CYBER SEC

IL PERIMETRO NAZIONALE

La garanzia della Difesa italiana ed europea nella dimensione cyber inizia dal controllo e dal monitoraggio della produzione industriale delle tecnologie informatiche. Non è possibile concepire un sistema sicuro, impiegando esperti e adottando soluzioni futuribili ma non considerando l'originaria integrità di ogni singola componente hardware e software.
Inoltre, le vulnerabilità introdotte nella rete di un singolo Stato membro della UE potrebbero ripercuotersi velocemente all'interno di infostrutture dell'Unione, causando violazioni su vasta scala difficilmente comprimibili, anche con una pronta reazione degli organismi operativi delle difese europee.
In questa prospettiva, l'Italia ha intrapreso con slancio l'opera di aggiornamento del suo sistema di norme e della sua architettura organizzativa agli orientamenti espressi in sede europea

Strategia UE del 2013 e direttiva *Network and Information Security* del 2016

Finalmente, nel 2013, dopo anni di limitati risultati, viene espresso dall'Unione Europea un articolato documento di natura programmatica, strutturato su un ampio spettro d'interventi per la sicurezza della dimensione digitale e volto a rendere omogenee le regole in materia in tutti gli Stati membri.
Uno dei cardini sui quali ruota l'intero sistema di protezione è rappresentato dal mercato unico digitale. La garanzia della Difesa europea e della privacy dei cittadini inizia dal controllo e dal monitoraggio della produzione industriale delle tecnologie informatiche. Importante sottolineare che la paternità del provvedimento "guida" risale alla Commissione, in particolare all'Alto rappresentante per gli affari esteri e la politica di sicurezza.
In ambito europeo, si strutturano coordinamenti maggiormente codificati tra l'Agenzia europea per

DI SICUREZZA CIBERNETICA

Umberto MONTUORO (*)
Tenente Colonnello (AM)

la sicurezza delle reti e dell'informazione (ENISA), l'Agenzia europea per la Difesa (EDA), l'EUROPOL, per i compiti di polizia, e l'EUROJUST, quest'ultima competente nel promuovere o nel rispondere alle richieste di assistenza giudiziaria provenienti dai singoli Stati membri.

Le attività legate al rafforzamento della *cyber* sicurezza rientrano nella politica di difesa comune e di contrasto delle minacce agli interessi essenziali degli Stati membri e dell'Unione. Si dovranno valutare i requisiti operativi in materia e si dovrà dare sviluppo alle capacità di organizzazione e risposta "nella gestione dinamica del rischio".

Naturalmente, ogni Stato membro dovrà designare, in base alla direttiva *Network and Information Security* (NIS), un'autorità, un punto di contatto nazionale unico al fine di coordinare nell'Unione le questioni concernenti la sicurezza delle reti e dei sistemi informativi.

Le parole d'ordine sono prevenzione, mitigazione, risposta e scambio di informazioni e assistenza reciproca.

Un attore di prima grandezza appare sulla scena europea dotato di poteri d'impulso e di coordinamento, destinato ad assumere un ruolo propositivo anche sul piano dell'intervento operativo: l'Agenzia europea per la sicurezza delle reti e dell'informazione (ENISA)[1].

Questo Ente dovrà analizzare strategie in materia di sicurezza della rete, articolando con precisione linee guida nella reazione agli incidenti ipotizzabili nei molteplici settori economici, delle infrastrutture critiche e istituzionali, predisporre esercitazioni europee dei piani di emergenza e ripristino in caso di disastro, agevolare lo scambio di informazioni e di migliori prassi.

Il modello organizzativo italiano

L'intero assetto delle misure indicate dal "Legislatore europeo" è stato recepito e sviluppato nel provvedimento normativo nazionale[2], in aderenza alle risorse umane, esperienziali e tecnologiche già esistenti nel tessuto istituzionale italiano.

Il primo risultato evidente è l'annunciato potenziamento delle capacità nazionali prioritariamente in termini di risorse finanziarie e umane.

La dimensione della sicurezza *cyber* del sistema Paese (pubblico e privato), segue la logica di un primo decentramento di competenze ministeriali che convergono immediatamente in una regia unitaria, centrata sugli organismi della Presidenza del Consiglio.

Sono designati l'autorità competente NIS in materia di sicurezza delle reti e dei sistemi informativi e il Dipartimento delle informazioni per la sicurezza (DIS) quale "punto di contatto unico" al quale è demandata la competenza nel coordinamento in materia e nella cooperazione transfrontaliera nell'ambito dell'Unione.

La strategia nazionale di sicurezza cibernetica è adottata dal Presidente del Consiglio, sentito il Comitato interministeriale per la sicurezza della Repubblica.

I comparti ministeriali dello sviluppo economico, delle infrastrutture e dei trasporti, dell'economia e delle finanze, della salute, della tutela dell'ambiente e della tutela del territorio e del mare divengono attori istituzionali assolutamente protagonisti nell'ambito delle competenze ora attribuite.

In questa prospettiva unitaria, è istituito presso la Presidenza del Consiglio il *Compart Security Incident Respons Team* (CSIRT) italiano, con le competenze e le funzioni del *Computer Emergency Response Team* (CERT) nazionale, gruppo di intervento per la sicurezza in caso di "incidenti informatici", preposto anche alla definizione delle procedure per la prevenzione e la gestione degli stessi.

Cooperazione e scambio di informazioni rappresentano un binomio indispensabile per assicurare tempestività ed efficacia nella reazione alle gravi perturbazioni del funzionamento della rete, in un'ottica di assistenza reciproca. In questa prospettiva operativa, il DIS partecipa alle attività del gruppo di cooperazione composto da rappresentanti degli Stati membri, della Commissione europea e dell'Agenzia della UE per la sicurezza delle reti e dell'informazione (ENISA).

La determinazione dell'importanza dell'impatto di un incidente sulla continuità dell'erogazione dei servizi informatici è legata a indicatori concreti: numero degli utenti interessati dalla compromissione, durata del disservizio e l'estensione geografica. Tali eventi devono essere notificati dagli "operatori di servizi essenziali" (ad esempio, dall'energia elettrica ai trasporti) e dai "fornitori di servizi digitali" (a titolo esemplificativo, gli operatori commerciali del settore) al CERT nazionale che a sua volta informa i livelli sovraordinati, con un meccanismo di valutazione e inoltro delle informazioni ritenute rilevanti, consentendo l'adozione delle dovute cautele decisionali e di pronta reazione a tutti i livelli interessati, entro i confini nazionali ed europei.

La legge nazionale sul perimetro di sicurezza nazionale cibernetica

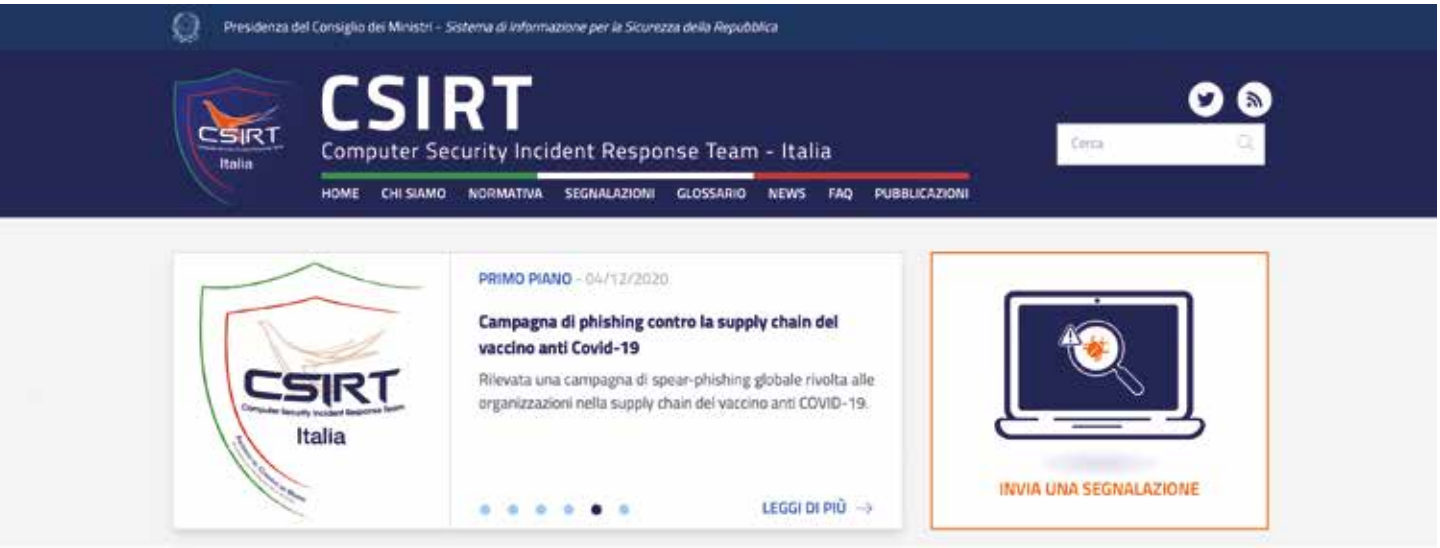
Il provvedimento legislativo nazionale è la risultante di un intenso dibattito e confronto parlamentare tra tutte le forze politiche, interessate nel fornire le proprie puntuali chiavi interpretative in merito alle esigenze di sicurezza. Vi è stata una rara quanto piena convergenza di intenti nei confronti di uno spettro di minacce concordemente avvertito in tutti i settori della vita civile ed economica, oltre che nella difesa e sicurezza[3].

La recente casistica di incidenti o di aggressioni cibernetiche risulta essere ampia ed eloquente, in tal senso, nel 2017 un grande impianto petrolchimico in Arabia Saudita ha rischiato di esplodere a seguito di una intromissione occulta nei sistemi informatici di

1 *Direttiva (UE) 2016/148 del Parlamento Europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione.*

2 *Decreto legislativo 18 maggio 2018, n. 65, concernente l'attuazione della direttiva (UE) 2016/148 del Parlamento Europeo e del Consiglio, del 6 luglio 2016.*

3 *Legge 18 novembre 2019 n. 133, conversione in legge, con modificazioni, del decreto legge 21 settembre 2019, n. 105, recante disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica e di disciplina dei poteri speciali nei settori di rilevanza strategica.*



sito istituzionale: https://csirt.gov.it

controllo della produzione industriale, mentre la rete digitale interna di numerosi ospedali in Gran Bretagna è stata paralizzata come molti dei servizi ospedalieri erogati. Le nuove tecnologie hanno reso possibile livelli qualitativi e quantitativi delle prestazioni inimmaginabili fino a un paio di decenni fa ma, contestualmente, l'interconnessione dei sistemi informatici e meccanici ha reso alquanto vulnerabile la certezza della loro affidabilità. L'assoluta necessità di un comune orizzonte d'azione in Europa, in tutti i momenti della progettazione, produzione e messa a sistema di ogni componente o servizio informatico deriva anche dal fatto che nell'Unione i confini e la concreta estensione dei settori pubblico e privato sono declinati dai singoli Stati in maniera estremamente eterogenea.

Liberalizzazione e privatizzazione rappresentano un binomio cangiante in relazione agli ordinamenti nazionali. Alcune infrastrutture critiche e un certo numero di servizi sono quindi gestiti da operatori privati in alcuni Stati membri e da enti pubblici in altri.

Inoltre, un'ulteriore conseguenza è rappresentata dalle scelte infrastrutturali adottate da soggetti pubblici o privati, inevitabilmente con differenti parametri decisionali e di investimento internazionale, con obiettivi di natura istituzionale i primi, commerciale i secondi. A mero titolo esemplificativo citiamo le politiche infrastrutturali: fibra ottica o costellazioni di satelliti dedicate e *dual use*, militare e civile?

Tali asimmetrie e il velocissimo progredire dello sviluppo tecnologico del settore ICT (Tecnologia dell'Informazione e Telecomunicazione) e satellitare, ad esso sempre più connesso, impone all'Unione l'adozione di misure uniformi, cogenti e messe a sistema in tutti gli Stati membri, tenuti a un'attenta e vigile cooperazione transnazionale nel monitoraggio, nella prevenzione e nella reazione a fenomeni che, se pur nominalmente interni, possono assumere proporzioni continentali.

In questo senso, le prospettive geopolitiche e, dunque, il confronto commerciale tra i colossi multinazionali statunitensi e gli enormi operatori industriali cinesi appaiono determinanti. Le tecnologie di base e le logiche di sistema sono diverse come gli obiettivi nella progettazione e produzione industriale, connessi anche alla protezione dei dati personali o esclusivamente alla sicurezza nazionale e agli interessi delle agenzie di informazione, ad esempio, nei *social media* come nei servizi bancari e postali o del trasporto aereo.

È stato necessario superare l'eterogeneità esistente nell'Unione nella definizione delle regole e delle misure adottate da ogni singolo Stato membro. La carenza di uniformità nella previsione di comuni doveri stabiliti per gli operatori di servizi essenziali e per i fornitori di servizi digitali rende irrealizzabile la creazione di un "meccanismo globale ed efficace di cooperazione" nell'ambito della UE. Livelli adeguati nelle capacità tecniche, organizzative e operative nonché approcci metodologici condivisi degli operatori europei rappresentano l'unica risposta efficace alle minacce provenienti soprattutto dall'esterno dei confini del vecchio continente.

Le norme d'urgenza e ordinarie emanate in sede nazionale

Il legislatore italiano ha proceduto a configurare uno strumento normativo articolato e puntuale nelle previsioni, spesso di natura organizzativa.

In tale maniera, è prevista la successiva emanazione di alcuni provvedimenti di attuazione dei meccanismi procedurali nella notifica degli eventi informatici verso il vertice, costituito dalla Presidenza del Consiglio dei Ministri.

I soggetti pubblici e privati (individuati in appositi elenchi da formare rapidamente) che intendano procedere all'affidamento di forniture di tecnologie ICT devono darne comunicazione preventiva al Centro di valutazione e certificazione nazionale (CVCN), istituito presso il Ministero dello sviluppo economico. Il parere di tale centro è vincolante sulle componenti sia hardware sia software e, quest'ultimo, può effettuare verifiche preliminari e imporre condizioni sulle tecnologie e apparati di settore.

Alla Presidenza del Consiglio sono demandate attività ispettive e di verifica del rispetto delle procedure e dei requisiti industriali e operativi stabiliti.

La Presidenza esercita poteri speciali, il cosiddetto *golden power*, in particolare, sulle acquisizioni della Pubblica Amministrazione. Si stabilisce un regime particolare in materia di contratti di forniture informatiche, sia di beni sia di servizi. "*Costituiscono attività di rilevanza strategica per il sistema di difesa e sicurezza nazionale i servizi di comunicazione elettronica a banda larga basati sulla tecnologia 5G*"[4].

In questo modo, vi è un'estensione dei poteri speciali di veto esercitabili dalle autorità governative nei settori ad alta intensità tecnologica. Si prevede l'obbligo di notifica per gli acquisti, da parte di soggetti esterni alla UE, di partecipazioni in società detentrici di beni e relazioni di settore, comprese le infrastrutture critiche connesse alla gestione delle masse di dati nonché flussi finanziari.

Conclusioni

È stato messo a punto uno strumento normativo frutto delle nuove riflessioni sulla evoluzione della minaccia *cyber*. Il perimetro di sicurezza cibernetica nazionale si rivela dunque di fondamentale importanza per ogni singolo Stato, a partire dal personale specializzato e dalle strutture organizzative dedicate. Infatti, uno dei cardini del sistema è rappresentato dall'impiego di giovani generazioni di tecnici informatici. Siamo solo all'inizio di un lungo percorso.

In questo scenario di intenso rinnovamento, si inserisce la recente costituzione del Comando per le Operazioni in Rete (CORDIFESA).

Il comparto della Difesa ha un ruolo fondamentale ed è in prima linea in questa prospettiva istituzionale di sviluppo e consolidamento delle capacità *cyber* e della formazione e crescita professionale delle risorse umane da impiegare in tale nuovo "dominio", che mette a disposizione del Sistema Paese Italia.

4 *Misure speciali disposte mediante decretazione d'urgenza, art.1 del decreto legge 25 marzo 2019, n.22 convertito nella legge 20 maggio 2019, n.41.*

(*) Umberto MONTUORO, *Ten. Col. commissario AM è l'Ufficiale Superiore Addetto al Procuratore Generale Militare della Repubblica presso la Corte Suprema di Cassazione; Segretario nazionale della International Society for Military Law and the Law of War; docente incaricato di Politica Estera e di Sicurezza Comune, presso l'Istituto di Studi Europei, "Alcide De Gasperi".*

PICOSATS: SPIN-OFF SPAZIALE

Specializzati nella progettazione di sistemi di telecomunicazione per piccoli satelliti

Fondata nel 2014 e insediata in AREA Science Park, il più grande parco scientifico e tecnologico in Italia e uno dei maggiori in Europa, PICOSATS è una PMI innovativa, spin off dell'Università degli Studi di Trieste, che si è posta come obiettivo primario quello di rendere più rapido ed economico l'accesso allo spazio.

Per PICOSATS la parola chiave è innovazione a cui diamo molteplici significati. Sicuramente identifica che i nostri prodotti sono il risultato di un importante lavoro di ricerca e sviluppo, in collaborazione con l'Agenzia Spaziale Italiana e con quella Europea, ma per noi un obiettivo fondamentale è migliorare la nostra società, quella italiana ma anche mondiale dal momento che lo Spazio è per definizione globale. Ulteriore elemento chiave è l'etica aziendale in quanto crediamo che questo sia un requisito fondamentale per un'azienda solida, sana e moderna.

La società attuale necessita di un mondo interconnesso, in questo periodo di emergenza le comunicazioni risultano ancora più cruciali, e le risorse derivanti dallo spazio possono essere utilizzate come mezzo per migliorare la vita della comunità, anche in modo sostenibile.

La nuova frontiera dello Spazio sono i piccoli satelliti, punto di partenza per PICOSATS è il settore delle telecomunicazioni in quest'ambito. PICOSATS lavora nel campo dei CubeSat: piccoli satelliti standard e modulari, il cui elemento base "1U" è un cubo di 10 cm di lato e 1 kg circa di massa, che possono arrivare fino a 50 kg di massa per sistemi a 27 unità, "27U". Proprio la modularità e la standardizzazione sono due caratteristiche fondamentali di questi sistemi perché permettono di ridurre drasticamente i tempi e i costi di sviluppo rispetto a sistemi satellitari tradizionali.

Attualmente PICOSATS lavora ad un nuovo sistema di telecomunicazioni che renda possibile la trasmissione dati ad alta velocità: RADIOSAT, un ricetrasmettitore miniaturizzato ad alte frequenze (in banda Ka) progettato per CubeSat e in generale per piccoli satelliti con il supporto dell'Agenzia Spaziale Europea. Di ridotta massa e volume (1,5 kg e 3U), RADIOSAT è integrato con un modem, il tutto caratterizzato da un basso consumo energetico. Inoltre, l'uso di questa banda di frequenza garantisce una velocità di trasferimento dati cinque volte superiore rispetto alle altre tecnologie presenti nel mercato nel campo dei piccoli satelliti. I segnali vengono elaborati dal modem che fornisce funzionalità di codifica e modulazione variabili e adattive. PICOSATS, a differenza dei pochi concorrenti presenti nel mercato internazionale, sta sviluppando una soluzione, unica e all'avanguardia, che consente la gestione separata del ricevitore e del trasmettitore. Un altro prodotto a cui sta lavorando l'azienda, BEAMSAT, è un'antenna a tromba da accoppiare alla radio al fine di realizzare un sistema di telecomunicazione efficiente e completo.

I punti di forza dell'azienda sono la profonda conoscenza del settore spaziale, della community e dei suoi attori, la consolidata esperienza nel campo delle telecomunicazioni, nonché nella gestione di missioni spaziali internazionali, grazie alla sua General Director Anna Gregorio e dei suoi soci (che comprendono alcuni ex dipendenti, dal 2019 ammessi alla compagine sociale) per rispondere alle sfide della New Space Economy. Inoltre, la presenza in azienda di persone con background e competenze diverse ha favorito e favorisce lo sviluppo di nuove idee e progetti, come ad esempio Quantum Ship, uno studio di fattibilità in collaborazione con l'Agenzia Spaziale Europea riguardante un collegamento di comunicazione quantistico, e quindi protetto, per la navigazione marittima autonoma.

PICOSATS ha collezionato premi e finanziamenti ottenendo, nel 2017 un contratto dall'Agenzia Spaziale Europea per sviluppare RADIOSAT, un Italian Masters Startup Award nel 2018, l'Unicredit Launch Pad nord-est nel 2019 e il Seal of Excellence dalla Commissione Europea nel 2020. In aprile 2020 Anna Gregorio è stata nominata da Forbes Italia fra le "100 donne italiane vincenti" e a settembre fra le 15 donne italiane di successo più influenti nell'innovazione da Digitalic "Digiwomen2020".

Per quanto riguarda i passi futuri, i primi test di RADIOSAT si sono appena conclusi con successo, ora PICOSATS punta al lancio per la dimostrazione in orbita sulla Stazione Spaziale Internazionale del suo primo rice-trasmettitore nel 2021 e ad acquisire i primi contratti entro la fine di quest'anno.

PICOSATS
SPACE TECHNOLOGIES SOLUTIONS