OPINIÓN

DESPUÉS DE LA PANDEMIA

La ciberdefensa europea no puede depender del permiso de Washington

Enrique Dans

Publicada 14 mayo 2026 02:44h

Durante décadas, Europa ha hablado de **soberanía tecnológica** como quien habla del tiempo: con preocupación, con diagnósticos acertados, con alguna declaración solemne, pero con muy poca consecuencia práctica. Cada crisis parecía confirmar lo mismo: dependemos de infraestructuras, plataformas, nubes, chips, sistemas operativos y modelos desarrollados, controlados o condicionados desde fuera. Pero el **caso Mythos** introduce una diferencia fundamental: ya no hablamos de productividad, de competitividad o de quién captura el valor económico de la innovación. **Hablamos de defensa.**

Mythos no es simplemente otro modelo de inteligencia artificial. Es, si creemos la información disponible y las reacciones que ha provocado, una herramienta capaz de identificar vulnerabilidades de día cero en sistemas operativos, navegadores e infraestructuras críticas a una escala que hasta ahora asociábamos a equipos humanos muy especializados, con mucho tiempo, mucho presupuesto y un altísimo nivel de conocimiento. Lo importante no es si Anthropic ha exagerado más o menos sus capacidades. Lo importante es que el umbral ha cambiado. La búsqueda de vulnerabilidades, que antes era una actividad artesanal, escasa y cara, empieza a convertirse en un proceso industrializable.

Cuando una actividad se industrializa, deja de depender de unos pocos expertos. Se abarata, se acelera y se distribuye. Y eso, en ciberseguridad, altera por completo el equilibrio. Atacar siempre ha sido más fácil que defender: basta encontrar una vía de entrada, mientras que defender exige protegerlas todas. Pero si además la búsqueda de esa vía de entrada puede automatizarse con modelos capaces de probar, iterar, encadenar fallos y generar *exploits*, entonces las organizaciones que no tengan acceso a herramientas equivalentes quedan en una posición sencillamente inaceptable.

> *La búsqueda de vulnerabilidades, que antes era una actividad artesanal, escasa y cara, empieza a convertirse en un proceso industrializable*

Por eso la discusión sobre si las empresas europeas deben tener acceso a Mythos, o a herramientas comparables, no es un capricho corporativo ni una petición de igualdad simbólica. Es una necesidad estratégica. **Un banco europeo, una empresa energética, una operadora de telecomunicaciones o una**

Administración Pública no pueden defenderse de una clase de ataques que no pueden simular. No pueden evaluar su exposición frente a capacidades que otros sí poseen. No pueden esperar a que un proveedor estadounidense les diga, cuando lo considere oportuno, qué vulnerabilidades ha encontrado en tecnologías que ellos también utilizan. **En seguridad, depender de la cortesía de otro es una forma elegante de llamar a la indefensión.**

La negativa de Washington a ampliar el acceso europeo, mientras sus propias agencias y empresas sí pueden utilizar la herramienta, revela algo profundamente incómodo sobre la relación transatlántica. Estados Unidos se presenta como aliado, pero actúa cada vez más como propietario de las condiciones de seguridad de los demás. La alianza funciona mientras Europa compre, se alinee y acepte el papel de socio subordinado. Pero cuando aparece una tecnología crítica, de doble uso, capaz de alterar el equilibrio defensivo de sectores enteros, la respuesta no es cooperación entre iguales, sino control unilateral.

> *Estados Unidos se presenta como aliado, pero actúa cada vez más como propietario de las condiciones de seguridad de los demás*

Es comprensible que una herramienta como Mythos no pueda ponerse en circulación sin restricciones. Sería irresponsable. Pero, precisamente por eso, la cuestión no debería depender de una decisión administrativa de la Casa Blanca ni de los incentivos comerciales de una empresa privada. Si el argumento es que el acceso debe estar estrictamente controlado, entonces constrúyanse mecanismos de acceso controlado, auditado, supervisado y limitado a usos defensivos. Lo que no es aceptable es que el control se traduzca en una frontera política: acceso para los nuestros, espera para los demás.

Europa debería leer este episodio como lo que es: una advertencia. No basta con pedir acceso. Pedir acceso es necesario en el corto plazo, porque **las amenazas no van a esperar a que Bruselas complete otro ciclo de consultas. Pero la respuesta real debe ser mucho más ambiciosa: construir capacidad propia. Capacidad técnica, regulatoria, industrial y militar.** Modelos europeos especializados en ciberdefensa, infraestructuras de evaluación, entornos seguros para uso por parte de empresas críticas, colaboración obligatoria con

mantenedores de *software* abierto, y supervisión pública seria, no meros códigos voluntarios redactados por los mismos actores a los que se pretende supervisar. De hecho, es precisamente ese factor, el código abierto, el que Europa debería tener de manera natural, por su filosofía, a apalancar lo más posible.

La paradoja es evidente: la herramienta que mejor puede defender un sistema es también una herramienta que puede atacarlo. Pero esa paradoja no se resuelve negando el acceso a quienes deben defenderse. Se resuelve creando instituciones capaces de gestionar tecnologías de doble uso con criterios democráticos, transparentes y proporcionados. Europa lleva años regulando tecnologías que no controla. **Quizá va siendo hora de controlar algunas de las tecnologías que regula.**

El caso Mythos debería poner fin a una ingenuidad peligrosa: la de creer que la alianza con Estados Unidos equivale automáticamente a seguridad compartida. Ya no es así, ni en ciberseguridad ni en seguridad convencional. En un mundo en el que la inteligencia artificial convierte la ciberseguridad en una carrera de velocidad, el aliado que te impide correr no te está protegiendo: te está dejando atrás. Y cuando hablamos de bancos, infraestructuras críticas y servicios esenciales, quedarse atrás no es una opción estratégica. Es una vulnerabilidad.

******Enrique Dans es profesor de Innovación en IE University.***