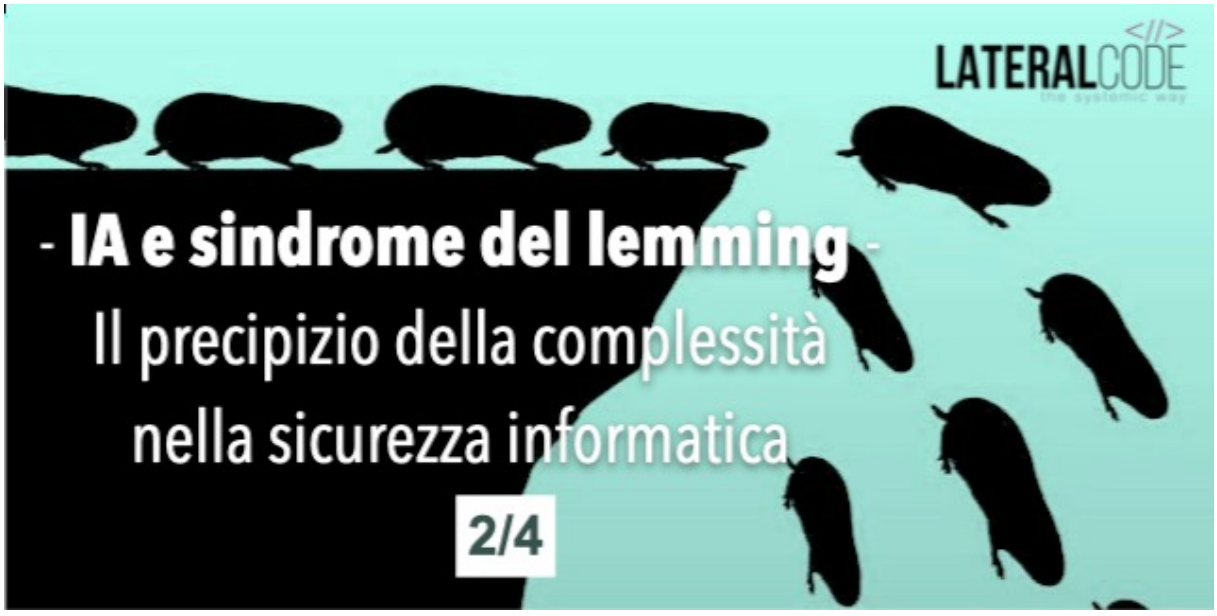
LATERAL NEWS — LATERALCODE

IA e sindrome del lemming: il precipizio della complessità (2/4)

11 luglio 2023



Proseguiamo il discorso iniziato la volta scorsa (a proposito, com'è andata?). Continuiamo a farlo con calma perché il tema della complessità è insidioso e occorre imparare e mantenere una prospettiva (ancora) inusuale: insomma, ricadere nei soliti schemi è un attimo!

I PROGRESSI NELLA SICUREZZA INFORMATICA A OGGI

C'è molto fermento intorno alla sicurezza informatica, sia perché è oggettivamente un tema delicato e centrale, sia perché è occasione di ***business*** milionari più o meno trasparenti.

Agenzie, super-agenzie, ***task-force***, università, consorzi, ***report***, commissioni, convegni, comitati, cabine di regia sono tutte occasioni di "confronto e crescita"; ma **in quale misura** è così?

Se osservate bene questi **progressi** attraverso la lente critica della **struttura di pensiero** noterete che siamo spesso di fronte a esasperazioni di **paradigmi noti**, di elevazioni a potenza di principi di sicurezza già ampiamente frequentati dove l'***hardening*** dei sistemi, pur necessario, e l'analisi riduzionistica, quasi atomica, sono inizio e fine del processo stesso di ricerca, un processo volto a **predisporre** quei medesimi sistemi all'inevitabile **scontro quotidiano** con gli attaccanti, nobilitato da principi come "identificazione", "prevenzione", "rilevamento", "risposta dinamica", "recupero" ecc. (lo so, **in italiano** sembrano meno risolutivi); il tutto demandato, per troppa parte e con **preoccupante** disinvoltura, ai nuovi e costosi dèi

dell'IA la quale, un giorno, non avrà pudore di comunicarci serenamente cose del tipo: "…sei stato violato con una tecnica che non conoscevo ma adesso che la conosco ho imparato a difenderti da chi ti attaccherà con la stessa tecnica o simile", oppure "…ci stanno attaccando, devo capire se è un'altra intelligenza artificiale oppure un genietto adoscelente ma, no problem, anche io sono intelligente!". Grazie Bob.

Abbiamo poi le attese funzioni interpretative e predittive dell'IA: ma cosa dovrebbe prevedere, di preciso? Dai, seriamente, cosa ci attendiamo nello specifico? Stiamo affrontando una **complessità fuori controllo** con un'altra complessità che, come dimostrato nella puntata precedente, rende il tutto ancora più incontrollabile: scusate la franchezza ma a volte mi viene da pensare che un simile approccio, così contraddittorio, sia in realtà o molto funzionale ad astronomiche parcelle di consulenza o reale frutto di insipienza. Colpa mia, che penso sempre male.

In ogni caso, ecco la più grave forma di miopia: osservare, studiare e tentare di risolvere i problemi sistemici pensando in termini lineari di causa-effetto.

Ormai dovrebbe esservi chiaro: **c'è differenza tra progresso ed evoluzione** e sarà bene tener presente questa distinzione o ci ritroveremo sempre più spesso con i cattivi (leggi "criminali") che nell'epoca della sorveglianza telefonica hi-tech si **ammanettano** gioiosi al loro fedele e fidato Nokia 8210.

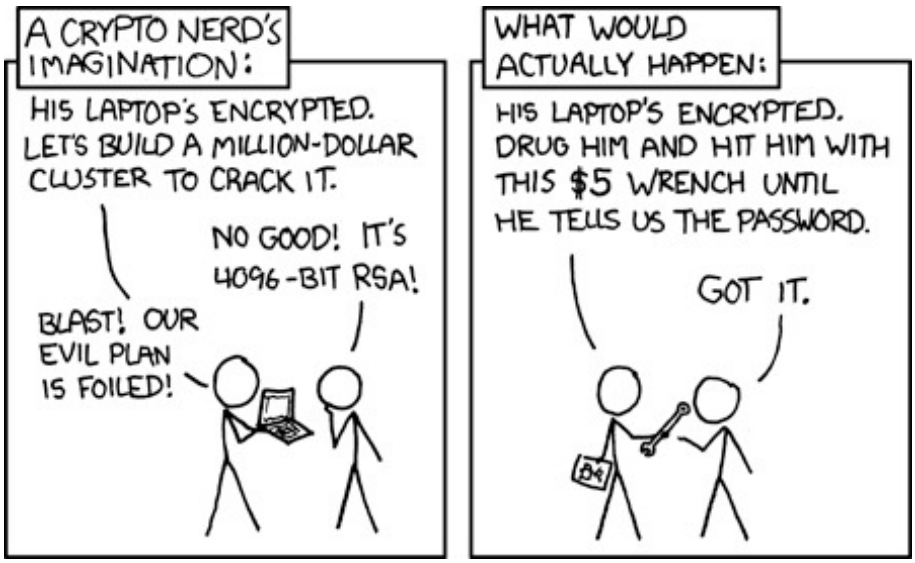
LA TRAPPOLA OPPOSTA (e una breve specifica)

Il binomio "**complessità del problema**" -> "**complessità della soluzione**" rischia di essere l'ennesima relazione lineare, pigra.

Capiamoci bene: non intendo dire che occorra semplificare purchessia, no, tutt'altro, dico solo che curare la complessità con la complessità è, paradossalmente, la risposta più **analitica**, semplicistica e meno efficiente che si possa proporre.

La difficoltà che dobbiamo accettare è quella di imparare a risolvere i problemi di un sistema dinamico complesso utilizzando **pensiero sistemico** anziché analisi lineari. E usare l'IA, per quanto controintuitivo, è stramaledettamente analitico.

Dobbiamo decidere per un profondo cambiamento del pensiero anche se ciò ci costerà più di qualche resistenza (guarda un po', un sistema che "resiste"…).



Permanent link to this comic: https://xkcd.com/538/

- LA BREVE SPECIFICA -

Contrariamente a quanto potrebbe sembrare, pensare in termini di sistema non significa vivere nel regno della teoria e dell'indefinito dove prendere decisioni è complicato dal fatto che non esisterebbe una verità assoluta in base alla quale deliberare; è, invece, esattamente l'opposto, è il luogo in cui le cose sono chiamate con il loro nome, dove se una situazione è complicata come tale la si affronta, evitando di semplificarla artificiosamente al solo scopo di prendere una qualsivoglia decisione (costringendola, per di più, nella forma dei nostri contenitori mentali).

Pensare in termini di sistema significa rispettare la complessità, trattarla come un elemento ineluttabile e infido delle attività umane e adattare il nostro pensiero a essa, non il contrario. Qui non facciamo un corso di pensiero sistemico e dinamica dei sistemi (ovvio) ma forse possiamo finalmente capire che l'approccio ai problemi DEVE essere diverso.

IL PARADOSSO DEL SECURE BY DESIGN

Questa è sia breve sia facile. "**Secure by Design**" è un altro straordinario concetto di cui però vediamo fare un uso strumentale e di spregiudicato marketing.

Sarà sufficiente che vi poniate **una sola domanda** per comprendere la ragione di questo giudizio. La domanda è:

> *stanti le premesse sui sistemi fatte finora, per es. in riferimento alle "emergenze di sistema", cosa c'è di così "progettualmente sicuro" in una soluzione di cyber security che comprenda l'IA?*

Fine del paragrafo più breve di sempre. Scrivete nei commenti.

(La prossima volta spenderemo due parole anche sulla Privacy by Default e credo vi divertirete).

ALTRE QUATTRO DOMANDE

Quando inizi con una domanda poi è difficile trattenere le altre (che ti escono pure sgrammaticate):

1. Ma davvero usereste l'IA per proteggere i vostri dati, la vostra azienda, il vostro Paese?

2. Ma davvero affrontereste la complessità a suon di **analisi**?

3. Ma davvero credete che l'IA **complichi** la vita ai cattivi della rete, specie a quelli più pericolosi e meglio **finanziati**, e la **semplifichi** a noi (che siamo ovviamente i buoni)?

4. E in ultimo: davvero credete che l'IA renda più "sicura" internet?

ALLA FINE DELLA SECONDA PUNTATA

Prima di parlare di "**sistemi di sicurezza informatica**" dovremmo cambiare modo di **pensare** e **progettare** accettando il fatto che la parte più importante e insidiosa della locuzione non è in "sicurezza informatica" ma in "**sistemi**"; fino a quel momento sarà più corretto chiamarli "**sistemi di speranza informatica**" perché l'unica cosa di cui possiamo essere sicuri è di una ventura crisi di sistema.

Spero (e credo) che in queste prime due puntate abbiamo raccolto sufficienti elementi, per quanto introduttivi, utili a sospendere il giudizio e a renderci possibilisti di fronte all'idea che… **stiamo sbagliando approccio al problema**.

La prossima volta vedremo, fra le altre cose, quali siano state le premesse logiche e progettuali della **nostra** ricerca: credo che sarà utile anche a chi, fra voi, volesse a sua volta tentare un primo simile approccio nei propri progetti.

> *"Di gran lunga, il più grande pericolo dell'intelligenza artificiale è che le persone concludano troppo presto di averla compresa." (Eliezer Yudkowsky)*

E poi, questi lemming, cosa c'entrano? Dai, sono convinto che ormai vi sia chiaro…

Alla prossima!

Gianluigi Merlino