# Cassandra Crossing 673- Il debito tecnico come arma cibernetica-


Photo by Towfiqu barbhuiya on Unsplash

*(673) - Il debito tecnico è fatto non solo di bug nascosti e di una qualità del codice sempre peggiore, ma anche dalle modalità di saldo; prima o poi qualcuno lo pagherà, ma le modalità di riscossione saranno imprevedibili ...*

**3 giugno 2026** - Cassandra ha già ripetutamente esternato in maniera "eruttiva" sulle questioni legate al debito tecnologico, sepolto nel software che ci circonda e ci fa vivere.

Qualche volta si meraviglia che i 24 indulgenti lettori non si siano ancora organizzati per fare su questa insistenza una dimostrazione di protesta proprio sotto le sue finestre.

Eppure ci sono ancora tante elucubrazioni da fare, che magari potrebbero sembrare azzardate; e siccome, secondo Andreotti, ne vale quasi sempre la pena, la vostra profetessa preferita procederà imperterrita.

**Stato dell'arte**: Industria e militari si muovono sempre amichevolmente e di comune accordo, ma quello che molto spesso i militari fanno senza clamore, anzi in segreto, è utilizzare doppi standard.

Quello che per l'industria è un problema, in questo caso più che altro per i "consumatori", per i militari può essere una interessante ulteriore opportunità.

Non da oggi Cassandra evoca la costruzione, anzi ormai il continuo potenziamento, degli arsenali di armi cibernetiche, metodicamente costruiti monitorando le infrastrutture informatiche, militari e soprattutto non militari, dei potenziali nemici.

Il monitoraggio nascosto, che richiede competenze da "red team" sofisticate, viene svolto in modalità "*prima di tutto non farti scoprire*", proprio come un tipico attacco alla catena di fornitura (Solarwinds docet).

Questo può richiedere l'utilizzo di personale molto qualificato, ma non di falle di sicurezza particolarmente nuove. Si va alla ricerca soprattutto di problemi software, spesso vecchi e noti, di tutto quello che gira sulle reti interne, con particolare riguardo alle componenti SCADA e di controllo industriale di reti elettriche, informatiche e di distribuzione. Questo senza ovviamente escludere fonti informative utili per l'intelligence.

Le debolezze dei sistemi SCADA e di controllo possono essere poi utilizzate per creare exploit specializzati per quel particolare target, che vengono a loro volta immagazzinati, ed utilizzati per preparare piani di attacco orchestrati a livello tattico e strategico.

Piani di attacco che possono essere lanciati con un solo click del mouse.

Secondo Cassandra, che tiene a precisare di non aver accesso a fonti informative che non siano assolutamente pubbliche, ma che è non solo profetessa ma anche andreottiana nel profondo, tutto questo è in atto almeno da un decennio.

Qualunque stato dotato di un apparato militare degno di questo nome, come pure vari attori non statali di una certa dimensione economica, lo stanno certamente già facendo, in varia misura, da anni.

Ora, cosa può cambiare, in questo "*ipotetico*" contesto, grazie ad una grande diffusione della programmazione assistita dagli LLM, ed al limite del Vibe coding?

In termini di vettori di attacco, tecniche come il prompt injection e la corruzione dei foundation model possono aprire nuove vie per potenziare attacchi alla catena di fornitura del software.

Ma l'utilizzo del Vibe coding apre scenari interessanti anche per una ben facile caccia di bug che siano stati precedentemente indotti agendo sugli strumenti di programmazione basati sugli LLM. Facile come la "*pesca sportiva*", insomma.

Ed infine, *last but not least*, anche semplicemente studiando la tipologia di bug evergreen indotti dall'utilizzo degli LLM nella programmazione, e vendemmiandone cospicue quantità, tanto più grandi quanto più si diffonde questo tipo di "*programmazione*".

Detto questo, per i militari non di un nuovo mondo si tratta, ma di interessanti e potenzialmente molto profittevoli ulteriori campi da sfruttare, sempre con il solito scopo di arricchire ed aggiornare i propri arsenali di armi cibernetiche.

Ed ovviamente nel mondo militare, mentre si lascia che il lo sviluppo software civile si corrompa al fine di avere più terra da arare, al proprio interno ci si guarderà bene dallo sviluppare secondo queste "nuove mode"; certo, solo per quanto possibile, visto che anche i militari sono esposti ad "inquinamenti" provenienti dal software "civile".

Vivremo (o moriremo) certamente in tempi interessanti.

---