MOZIONE

Posti di lavoro nuovi e innovativi portando in Ticino il Centro di competenza federale di sicurezza cibernetica

del 5 novembre 2018

«*Con la finalità concreta di portare in Ticino nuove competenze federali, nuove conoscenze tecniche e nuovi posti di lavoro, nuove sinergie con enti pubblici e privati presenti sul territorio cantonale, con la mozione, il gruppo PPD+GG chiede che il Cantone Ticino si adoperi per portare nel nostro Cantone delle competenze federali (organo/autorità federale) nell'ambito della sicurezza cibernetica collegato alle facoltà di scienze informatiche/ingegneria informatica di USI e SUPSI. Il Consiglio federale ha recentemente pubblicato la strategia nazionale per la protezione della Svizzera contro i rischi cibernetici (SNPC) e tra le varie misure da mettere in atto è in procinto di decidere sulla futura creazione del centro di competenza di sicurezza cibernetica. Il Ticino - se lo vorrà - potrà cogliere questa opportunità di incrementare le proprie competenze tecniche in un ambito strategico a livello nazionale. La tecnologia fa parte della nostra vita quotidiana e siamo costantemente circondati da oggetti interconnessi ed interattivi. Nonostante ciò non siamo pronti ad affrontare i rischi del mondo cibernetico. Infatti, se fino a poco tempo fa si reputava che un attacco informatico potesse arrecare solo danni informatici, l'attualità ci conferma che un attacco cibernetico può avere anche conseguenze cinetiche, ovvero danni materiali a persone e cose*».

INTRODUZIONE

Negli scorsi mesi la deputata Sara Beretta Piccoli (PPD+GG) si è attivata chiedendo al Governo cantonale di adattare le normative riguardanti il cyberspazio al fine di combattere vari crimini cibernetici, tra cui i furti di identità, lo stalking e il grooming e di creare un Corpo di polizia formato e preposto alla lotta contro questi crimini. Il Governo e il Parlamento hanno risposto picche spiegando che fondamentalmente all'interno del Corpo della Polizia cantonale esiste già un gruppo specializzato e preposto alla lotta contro i crimini informatici.

La mozione "Posti di lavoro nuovi e innovativi portando in Ticino il centro di competenza federale della sicurezza cibernetica" va oltre e chiede di rafforzare le competenze cantonali in ambito di sicurezza cibernetica accogliendo in Ticino delle competenze federali oggi in fase di definizione a livello nazionale. Infatti, se è vero che sono numerosi gli atti parlamentari federali che vertono attorno al tema della sicurezza cibernetica, è altrettanto vero che in questa fase anche il Ticino potrà – se lo vorrà – ritagliarsi uno spazio.

LA SICUREZZA CIBERNETICA

La tecnologia fa parte della nostra vita quotidiana e siamo costantemente circondati da oggetti interconnessi ed interattivi. Questo "nuovo mondo", fatto di reti, antenne, computer, telefoni, applicazioni, basi dati e oggetti intelligenti a vari livelli costituisce quello che ora viene definito "Cyber Spazio". Ed è proprio in questo contesto che dobbiamo intervenire per minimizzare la "minaccia cyber": come nel mondo reale anche nel mondo virtuale vi sono persone che agiscono con finalità malevoli e criminali. La struttura aperta del sistema Internet è vulnerabile ad attacchi che possono avere origine: criminale (cyber crime), terroristica (cyber terrorism), attività di spionaggio (cyber espionage) o, addirittura, dar vita ad una cyber war, cioè un vero e proprio conflitto tra nazioni combattuto attraverso la paralisi di tutti i gangli vitali per le attività sociali dei reciproci contendenti. A differenza del

mondo reale, il mondo virtuale non è pronto a combattere queste minacce che toccano persone fisiche, aziende private, istituzioni private e pubbliche nonché l'amministrazione pubblica. **Attualmente sebbene vi sia un monitoraggio e una maggiore consapevolezza di questa tipologia di attacchi, manca un'autorità definita e competente nell'ambito della sicurezza cibernetica seppur attualmente in fase di definizione a livello federale.**

Wannacry e Petya sono denominazioni di due recenti attacchi cibernetici noti a livello internazionale molti altri attacchi meno noti sono sistematicamente in atto – e hanno mostrato come la privacy di ogni cittadino è messa in continuo pericolo da potenziali scorribande all'interno dei database di banche, aziende pubbliche sistemi sanitari e leggiamo questi eventi sempre con una certo senso di distacco – "accadono a qualcun altro di solito" – **ma cosa succede quando diventiamo noi stessi uno specifico target?**

Se l'attacco alla persona potrebbe essere considerato un affare personale legato all'individuo - quesito degno di approfondimento - non si può dire altrettanto degli attacchi ad aziende private, para-statali e enti pubblici che sempre di più sono oggetto di attacchi, non più "dimostrativi", ma di azioni reali con rischi rilevanti: intrusioni nella rete wifi pubblica (comunale o cantonale) con accesso a dati sensibili, vittime di spionaggio industriale con conseguenze finanziarie gravi, manipolazione di informazioni confidenziali del contribuente in ambito fiscale, modifica del sito web dell'ente attaccato con danni concreti nei confronti degli utenti, ecc. Nel momento in cui più enti privati e pubblici di un certo rilievo sono sotto attacco e sotto l'attenzione di entità esterne il problema non coinvolge più solo la singola azienda, ma dovrebbe essere considerato un **problema generale di sicurezza cantonale e nazionale.**

Infatti, se fino a poco tempo fa si reputava che un attacco informatico potesse arrecare solo danni informatici, **l'attualità ci conferma che un attacco cyber può avere conseguenze cinetiche, ovvero danni materiali a persone e cose**. Proviamo ad esempio ad immaginare i danni causati dalla eventuale manomissione del sistema di controllo dell'altezza dell'acqua in una diga, o se tutti i semafori e gli scambi di un importante nodo ferroviario venissero hackerati o ancora, se il sistema di dosaggio del disinfettante di un acquedotto venisse compromesso.

La minaccia cyber evolve con la stessa rapidità con cui evolvono le tecnologie. È evidente a tutti che le regole di difesa tradizionali, ovvero contrastare un attacco, non sono più praticabili con efficacia nel contesto attuale.

IL CONTESTO NAZIONALE

A livello federale lo scorso mese di novembre il procuratore generale Lauber ha affermato con convinzione la necessità di creare un centro di competenze federale di lotta alla cybercriminalità. Numerosi atti parlamentari ed interventi pubblici hanno evidenziato la necessità di intervenire in questo ambito. In questo senso a livello nazionale, nel corso del 2018 il Consiglio federale ha pubblicato la strategia nazionale per la protezione della Svizzera contro i rischi cibernetici (SNPC) al fine di combattere attivamente i cyber-rischi e adottare le misure necessarie per preservare la sicurezza della Svizzera contro le minacce provenienti dal cyberspazio. Più recentemente, lo scorso 4 luglio 2018, il Consiglio federale ha adottato le prime decisioni di principio in ambito di prevenzione e lotta ai cyber-rischi, conferendo diversi mandati in vista della creazione di un apposito centro di competenza ed ha stabilito che la decisione finale sulla creazione del centro avrà luogo entro la fine del 2018.

Il Ticino sembrerebbe lontano da queste logiche ma in realtà può vantare numerose competenze specifiche che permetterebbero al nostro Cantone di ritagliarsi uno spazio importante nella protezione cibernetica della Svizzera.

Basti pensare al **Laboratorio di informatica forense del Dipartimento tecnologie innovative della SUPSI**, condotto dal Dr. Alessandro Trivilini. Il Dr. Trivilini funge anche da

rappresentante della Svizzera in seno al comitato di gestione dell'azione COST "Multi-modal imaging of forensic science evidence – tools for forensic science", del programma intergovernativo di cooperazione europea nella ricerca scientifica e tecnologica.

Si pensi anche all'**Istituto Dalle Molle di studi sull'intelligenza artificiale**, diretto da Luca Gambardella e Jürgen Schmidhuber. Si tratta di un istituto di ricerca non profit, affiliato sia con l'Università della Svizzera italiana di Lugano che con la Scuola universitaria professionale della Svizzera italiana. Le attività di ricerca dell'Istituto Dalle Molle si concentrano su apprendimento automatico, intelligenza artificiale universale ottimale, agenti razionali ottimali, ricerca operativa, teoria della complessità, informatica ambientale e supporto alle decisioni, sistemi bio-ispirati e sistemi di robotica.

Non da ultimo, è importante menzionare anche il **Centro svizzero di calcolo scientifico**, un'unità autonoma dell'Istituto Federale Svizzero di Tecnologia di Zurigo (ETH Zurigo) che collabora strettamente con l'Università della Svizzera italiana (USI). Il CSCS già oggi fornisce risorse di calcolo dedicate a specifici progetti di ricerca e mandati nazionali, come nel caso delle previsioni del tempo.

LA PROPOSTA

Per farla breve, in Ticino negli ultimi anni non solo si è sviluppata la facoltà di scienze informatiche (USI) che nell'ambito della sicurezza cibernetica beneficerebbe anche delle competenze legate alla facoltà di comunicazione e di economia, ma ha trovato spazio anche la SUPSI con il Laboratorio di informatica forense e l'istituto Dalle Molle di studi sull'intelligenza artificiale, senza dimenticare **vari enti parastatali e aziende private che potrebbero certamente contribuire alla creazione di un centro di competenze di interesse nazionale ed internazionale.**

Concretamente, più nello specifico, il Gruppo PPD+GG, facendo uso delle facoltà previste dall'art. 101 della Legge sul Gran Consiglio e sui rapporti con il Consiglio di Stato, chiede con la presente mozione, alla luce delle indicazioni e considerazioni espresse in precedenza, che:

- venga preso contatto con l'autorità federale per dare la disponibilità ad accogliere in Ticino un centro di competenze federale nell'ambito della sicurezza cibernetica collegato alla facoltà di scienze informatiche e di comunicazione che si occupi:

    1. di incrementare sinergie strategiche locali in forma public-private-partnership, con lo scopo di contenere i costi generati dalla lotta al crimine informatico, in forma interdisciplinare, con il supporto di ricercatori scientifici di SUPSI e USI, e di rafforzare l'impatto e la condivisione di buone pratiche per meglio mettere in sicurezza i dati e le infrastrutture critiche;

    2. di coordinare con l'autorità federale gli interventi di difesa;

    3. di attuare azioni periodiche di esercitazione contro attacchi cyber;

    4. di promuovere gli interventi di sensibilizzazione a partire dalle famiglie e dalle scuole, per passare dai contesti lavorativi pubblici e privati fino ai massimi livelli aziendali ed istituzionali.

Marco Passalia
Per il Gruppo PPD+GG