SICUREZZA ONLINE

L'INTERVISTA **EUGENIO SANTAGATA**

«Per blindare il nostro cyber spazio ora serve un'industria nazionale»

Cy4Gate del gruppo Elettronica chiude un accordo con la Nato. L'ad fa il punto delle attività militari Per quelle civili «serve più collaborazione tra privato e pubblico e più software made in Italy»

di **CLAUDIO ANTONELLI**

Cy4Gate, joint venture tra Elettronica ed Expert system, ha siglato la scorsa settimana un accordo di partnership con la Nato per la condivisione di informazioni riguardanti le minacce cibernetiche. Il patto è stato firmato con l'Ncia, l'Agenzia di comunicazione e informazione dell'Alleanza Atlantica responsabile anche della gestione e della difesa delle reti, con il proposito di agevolare e velocizzare lo scambio di informazioni tecniche non classificate relative a minacce e vulnerabilità cyber.

La partnership fa parte di una più ampia strategia promossa da per contribuire al miglioramento della resilienza delle reti informatiche e potenziarne le capacità di prevenzione, contrasto e recupero dagli attacchi. Tenendo presente che la maggior parte delle reti informatiche è posseduta e gestita da società private.

L'accordo anticipa di qualche giorno la conferenza conferenza annuale Internazionale sui Conflitti Cibernetici, organizzata dal Nato cooperative cyber defence dentre of excellence che si svolgerà a Tallinn a partire da oggi e che unisce le competenze dei 600 principali decision makers ed esperti governativi, militari e dell'industria in materia di guerra cibernetica. «Con la firma di questo nuovo accordo», spiega alla *Verità* l'amministratore delegato di Cy4Gate, Eugenio Santagata, «la società conferma il suo forte impegno con la comunità Cyber della Nato nella lotta contro le minacce informatiche e la partecipazione al Cycon conferma la direzione che ci interessa prendere».

Siete tra i principali sponsor insieme a Microsoft dell'evento e parlerete appena dopo Google e prima di Harvard, con la differenza che siete nati da pochi anni. Quale è la vostra peculiarità?

«Le due anime della nostra azienda uniscono lo spettro elettromagnetico e l'intelligenza semantica in area digitale. L'evento di Tallin, alla sua decima edizione, racconta proprio questa convergenza. Questo è il motivo della nostra presenza. Operiamo in maniera sistematica in ambito della cyber electronic warfare, cyber intelligence e cyber security offrendo un'ampia gamma di soluzioni alle agenzie di intelligence, alle organizzazioni governative della sicurezza (militari e non) e alle aziende, compreso le capacità di analisi della vulnerabilità».

Lo scorso maggio il governo Gentiloni ha varato il piano nazionale per la cyber security, lo vede come un passo avanti anche per la componente privata del comparto?

«Il Piano contiene grandi innovazioni per la componente convenzionale relativa a tutte le infrastrutture critiche. La parte non convenzionale, ovvero quella difensiva, meriterebbe ulteriori sviluppi. Per innovare veramente in questo campo bisogna essere relativamente piccoli e avere linee guida precise. Per quanto riguarda la filiera militare i paletti sono adesso precisi, ben delineati e decisamente innovativi. A oggi il numero di aziende che sviluppano prodotti (e non si limitano a vendere servizi) non supera le dieci unità. Significa che non è ancora sviluppato una industria Cyber nazionale. A differenza di Paesi come la Francia o l'Australia».

Quali sono i rischi di un know how prodotto all'estero?

««Francia e Usa hanno capito perfettamente che senza un perimetro nazionale di sviluppo dei software non si avrà mai la garanzia di blindare al 100% il perimetro. D'altronde la proprietà intellettuale è la vera certezza di sicurezza».

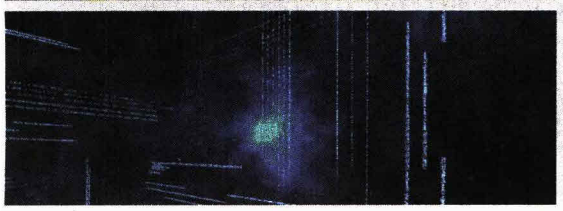
Se il governo vede una vulnerabilità nel comparto privato deve intervenire in anticipo? e questo può aiutare lo sviluppo nell'industria nazionale?

«Il pubblico non sa se le aziende private non comunicano. Per crescere bisogna certamente avere una agenda cyber ben definita che aiuti anche il comparto privato. Dal punto di vista degli investimenti, ma anche dello scambio di informazioni utili».

I rischi cyber sono sufficientemente percepiti in Italia?

«La consapevolezza della portata della minaccia cyber non è percepita appieno. Le contromisure che altri Paesi hanno messo in pista da tempo, sembrano più efficaci. Come detto sopra, negli Stati Uniti la selezione e la formazione di talenti cyber coinvolge giovani cittadini fin dall'adolescenza. A Beersheva, una città in Israele, è stato creato un cyber security center. Ecosistema ideale dove multinazionali si confrontano con start up locali e centri di formazione universitaria. E presto anche con le unità specializzate nello spionaggio e nel cyberwarfare».

IL GRUPPO



CY4GATE

Startup 100% italiana specializzata in cyber security & intelligence

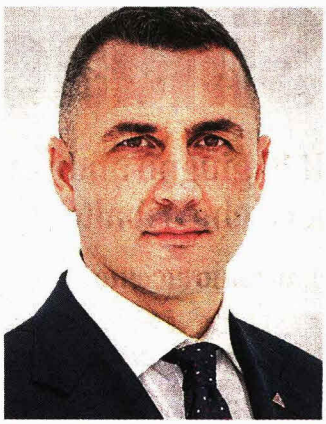
Nasce da una joint venture tra la romana **Elettronica**, società di ingegneria high-tech leader a livello internazionale nel campo della electronic warfare, ed **Expert system**, azienda modenese di software leader nel settore del cognitive computing e text analytic

Fa parte di Elettronica group

ELETTRONICA GROUP
A FOCUSED GLOBAL LEADER

Si occupa di guerra elettronica, guerra informatica, formazione e intelligence

LaVerità



MANAGER Eugenio Santagata