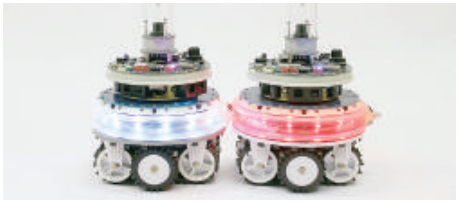
TUTTOSCIENZE
MERCOLEDÌ 20 SETTEMBRE 2017
NUMERO 1760

A CURA DI:
GABRIELE BECCARIA
REDAZIONE:
CLAUDIA FERRERO
www.lastampa.it/tuttoscienze/

RICERCA DI UN ITALIANO IN BELGIO

Ecco i mini-robot mutanti che assumono qualsiasi forma

Robot con sistema nervoso e cervello, ma senza una forma né una funzione particolare e capaci di unirsi per prendere qualsiasi aspetto e fare qualsiasi cosa: è la strada aperta dal test dell'Università libera del Belgio, coordinato dall'italiano Marco Dorigo, e descritto su «Nature Communications». I ricercatori hanno realizzato mini-unità modulari in grado di auto-assemblarsi e assumere qualsiasi «look», pur conservando un pieno controllo sensomotorio. «Quando due robot si uniscono - dice Dorigo - uno cede il controllo all'altro»: così, mentre cresce, la creatura decide in autonomia la forma e le dimensioni migliori per il compito da svolgere.



tutto SCIENZE & salute

L'acqua val bene una cyberguerra

A Tel Aviv un summit di matematici, imprenditori e specialisti di intelligence: "Ecco come difenderemo l'oro blu"

GABRIELE BECCARIA
INVIATO A TEL AVIV

Oren Segev è un matematico e gli algoritmi lo accompagnano da sempre. Quando era ufficiale dell'esercito israeliano e anche adesso, ricercatore per la società high-tech IoSight. Qui l'oggetto dei suoi studi teorici e delle sue applicazioni è la realtà più universale che c'è, apparentemente banale eppure straordinariamente complessa: l'acqua.

Gli algoritmi sono i gangli nervosi di una serie di sensori che la IoSight ha installato lungo il fiume Giordano, una delle fonti idriche di Israele. E quella intelligenza offre qualcosa che - spiegata con pazienza da Segev - spalanca un modo di sorprese, tra opportunità inattese e impensabili terrori. «Si tratta di nuove soluzioni per affrontare nuove sfide», sintetizza in forma di slogan, evocando subito dopo il paziente lavoro per educare i software a leggere e interpretare l'«oro blu», a partire dal Big Data, gonfio di masse di dati in evoluzione, fino al «machine learning», il processo cognitivo che dà forma all'Intelligenza Artificiale.

Il problema è ancora al di là del senso comune, ma - sottolinea Segev - l'acqua è uno degli obiettivi del cuore di tenebra che incombe sulle società ipertecnologiche: la cyberguerra. È lì che dimensione fisica e dimensione virtuale si scontrano, generando le prossime emergenze. Che cosa accadrebbe se i sistemi computerizzati di una diga o di un acquedotto finissero sotto attacco informatico e un hacker - in forma di lupo solitario o con le sembianze di un gruppo cybercriminale o cyberterrositico - mandasse tutto in tilt? Potrebbe contaminare ogni goccia che scende dai rubinetti di milioni di abitazioni o bloccarle, seminando un panico difficilmente controllabile. Sembra un'opzione fantahorror, da aggiungere alle troppe ansie che ci attanagliano, ma non è affatto così.

Ecco perché Segev è al lavoro e si racconta volentieri: se l'identità del nemico resta avvolta in una nube che ne confonde le sembianze, l'allarme è chiaro nei suoi mutevoli aspetti, nella vita civile e nelle attività industriali. «I sensori identificano velocità e qualità dei flussi del fiume, li valutano secondo una scala da 1 a 10, e poi elaborano i rapporti in tempo reale - spiega -. Online e in laboratorio». Così Mekorot - la società numero 1 in Israele per le forniture idriche - può disporre delle informazioni con cui parare subito il colpo. In caso di blitz che dai malware - i software «cattivi» - si diffondono nelle profondità del Giordano scattano quindi le contromisure. Il più rapidamente possibile e, almeno al momento, le più efficaci. «Ingegneria e matematica - aggiunge con orgoglio - si combinano».

È una coppia solida che fa il paio con un'altra e che il chairman di IoSight, Yoav Navon, esemplifica così: «Sicurezza e business». E non è un caso che l'intreccio di elementi eterogenei come acqua, cyberguerra e start-up siano diventati protagonisti dell'evento «Watec 2017» di Tel Aviv: qui, in una delle capitali mondiali dell'innovazione, si è dato appuntamento, dal 12 al 14 settembre, il meglio dell'high tech dell'acqua. Ricercatori e accademici, aziende e investitori, «venture capitalists» accanto a specialisti e amministratori (quelli che amano definirsi «decision makers»), hanno messo insieme idee e competenze, oltre che prodotti, per espandere il raggio d'azione di un settore cruciale: nel XXI secolo l'acqua sarà ancora più essenziale di ciò che è stato il petrolio nel XX. Una linfa da utilizzare senza abbandonarsi agli eccessi dell'oro nero, ma con le logiche eco e bio che innervano oggi le strategie globali.

A esserne convinto è anche Yair Cohen. Ex comandante dell'Unità 8200, il corpo d'élite dell'esercito israeliano specializzato in intelligence e - non potrebbe essere altrimenti, vista la vocazione visionaria - negli inediti scenari della cyberguerra, accenna alla natura ibrida di molti compagni d'armi. Matematici e «computer scientists», prima di tutto, stanno creando un numero crescente di aziende avanzate. «L'85% dei "tech people" - le super-menti - proviene dalla nostra unità», dice Cohen e cita l'icona di questo trend: è Elbit, gigante del settore. Se la cybersicurezza è il cuore delle nuove attività, dalle consulenze ai prodotti, le infrastrutture sono uno dei punti nodali da proteggere. E quelle legate all'acqua salgono in primo piano. «Come accade con i trasporti e l'energia si tratta di sistemi ad alta criticità. Perlopiù funzionano con protocolli superati, degli Anni 60, e rappresentano perciò un obiettivo attraente per i cybercriminali».

Tra difesa e attacco si estende un vasto fossato, con i terroristi in vantaggio. Molto dev'essere fatto, osserva Cohen, inventando forme inedite di spionaggio e protezione, sia dei software sia delle macchine. «Barack Obama ideò un "ordine" sulla cybersecurity, enfatizzandone l'importanza per la sicurezza nazionale, e tuttavia il ruolo dei governi resta poco definito». E intanto non c'è Paese che possa dirsi al sicuro (il blitz contro l'Ucraina è solo il caso più eclatante), «mentre i civili diventano il bersaglio principale». D'ora in poi, ogni volta che apriremo il rubinetto, l'acqua ci stupirà con le sue metamorfosi, in cui miracoli di sostenibilità e minacce terroristiche si specchiano senza sosta.

1 - Continua

BY NC ND ALCUNI DIRITTI RISERVATI

Scenari

Tra le start-up che inventano la sicurezza del XXI secolo

FABIANA MAGRÌ
TEL AVIV

Dagli acquedotti alle industrie alimentari e farmaceutiche, dai pozzi petroliferi alle centrali nucleari, i sistemi OT di infrastrutture e aziende, quelli della «Operation Technology», sono i nuovi bersagli di cybercriminali e terroristi informatici.

«Negli ultimi mesi il panorama delle minacce è cambiato drammaticamente e le soluzioni dal mondo dell'IT, l'Information Technology, non funzionano. Si può bloccare un server di posta elettronica sotto attacco senza grandi conseguenze, ma non si può fare lo steso con un impianto di produzione». La premessa di Amir Zilberstein, co-fondatore e ad di Claroty, è ribadita nelle sale riunioni delle principali start-up israeliane che si occupano di cybersecurity applicata ai sistemi di controllo industriale e infrastrutturale. A pochi isolati una dall'altra, a Tel Aviv, sono concentrate Claroty, Indegy e Scadafence. Se le prime due hanno stabilito lì sede e laboratori, gli uffici commerciali sono nel mercato più importante, gli Usa. Scadafence, con un piccolo ufficio a Tel Aviv, svolge invece ricerca&sviluppo a Be'er Sheva, l'hub tecnologico alle porte del Negev.

Tradizionalmente, IT e OT avevano ruoli separati. Oggi, nel pieno della quarta rivoluzione industriale, con l'integrazione tra macchinari e rete, il confine tra i due sistemi è stato abbattuto. «Impianti e infrastrutture sono vecchi di decenni. Non sono dotati di username e password, non hanno lucchetti informatici. Oggi, però, anche questi dinosauri - così li definisce Dana Tamir, specialista di Indegy - sono connessi con nuovi dispositivi high tech. La connettività porta con sé ovvi vantaggi, ma l'altro lato della medaglia è l'altissima vulnerabilità».

Il primo passo è quindi il monitoraggio in tempo reale. «Il nostro ruolo - chiarisce Yoni Shohet, ad di Scadafence - è ascoltare senza interferire. Questi prodotti sono soluzioni basate su software per allertare. Dobbiamo garantire di essere non invasivi e non distruttivi». Oltre che discreti. I danni d'immagine legati ai blitz informatici possono creare perdite finanziarie tanto quanto un blocco della produzione. E preoccupano le aziende ancora di più.

BY NC ND ALCUNI DIRITTI RISERVATI

VkVSlyMjVm9sb0Vhc3lSZWFkZXJfQW5zYSMjIzJlMzI0YTk4LTAwNGEtNDQ0Zi1hMjVkLWNjZmY3N2JiNzMyMiMjIzIwMTctMDktMjBUMDU6MTg6NTMjIyNWRVI=