alla storia come "Atoms for Peace speech". Discorso del Presidente Dwight Eisenhower presso l'Assemblea Generale delle Nazioni Unite, consultabile sul sito https://www.iaea.org/about/history/atoms-for-peace-speech.

[3] Già nel 1946, con l' "Atomic Energy Act" con Truman gli Stati Uniti aprono il proprio mercato in tecnologia nucleare e Eisenhower, intuendo la paradossale dualità dell'era atomica, avvia il suo programma di condivisione del nucleare civile americano allo scopo di fornire il know-how tecnologico per lo sviluppo civile e allo stesso tempo promuoverne l'uso pacifico.

[4] Mustafa Kibaroğlu, *Iran's Nuclear Ambitions from a Historical Perspective and the Attitude of the West*, articolo contenuto all'interno della rivista Middle Eastern Studies, Vol. 43, n. 2, 2007

Nel 1987 venne siglato un accordo di cooperazione con il Pakistan per la formazione tecnica di personale, nel 1991 con la Cina per la realizzazione dell'impianto per la produzione di acqua pesante e la conversione e l'arricchimento dell'uranio di Isfahan e nel 1995 l'"Accordo di Cooperazione Nucleare" con la Russia, che comprendeva il completamento del blocco n.1 della centrale di Bushehr[5].

1.1.3 La controversia nucleare e delle tecnologie dual-use.

Nel 2002 si apre a livello internazionale e multilaterale la cosiddetta "questione sul nucleare iraniano", attraverso la crisi innescata dalle rivelazione fatte dal NCRI (Consiglio Nazionale della Resistenza Iraniana), oppositore del regime e che si proclama governo iraniano in esilio. Venne dichiarato in una conferenza stampa che l'Iran aveva continuato al lavorare sul suo programma nucleare clandestinamente; nella fattispecie ci si riferì agli impianti in costruzione di tecnologia *dual-use* per l'arricchimento dell'uranio di Natanz e per la produzione di acqua pesante di Arak. La notizia destò scalpore poiché lo sviluppo dei siti in questione non fu mai notificato all'Agenzia Internazionale per l'Energia Atomica (AIEA), per cui parve a tutti gli effetti una prova schiacciante per dimostrare la volontà dell'Iran di costruire armi nucleari. Gli Stati Uniti, appellandosi al TNP, definirono il fatto come una violazione dell'articolo II del trattato, mentre l'Iran replicò che nessuna disposizione del trattato pregiudicava il diritto inalienabile degli Stati firmatari di sviluppare un programma d'energia nucleare a scopi pacifici (art. IV(1), TNP). L'Agenzia Internazionale per l'Energia Atomica (IAEA) nei suoi sopralluoghi tra il 2002 e il 2003 notificò la presenza dei siti incriminati e di uranio arricchito[6].

La controversia politica e diplomatica si sviluppa e ruota attorno alle capacità della Repubblica islamica di Iran di procedere in modo autonomo all'arricchimento dell'uranio, sebbene sia consentito dall'articolo IV del TNP, in quanto necessario per la produzione di energia. Il motivo è rappresentato dal fatto che questo processo, che è la fase più delicata e rilevante del ciclo di produzione del combustibile nucleare, è reso possibile da sistemi tecnologici definiti *dual use*[7] cioè impiegati tanto a fini civili quanto a fini militari.

---

[5] Ibidem.

[6] Nima Gerami e Pierre Goldschmidt, *The International Atomic Energy Agency's Decision to Find Iran in Non-Compliance, 2002–2006*, Washington D.C., Center for the Study of Weapons of Mass Destruction, National Defense University Press, 2012

[7] Con il termine *dual use* (duplice uso) si identificano quei beni e quelle tecnologie che, pur essendo principalmente utilizzati per scopi civili, possono essere adoperati nella fabbricazione e nello sviluppo di diverse tipologie di armamenti.

Sia per la produzione di energia nucleare che per la costruzione di armi nucleari è indispensabile l'uranio arricchito; mentre per l'uso civile l'arricchimento necessario affinché avvenga il processo di fissione nucleare - e quindi di produzione di energia - si attesta intorno al 3-5 percento (LEU, low enriched uranium), per produrre un'arma nucleare efficace c'è bisogno di un arricchimento di oltre il 90 percento (HEU, high enriched uranium), definito come livello *weapon-grade*. Pertanto, se uno Stato ha la capacità di arricchire l'uranio ha potenzialmente anche la capacità di compiere il primo passo verso la costruzione della bomba atomica.

Un Iran in possesso di armi nucleari costituisce per la comunità internazionale una minaccia alla sicurezza internazionale sia sul fronte dell'evoluzione del sistema di relazioni internazionali in Medio Oriente sia per quanto riguarda il futuro dei regimi multilaterali di non-proliferazione nucleare.

La bomba atomica rappresenta un potente strumento politico per incrementare lo status di un paese nel Sistema internazionale, dal momento che fornisce uno dei più potenti deterrenti contro le minacce esterne e, allo stesso tempo, una leva per esercitare maggiore pressione diplomatica.

La potenziale acquisizione della capacità offensiva nucleare da parte di Teheran rivoluzionerebbe i delicati equilibri regionali nel Golfo Persico e in Medio Oriente, con conseguenti effetti negativi sugli obiettivi di non proliferazione a livello globale. Infatti, la probabile corsa alle armi nucleari che ne scaturirebbe potrebbe sgretolare i complessi sistemi multilaterali di controllo degli armamenti e di non proliferazione. Inoltre, se l'Iran diventasse una potenza nucleare rafforzerebbe enormemente la sua posizione rispetto ad Israele e agli altri Stati arabi del Golfo, stravolgendo così i rapporti di forza regionali che hanno finora mantenuto quel fragile equilibrio in Medio Oriente portandosi dietro anche l'intero sistema di alleanza costruito e retto dagli Stati Uniti, grazie al quale si sono assicurati il loro primato regionale in termini di sicurezza da dopo il 1979[8].

[8] Riccardo Alcaro, *Il Contenzioso sul Programma Nucleare Iraniano: origini, stato attuale, prospettive*, Roma, Servizio Studi Affari Internazionali - Contributi di Istituti di ricerca specializzati, 2006.

1.2 L’attacco informatico e le sue implicazioni

1.2.1 Analisi della minaccia

L’attacco alla nucleare di Natanz in Iran rappresenta un tema di discussione internazionale in quanto non si tratta solo di un caso di ingegneria informatica estremamente avanzato, ma, allo stesso tempo, viene identificato come il primo caso di cyber war. Di seguito si riportano le riflessioni emerse dall’analisi dell’evento da un punto di vista fattuale e tecnico.

L’attacco informatico perpetuato nel 2010 ai danni della centrale di Natanz ha provocato il malfunzionamento di circa 1000 delle 5000 centrifughe presenti nella centrale iraniana, mettendo in ginocchio una delle infrastrutture critiche della nazione. Le attività condotte nella centrale rientravano all’interno del progetto nucleare che l’Iran ha sempre dichiarato avere uno scopo energetico e quindi pacifico, anche se di questo non si può averne la certezza. In particolare, le centrifughe in questione trattavano l’esafluoruro in forma gassosa e servivano per operare il processo dell’arricchimento” dell’uranio ovvero, la separazione dell’isotopo U-235 da quello U-23. Stuxnet avrebbe provocato un’accelerazione improvvisa dell’attività delle centrifughe, spingendole al sovraccarico e poi al collasso.

Era giugno 2010 quando Stuxnet è venuto alla luce per la prima volta, identificato da VirusBlokAda, una società di sicurezza con sede in Bielorussia. Subito dopo Siemens, un gigante industriale tedesco, ha avvertito i suoi clienti che i loro sistemi di gestione "controllo di supervisione e acquisizione dati" (SCADA) erano vulnerabili al worm. Un worm è una tipologia di malware in grado di autoreplicarsi e fa parte della categoria degli *Advanced Persistent Threat* (APT). Più precisamente Stuxnet si rivolge ad una parte del software Siemens, chiamato WinCC, che gira su Microsoft Windows. Per motivi di sicurezza tali sistemi di solito non sono connessi a Internet. Ma Stuxnet si diffonde tramite memory stick USB o unità chiave. In pratica, quando una memory stick infetta viene collegata ad un computer, il software Stuxnet verifica se WinCC è in esecuzione. Se lo è, prova ad accedere, installa un sistema di controllo backdoor e contatta un server per istruzioni. Se non trova una copia di WinCC, cerca altri dispositivi USB e tenta di copiarsi su di essi. Può anche diffondersi su reti locali tramite cartelle condivise e spooler di stampa. WinCC è un sistema di gestione SCADA ragionevolmente oscuro. Secondo Ralph Langner, un esperto di sicurezza tedesco, Stuxnet esamina il sistema su cui è in esecuzione e, solo se vengono rilevate alcune caratteristiche molto specifiche, arresta processi specifici.

Utilizzando due certificati di sicurezza compromessi e un buco di sicurezza precedentemente sconosciuto di windows, il malware è stato in grado di avviarsi automaticamente nel momento in cui un utente tenta ha fatto accesso alla memory stick infettata. L'uso di falle di sicurezza precedentemente sconosciute (note nel commercio come "vulnerabilità zero-day") da parte dei virus non è insolito. Ma Stuxnet è stato in grado di sfruttare diverse di queste vulnerabilità per inserirsi nel sistema. Considerando il costo di una singola zero vulnerability, che viene venduta sul dark web a cifre esorbitanti, e la complessità tecnica dell'attaccare numerose superfici nello stesso momento, si presume che chiunque fosse dietro al progetto di Stuxnet avesse ideato l'attacco in modo molto strutturato e preciso, e disponesse di risorse, sia monetarie, che umane, rilevanti.

Alla luce dell'analisi condotta e delle riflessioni riportate, si può affermare che Stuxnet non ha colpito casualmente le centrifughe iraniane, ma che gli attaccanti avevano sicuramente Natanz e il suo impianto nucleare come obiettivo finale. Per quanto riguarda il tema dell'attribuzione, non si hanno informazioni certe ed ufficiali in quanto l'Iran non ha mai reso pubblica l'intera questione; diverse fonti riportano che l'attacco sia stato presumibilmente organizzato dagli Stati Uniti d'America con la collaborazione di Israele. Questo pone l'analisi sul piano della sicurezza delle nazioni, si tratta infatti di un esempio di cyber war, dove l'arma informatica viene impiegata per fini politici contro entità statuali.

1.2.2 Oltre Suxnet

Le centrali nucleari non sono gli unici sistemi presi di mira, ma anche altre infrastrutture sono state colpite da attacchi di hacker. Il 5 febbraio del 2021 le infrastrutture idriche di Oldsmart, una piccola città dello stato della Florida, hanno subito un cyber attacco che ha causato un aumento del livello di idrossido di sodio, sostanza che usata in grandi quantità avrebbe potuto avvelenare i cittadini della città di Oldsmart. Fortunatamente, l'operatore che si occupava delle infrastrutture idriche è riuscito ad intervenire prima che la composizione chimica dell'acqua cambiasse. La digitalizzazione delle infrastrutture, in aumento anche a causa della recente pandemia, espone queste infrastrutture a maggiori rischi. La differenza fra *Stuxnet* e questo attacco cibernetico, è che quest'ultimo è partito dal software TeamViewer, il quale permette di controllare a distanza un computer. Ciò crea dei vantaggi agli operatori che si occupano di monitorare queste infrastrutture potendo controllare a distanza, fattore importante durante un periodo di pandemia che predilige il lavoro a distanza. Questo vantaggio però può nascondere gravi problemi futuri, come visto nel caso dell'attacco alle centrali idriche in Florida.

Un altro caso di cyber attacco recente è il *Colonial Pipeline*, un sistema di condutture per prodotti petroliferi che rifornisce la costa orientale degli Stati Uniti d'America che si estende dal Texas fino al New Jersey. Il 7 maggio del 2021 un cyber attacco ha spinto la società americana a chiudere i tubi che permettono di rifornire benzina e carburante a buona parte delle città della costa orientale. Il virus che ha bloccato l'intera società di oleodotti è un *ransomware*, opera di *DarkSide* una società di hacker con sede in Russia. Il 12 maggio del 2021 la *Colonial Pipeline* ha iniziato il riavvio degli oleodotti, lo stesso giorno il prezzo medio della benzina ha superato i 3 dollari al gallone (non succedeva dal 2014). Nonostante il cyber attacco sia stato risolto dopo giorni e i rifornimenti di carburante siano stati ripristinati rapidamente, il problema di questo tipo di attacchi rimane negli Stati Uniti d'America crescente. Le strutture energetiche negli *States* restano vulnerabili agli attacchi degli hacker. Questi cyber attacchi destano preoccupazione non solo per il loro aumento negli anni, ma anche per i loro obiettivi, sempre più ambiziosi e pericolosi per il funzionamento delle infrastrutture cruciali che forniscono servizi essenziali alle popolazioni.

Architettura cibernetica italiana: la nazione è pronta per un nuovo Stuxnet?

Alla luce di quanto esaminato nel capitolo precedente relativamente al caso Stuxnet si è ritenuto opportuno procedere ad una valutazione della situazione attuale in Italia in ambito informatico e cibernetico, in modo da capire se il nostro paese sarebbe in grado di fronteggiare una minaccia informatica del calibro di Stuxnet. Al fine di analizzare lo stato dell'arte dell'architettura cibernetica italiana a livello sia privato che pubblico, si sono definiti i suoi punti di forza e i punti di debolezza.

Nell'ottica della sicurezza nazionale alla luce di casi come quello di Stuxnet, il piano normativo che in Italia regola la sicurezza digitale è da considerarsi un punto di forza. L'Italia infatti è stata uno dei primi paesi dell'UE a dotarsi di un'intelaiatura tecnica, legale e politica per far fronte alle minacce del cyber spazio. Dal 2005 esiste il "Codice dell'amministrazione digitale" (D.Lgs. n. 82/2005) che costituisce il riferimento normativo principale che disciplina l'adozione, l'utilizzo e l'evoluzione degli strumenti IT da parte delle Pubbliche Amministrazioni, promuovendone l'uso come strumento principale nei rapporti con il cittadino.

Nonostante l'importanza della norma appena citata, la vera svolta in termini di sicurezza è stata realizzata col DPCM del 24 Gennaio 2013 che definisce gli "Indirizzi per la protezione cibernetica e la sicurezza informatica nazionale". Questo è il testo che per la prima volta ha definito e regolamentato l'architettura di sicurezza cibernetica di cui l'Italia deve dotarsi.

L’allineamento fra gli standard italiani e quelli europei è arrivato nel 2016 con la direttiva EUNIS (*European Union Network and Information Security*) 2016/1148, volta a stabilire le misure per la realizzazione in Europa di un ambiente digitale sicuro e affidabile. Essa dispone che gli Stati Membri dell'Unione europea adottino di una serie di misure di sicurezza comuni ed adeguate, imponendo allo stesso tempo la notifica degli incidenti alle autorità nazionali istituite allo scopo.

Nel 2019 sono stati avviati i lavori per riformare completamente l’architettura nazionale della sicurezza informatica. Il provvedimento dello stesso anno istituisce il Computer Security Incident Response Team (CSIRT) presso il Dipartimento delle Informazioni per la Sicurezza (DIS) della Presidenza del Consiglio dei Ministri, con il compito di definire le procedure tecniche per la prevenzione, la gestione degli incidenti, e per informare gli altri Stati membri dell’UE eventualmente coinvolti da incidenti, garantendo la collaborazione nella rete CSIRT, attraverso l’individuazione di forme di cooperazione appropriate, lo scambio di informazioni e la condivisione di best practices.[9]

L’ammodernamento è durato fino all’anno scorso con la creazione del “Perimetro Nazionale di Sicurezza Cibernetica”. Questo, attraverso cinque diversi provvedimenti (DPCM 131/2020, DPCM 1/9/2020, DPR 24/7/2020, DPCM 1/11/2020, DPCM 8/3/2021), definisce una serie di soggetti ed elementi da salvaguardare perché vitali alla sicurezza nazionale.[10]

Un altro punto di forza del sistema nazionale di sicurezza informatico è dato dalla presenza di aziende leader e istituzioni che permettono all’Italia una leva strategica non irrilevante. Leonardo SPA è un’azienda finanziata al 79% dallo stato (48,8% investitori istituzionali + 30,2% MEF), che si occupa di “soluzioni di cyber security ed intelligence all’avanguardia per prevenire e gestire il crimine”. L’azienda è un consorzio di nove imprese diverse che si occupano anche di sistemi missilistici, aerospaziali, radar, sorveglianza e telecomunicazioni. I siti di Leonardo sono distribuiti in 20 Paesi (42% in Italia e 58% all’estero). Nel mondo sono circa 150 i paesi utilizzatori di prodotti, sistemi e servizi dell’azienda.

[9] Cfr. https://www.sicurezzanazionale.gov.it/sisr.nsf/archivio-notizie/cybersecurity-come-cambia-larchitettura-nazionale.html

[10] Cfr. https://www.agendadigitale.eu/sicurezza/perimetro-di-sicurezza-cibernetica-e-agenzia-dedicata-cosi-la-cyber-italiana-cerca-il-salto-di-qualita/

Le attività produttive e le basi industriali e commerciali principali sono collocate prevalentemente, oltre che in Italia, nel Regno Unito, in Polonia e negli Stati Uniti. Nel tempo la società ha stabilito una solida presenza anche in Francia e Germania ed è partner di riferimento in diverse collaborazioni industriali e istituzionali (come NATO, UE e Ministero della Difesa) su scala internazionale.[11]

Oltre a Leonardo è utile nominare Yarix, che dal 2001 fornisce servizi integrati di sicurezza informatica e disaster recovery. Fin dall'inizio Yarix ha messo a disposizione dello Stato la sua expertise, collaborando con esso sia sul piano della formazione nei confronti di agenti e funzionari, sia sul piano della consulenza, in occasione di indagini che richiedevano competenze specifiche in digital forensics, supportando gli ufficiali di pubblica sicurezza nell'identificazione delle prove memorizzate all'interno di sistemi e dispositivi informatici. Nel luglio del 2016 l'azienda ha firmato un Protocollo d'Intesa con la Polizia di Stato per la prevenzione e il contrasto dei crimini informatici su sistemi informativi critici. Un accordo importante e strategico che ha preso le mosse dalla necessità di garantire un'elevata sicurezza al Paese e al suo sistema economico e sociale, ormai fortemente dipendente dallo spazio cibernetico, mediante la cooperazione mirata, di pubblica utilità, tra lo Stato ed i privati, così come previsto dal Quadro Strategico Nazionale e dal Piano Nazionale per la Protezione Cibernetica e la Sicurezza Informatica. Una collaborazione che prevede la condivisione e l'analisi di informazioni idonee a prevenire attacchi o danneggiamenti che possano pregiudicare la sicurezza delle infrastrutture informatiche monitorate da Yarix, la segnalazione di emergenze relative a vulnerabilità, minacce ed incidenti e l'identificazione dell'origine degli attacchi subiti dalle infrastrutture tecnologiche. L'accordo ha previsto inoltre attività di comunicazione fra le parti in caso di situazioni di emergenza.[12]

A prescindere da quelle che possono essere considerate "eccellenze" Italiane nel campo della cyber security, recenti attacchi informatici che hanno avuto come protagoniste entità pubbliche e private Italiane (si ricordano i recenti attacchi al Comune di Brescia e alla sopracitata Leonardo) ci dimostrano che ancora tanto deve essere fatto sul fronte della sicurezza informatica. In una prospettiva comparata, è utile anche menzionare l'attacco cibernetico tramite ramsonware "Ekans", condotto fra il 7 e l'8 Giugno 2020 nei confronti di Enel e Honda: ideato per targetizzare e colpire sistemi di controllo industriale (in linea dunque, con il target per cui era stato ideato Stuxnet), ha causato disservizi temporanei alle attività di assistenza ai clienti, ma non ha avuto effetti deleteri e

[11] Cfr. https://www.leonardocompany.com/it/security-cyber/cyber-digital-solutions
[12] Cfr. https://www.yarix.com/about-yarix/

dannosi sulle centrali elettriche, impattando quindi in maniera minore rispetto a quanto accaduto nel caso delle centrali nucleari iraniane[13]. Nel caso specifico di Honda, l'azienda ha comunicato di aver riscontrato problemi a livello di relazioni produttive con alcuni partners europei, a dimostrazione del fatto che, nel mondo interconnesso di oggi, un cyber-attack mirato possa avere delle ripercussioni non soltanto in un singolo contesto aziendale, ma soprattutto anche nelle relazioni bilaterali e/o multilaterali con gli altri attori statuali.

I punti deboli del "sistema Italia" sembrano essere amministrazioni locali e piccole-medie imprese, spesso messe in difficoltà da leadership poco qualificata e fondi insufficienti. Questa realtà si inserisce all'interno di un contesto più ampio che è stato acutizzato dalla recente pandemia da COVID-19. Un articolo su l'analfabetismo digitale di Milena Gabanelli nella rubrica Dataroom del Corriere della sera ci racconta che secondo l'OCSE, solo il 21% degli italiani ha un livello di alfabetizzazione digitale sufficiente e che:

- Il 31% degli italiani non utilizza Internet;
- Solo il 13% degli italiani utilizza l'online per le procedure amministrative (media UE: 30%);
- In Italia l'8% delle PMI vende anche online (in Germania il 23%);
- Il 40% dei dipendenti di imprese private italiane non sa utilizzare bene i software da ufficio (Office, CSM, CRM e simili)[14].

Un qualunque lavoratore o impiegato (pubblico o privato), senza il dovuto livello di alfabetizzazione digitale, è facile preda di attacchi di phishing, non sa proteggere i propri dati con copie di backup, non sa distinguere un sito web o un'e-mail legittima da una ingannevole, e soprattutto non sa diagnosticare la possibile presenza di malware sul proprio computer. Appare pertanto cruciale accrescere la cosiddetta *People Awareness* a livello nazionale, con lo sviluppo di iniziative di sensibilizzazione e alfabetizzazione digitale che coinvolgano non solo le realtà istituzionali e aziendali, ma anche i soggetti privati che operano a stretto contatto con le reti e i sistemi informativi. Indubbiamente, nel momento in cui entrano in gioco interessi economici, geopolitici e geostrategici (si pensi al furto di proprietà intellettuale o all'acquisizione di know-how straniero), è più "semplice" ipotizzare che grandi realtà possano essere bersaglio di un cyberattacco.

[13] Cfr. https://www.cybersecurity360.it/nuove-minacce/ransomware/ekans-ransomware-colpisce-enel-e-honda-ecco-come-e-gli-effetti/
[14] Cfr. https://www.pandasecurity.com/it/mediacenter/mobile-news/analfabetismo-digitale-italia/

Tuttavia, va rilevato come le minacce cibernetiche costituiscano una realtà con cui ciascuno di noi si ritrova a fare i conti quotidianamente. Basti pensare, infatti, alle minacce cyber a cui l'intera comunità nazionale è stata esposta in maniera esponenziale durante il periodo pandemico e in particolare durante le varie fasi di lockdown: l'esigenza di effettuare acquisti online e di adempiere ad impegni lavorativi esperibili solo in smart-working, hanno accresciuto e moltiplicato le possibilità di essere vittime di attacchi informatici, come frodi e campagne di phishing tramite e-mail, ma anche tramite app di messaggistica quali Telegram o Signal (si consideri, ad esempio, il caso di social engineering che ha coinvolto molti utenti Signal lo scorso marzo, colpiti da una campagna di phishing che ha sfruttato il marchio Amazon per poi rubare dati personali e bancari).

Nell'ottica di una maggiore o minore esposizione alle minacce cibernetiche, il cosiddetto "fattore umano" costituisce la *vulnerability* ineliminabile di ogni contesto pubblico o privato, che può inficiare in modo gravoso la tutela della sicurezza del personale e di un contesto lavorativo in generale[15]. Da una prospettiva di governance e di predisposizione di adeguate strategie difensive e di cybersecurity, è sicuramente possibile limitare i danni, ma va altresì rilevato come anche realtà dotate di avanzate misure di cyber-difesa, con SOC e CERT di rilievo e ben organizzati, possano poi essere oggetto di attacchi sofisticati (come i sopracitati casi di Enel e Honda).

Discostandosi dal contesto prettamente nazionale e osservando la questione da una prospettiva europea, va sicuramente menzionata l'opera mirata di *raising awareness*, nonché di agevolazione della cooperazione in ambito cyber a livello interstatale e interaziendale, portata avanti dall' European Cyber Security Organization (ECSO), fondata nel 2016[16]. Nello specifico, appare utile citare il ruolo del *Working Group 5* della suddetta organizzazione, che svolge un ruolo di rilievo nella sensibilizzazione delle nuove generazioni (con focus specifico sulla fascia di popolazione compresa entro i 6 e i 26 anni) circa l'importanza di una cultura dell'awareness digitale a livello europeo[17]. Come stabilito dalla Comunicazione della Commissione Europea del 2013 sulla strategia dell'UE per cybersicurezza, un'importante opera di sensibilizzazione a livello europeo è affidata anche all'ENISA[18] (Agenzia Europea per la Sicurezza delle Reti e dell'Informazione), impegnata in prima linea ad assistere gli Stati membri nello sviluppo di adeguate capacità di cyber-resilienza.

---

[15] Cfr. https://www.cybersecurity360.it/nuove-minacce/fattore-umano-e-attacchi-apt-tecniche-offensive-e-strategie-di-remediation/

[16] Cfr. https://ecs-org.eu/cppp

[17] Cfr. https://ecs-org.eu/working-groups/wg5-education-training-awareness-cyber-ranges

[18] Cfr. https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52013JC0001&from=en, pag. 8.

L'ENISA, in particolare, riveste una posizione di punta nella sensibilizzazione dell'opinione pubblica circa i rischi connessi alla cybersecurity, nonché nell'elaborazione di orientamenti e buone pratiche destinati alle imprese, ai cittadini e a chiunque si ritrovi ad operare nel contesto del cyberspazio[19].

In considerazione dell'impatto avuto dal worm Stuxnet sul contesto iraniano, appare necessario chiedersi, in una prospettiva comparativa, quali potrebbero essere le ripercussioni e implicazioni di un eventuale Stuxnet 2 (o di altri worm, malware o ransomware con caratteristiche simili) sul contesto italiano. In altre parole: come si pone il nostro Paese nello scacchiere geopolitico europeo e internazionale in ambito cyber? Rispetto agli altri attori statuali, riveste, ad oggi, un ruolo di rilievo in termini di capacità di cyber-resilienza e cyber-difesa? Stando a quanto analizzato finora, è osservabile come l'Italia possa essere verosimilmente pronta a una situazione critica come potrebbe essere uno Stuxnet 2; anche alla luce del fatto che il nostro paese si è affermato in posizione di rilievo sia nel contesto dell'Unione Europea, partecipando attivamente e proficuamente ad esercitazioni cibernetiche particolarmente complesse e ad iniziative propugnate a livello unilaterale da alcuni Paesi (ad esempio, la CETATEA, organizzata dall'esercito rumeno[20]), ma anche a livello NATO. I risultati raggiunti dal nostro Paese in tali esercitazioni farebbero ben sperare in previsione di un eventuale attacco informatico, del calibro di Stuxnet, a infrastrutture critiche nazionali. Tra le esercitazioni organizzate in contesto UE e promosse in particolare dalla sopracitata ENISA, vanno menzionate:

- L'esercitazione biennale Cyber Europe 2018, che ha visto la proficua partecipazione dell'Italia tramite il CSIRT nazionale e il CIOC (Comando Interforze per le Operazioni Cibernetiche) dello Stato Maggiore della Difesa[21] nella «*gestione e mitigazione di un attacco informatico su vasta scala mirato alle infrastrutture di controllo del traffico aereo*[22]»;

[19] Regolamento (UE) 2019/881 del Parlamento Europeo e del Consiglio del 17 aprile 2019, relativo all'ENISA. Disponibile al link: https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32019R0881&from=PT

[20] F. Vestito (2020), *L'Italia nelle esercitazioni di cyber defence internazionali*, disponibile su: https://www.ispionline.it/it/pubblicazione/litalia-nelle-esercitazioni-di-cyber-defence-internazionali-22220

[21] Istituito nel 2017, persegue l'obiettivo di proteggere le reti strategiche della difesa, nonché di condurre delle operazioni cibernetiche a supporto delle attività militari dell'esercito italiano.

[22] F. Vestito (2020), *L'Italia nelle esercitazioni di cyber defence internazionali*, disponibile su: https://www.ispionline.it/it/pubblicazione/litalia-nelle-esercitazioni-di-cyber-defence-internazionali-22220

- La Blue OLEx (*Blueprint Operational Level Exercise*), che ha avuto luogo in settembre 2020 e che ha visto l'Italia affermarsi come *player* statuale di grande livello in termini di capacità di cyber-defence e cyber-resilienza[23]. La Blue OLEx ha rappresentato altresì l'occasione per presentare la rete CyCLONe (*Cyber Crisis Liaison Organisation Network*), che deve servire a fornire una risposta tempestiva e coordinata a livello UE a qualsiasi tipologia di attacco cibernetico nei confronti degli Stati membri; per l'ideazione di CyCLONe va menzionato l'impegno profuso in particolare dal DIS italiano e dall'ANSSI francese[24].

Anche in ambito NATO il nostro Paese si è distinto in modo ragguardevole:

- Nel 2013[25], ha preso parte alla *Bold Quest demonstration*, organizzata dal Joint Staff statunitense sin dal 2003 e che prevede, tra le altre, la verifica delle capacità acquisite e sviluppate in ambito cyber, in termini di efficacia, tattica e difesa[26];

- È stato uno dei primi a partecipare all'esercitazione NATO *Cyber Coalition*, che prevede la cooperazione tra i Paesi membri dell'Alleanza al fine di elaborare e sviluppare procedure comuni per la tutela del cyberspazio dell'Alleanza. Giunta alla sua tredicesima edizione, nel novembre 2020 l'esercitazione è stata svolta virtualmente, nel rispetto delle misure precauzionali causa COVID-19[27];

- Figura tra le *Sponsoring Nations* del Centro di Eccellenza NATO per la Difesa Cibernetica[28], che ogni anno organizza la *Locked Shields*, esercitazione per la difesa cibernetica unica al mondo e tra le più complesse in assoluto, durante la quale i Paesi partecipanti vengono addestrati alla difesa dei sistemi IT e delle infrastrutture critiche nazionali da oltre 2500 attacchi di varia natura[29].

---

[23] F. Cabassi (2020), *ENISA, Blue OLEx: L'Italia in prima linea nella cyber security UE*, disponibile su: https://www.aicom.it/it/enisa-blue-olex-litalia-in-prima-linea-nella-cyber-security-ue/

[24] Cfr. https://www.sicurezzanazionale.gov.it/sisr.nsf/archivio-notizie/cybersecurity-leuropa-testa-la-sua-sicurezza-cibernetica-con-lesercitazione-blue-olex.html

[25] G. Caravelli-V. Falzarano (2013), *La Difesa italiana partecipa alla Bold Quest 2013*, disponibile su: https://www.difesa.it/InformazioniDellaDifesa/Pagine/bold-quest-2013.aspx

[26] Cfr. https://www.jcs.mil/Media/News/News-Display/Article/1378256/us-forces-complete-coalition-capability-demonstration-and-assessment-with-16-pa/

[27] Cfr. https://www.act.nato.int/cyber-coalition

[28] Cfr. https://ccdcoe.org/about-us/

[29] Cfr. https://ccdcoe.org/exercises/locked-shields/

Conclusione

Come detto nella sezione introduttiva il presente lavoro non intendeva limitarsi all'analisi dell'attacco Stuxnet, ma ambiva ad ampliare la questione analizzando il grado di resilienza del contesto cibernetico italiano a fronte di un'eventuale "Stuxnet2".

La risposta a tale interrogativo appare piuttosto complessa e sarebbe riduttivo, oltre che difficile, rispondere in modo totalmente affermativo o negativo.

Alla luce dei dati riportati, si è potuto vedere come l'Italia sia all'avanguardia in materia, in particolare a livello giuridico ed istituzionale, e abbia raggiunto alti livelli di expertise sia nel contesto europeo che in quello atlantico, alla luce anche della partecipazione a esercitazioni cibernetiche multilaterali. Si evince quindi che l'Italia ravvisi il suo principale punto di forza sul piano della governance del fenomeno a livello nazionale ed europeo, grazie ad un'infrastruttura reattiva e ben organizzata (CSIRT e la definizione e regolamentazione costantemente aggiornata del Perimetro Nazionale di Sicurezza Cibernetica).

Come già delineato precedentemente, il principale punto debole italiano, e quindi più vulnerabile a potenziali attacchi cyber di tipo APT o più probabilmente ransomware, sembrerebbe essere la grande quantità di PMI e le amministrazioni locali. I due casi sono estremamente peculiari all'interno del sistema Italia (le prime, pilastro del tessuto economico italiano al 2019, prima della pandemia da COVID-19, rappresentavano il 92% delle imprese attive in Italia[30]). ed entrambe hanno in comune la bassa disponibilità di risorse da investire nella sicurezza digitale, sia a livello operazionale, che di governance e formazione, e la poca *awareness* in materia di rischi informatici.

Inoltre, dato il basso livello di alfabetizzazione digitale in Italia, appare evidente che eventuali *policies* nazionali da attuare in contrasto alle minacce cibernetiche debbano essere prima di tutto orientate verso la formazione digitale e la sensibilizzazione sulla sicurezza informatica, affinché si sviluppi consapevolezza sull'importanza della prevenzione, che rimane il principale argine alle *cyber threats*.

[30] Cfr. https://www.infodata.ilsole24ore.com/2019/07/10/40229/

Bibliografia e sitografia:

- Mustafa Kibaroğlu, *Iran's Nuclear Ambitions from a Historical Perspective and the Attitude of the West*, articolo contenuto all'interno della rivista Middle Eastern Studies, Vol. 43, n. 2, 2007
- Nima Gerami e Pierre Goldschmidt, *The International Atomic Energy Agency's Decision to Find Iran in Non- Compliance, 2002–2006*, Washington D.C., Center for the Study of Weapons of Mass Destruction, National Defense University Press, 2012
- Riccardo Alcaro, *Il Contenzioso sul Programma Nucleare Iraniano: origini, stato attuale, prospettive*, Roma, Servizio Studi Affari Internazionali - Contributi di Istituti di ricerca specializzati, 2006 consultabile al sito: http://www.iai.it/sites/default/files/pi_a_c_040.pdf
- https://www.sicurezzanazionale.gov.it/sisr.nsf/archivio-notizie/cybersecurity-come-cambia-larchitettura-nazionale.html
- https://www.agendadigitale.eu/sicurezza/perimetro-di-sicurezza-cibernetica-e-agenzia-dedicata-cosi-la-cyber-italiana-cerca-il-salto-di-qualita/
- https://www.leonardocompany.com/it/security-cyber/cyber-digital-solutions
- https://www.yarix.com/about-yarix/
- https://www.pandasecurity.com/it/mediacenter/mobile-news/analfabetismo-digitale-italia/
- https://www.cybersecurity360.it/nuove-minacce/ransomware/ekans-ransomware-colpisce-enel-e-honda-ecco-come-e-gli-effetti/
- https://www.cybersecurity360.it/nuove-minacce/fattore-umano-e-attacchi-apt-tecniche-offensive-e-strategie-di-remediation/
- https://ecs-org.eu/cppp
- https://ecs-org.eu/working-groups/wg5-education-training-awareness-cyber-ranges
- https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52013JC0001&from=en, pag. 8.
- https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32019R0881&from=PT
- F. Vestito (2020), *L'Italia nelle esercitazioni di cyber defence internazionali*, disponibile su: https://www.ispionline.it/it/pubblicazione/litalia-nelle-esercitazioni-di-cyber-defence-internazionali-22220

- F. Cabassi (2020), *ENISA, Blue OLEx: L'Italia in prima linea nella cyber security UE*, disponibile su: https://www.aicom.it/it/enisa-blue-olex-litalia-in-prima-linea-nella-cyber-security-ue/
- https://www.sicurezzanazionale.gov.it/sisr.nsf/archivio-notizie/cybersecurity-leuropa-testa-la-sua-sicurezza-cibernetica-con-lesercitazione-blue-olex.html
- G. Caravelli-V. Falzarano (2013), *La Difesa italiana partecipa alla Bold Quest 2013*, disponibile su: https://www.difesa.it/InformazioniDellaDifesa/Pagine/bold-quest-2013.aspx
- https://www.jcs.mil/Media/News/News-Display/Article/1378256/us-forces-complete-coalition-capability-demonstration-and-assessment-with-16-pa/
- https://www.act.nato.int/cyber-coalition
- https://ccdcoe.org/about-us/
- https://ccdcoe.org/exercises/locked-shields/
- https://www.economist.com/united-states/2021/02/09/a-cyber-attack-on-an-american-water-plant-rattles-nerves
- https://www.economist.com/graphic-detail/2021/05/10/ransomware-attacks-like-the-one-that-hit-colonial-pipeline-are-increasingly-common
- TNP:https://www.un.org/en/conf/npt/2015/pdf/text%20of%20the%20treaty.pdf , https://www.armscontrol.org/factsheets/nptfact;
- Atoms for Peace speech: https://www.iaea.org/about/history/atoms-for-peace-speech .
- https://www.infodata.ilsole24ore.com/2019/07/10/40229/