Automotive e difesa, occasione per Torino

Claudio Chiarle 10 Dicembre 2025

Torino è al centro dell'Europa e abbiamo due grandi occasioni che non ci devono sfuggire: l'automotive e la difesa. L'incontro del 10 dicembre sul futuro dell'automotive è slittato di qualche giorno o a gennaio, poco importa: il cambio di passo di Stellantis con l'arrivo del nuovo Ceo, Antonio Filosa, è chiaro e va incontro al mercato.

L'Europa, anche alla luce del nuovo piano Trump sulla Nss (National Security Strategy), che indica la marginalità dell'Europa, ha bisogno di reagire celermente rilanciando il mercato dell'auto europeo e innovando l'industria della difesa. Ma ci vuole coraggio per scelte importanti.

Oggi le priorità sono due: **la cybersicurezza e il munizionamento**. Molto ostico, soprattutto, il secondo argomento, ma o siamo capaci di realpolitik o saremo destinati alla marginalità, come già sostengono Usa, Russia e Cina. E il passaggio da alleati fidati a servi della gleba avverrà senza che ce ne rendiamo conto, soprattutto per chi oggi pensa – come gran parte della destra – che siamo alleati fedeli e indispensabili.

Restiamo però sul concreto, perché le dichiarazioni di qualche giorno fa dell'ammiraglio Cavo Dragone sono di una semplicità realistica disarmante e invece sono state lette come una dichiarazione di guerra.

Dal sito Difesa Online: «*Le parole di Cavo Dragone al quotidiano britannico fotografano una realtà che l'Italia sta sperimentando sulla propria pelle. L'ammiraglio ha dichiarato che la Nato sta "studiando tutto sul fronte informatico" e che "essere più aggressivi o proattivi invece che reattivi è qualcosa a cui stiamo pensando*". Un "*attacco preventivo*", ha spiegato, "*potrebbe essere considerato un'azione difensiva",* anche se *"è più lontano dal nostro normale modo di pensare*"».

Salt Typhoon, entità che svolge attacchi cyber e collegata alla Cina, ha intensificato le proprie operazioni nel corso del 2025, tornando a colpire le infrastrutture di telecomunicazione europee con tecniche sempre più sofisticate. Secondo quanto riportato da **Darktrace**, azienda leader mondiale nelle soluzioni di cybersecurity: «*Le attività di Salt Typhoon hanno preso di mira organizzazioni in almeno ottanta paesi diversi, con almeno seicento entità notificate di essere state oggetto di interesse da parte degli hacker. L'Fbi ha confermato che oltre duecento aziende sono state compromesse a livello globale e l'azione di hackeraggio si è diffusa ben oltre il settore delle telecomunicazioni, includendo reti governative, infrastrutture di trasporto, strutture ricettive e reti militari».*

L'azione preventiva e proattiva di cybersicurezza non ha confini: se il server di un hacker è allocato in Russia o in Cina, abbiamo il dovere di neutralizzarlo laddove si trova.

Secondo Ict Magazine: «*Il gruppo NoName057(16) si è fatto conoscere nel 2022, poco dopo l'inizio dell'offensiva russa in Ucraina. Da allora si è attribuito numerose azioni contro siti governativi e istituzionali ucraini, statunitensi ed europei: l'Italia è stata presa di mira a partire dal 2023, con una serie di attacchi rivolti a ministeri, Carabinieri, Guardia di Finanza e Aeronautica Militare; agli aeroporti di Malpensa e Linate, ai porti di Trieste e Taranto e all'Agenzia Industrie Difesa; a società che erogano servizi idrici o di trasporto pubblico locale, all'Automobile Club Italiano (Aci); alle banche Intesa Sanpaolo, Nexi e Mediobanca; a diverse industrie del comparto bellico. Tutti rivendicati dal cyber group filo-russo NoName057(16), nel cui manifesto si ricorda "ai nemici" le parole dell'eroe nazionale russo Aleksandr Nevskij: "Whoever*

comes to us with a sword will perish by the sword!" (Chi viene da noi con la spada, di spada perirà)».

L'Italia e l'Europa non stanno a guardare e reagiscono, ma tra i Paesi europei l'Italia è il più debole in termini di capacità di difesa cibernetica: ecco perché le parole di Cavo Dragone non sono fuori luogo, bensì attuali, e vanno prese in considerazione anziché denigrate o fraintese, come hanno fatto anche esponenti e supponenti politici della sinistra.

L'altro aspetto ostico ma da affrontare è il munizionamento. Prima, però, una considerazione sul sistema di difesa europeo, in cui spicca il progetto **Michelangelo Dome di Leonardo**, che punta a proteggere l'Europa dalle minacce aeree – **dai droni fino ai missili balistici** – sul modello **dell'Iron Dome israeliano**. La cupola protettiva potrebbe essere operativa entro il 2030. Il Michelangelo Dome rappresenta la via di mezzo realistica tra la difesa comune europea oggi irrealizzabile e un primo passo concreto per attuarla, perché prevede un sistema di intelligenza artificiale capace di collegare tutti i sistemi diversi e farli funzionare come un'unica rete.

Se l'Europa riuscirà a parlare un linguaggio comune nella gestione di un sistema industriale e operativo di difesa comune, sarà un grande passo verso una difesa politica comune. La pace, e quella sin qui conseguita lo dimostra, si basa molto sulla deterrenza: sull'idea che un eventuale aggressore non si azzardi a compiere azioni di attacco se conosce il potenziale difensivo del possibile aggredito. E oggi l'Europa mostra un fianco scoperto con il progressivo disimpegno Usa nella Nato.

Se l'Italia e l'Europa hanno sistemi d'arma difensivi tecnologicamente insuperabili – dalle forze aeree a quelle terrestri – questi vanno alimentati. Puoi avere molti caccia intercettori, ma se non hai il munizionamento è come non avere nulla.

L'Europa ha adottato il programma Safe, a cui l'Italia aderisce insieme ad altri 18 Paesi Ue. Safe è un nuovo strumento finanziario di difesa congiunto dell'Unione Europea, approvato nel 2025, che consente agli Stati membri di ottenere prestiti a lungo termine agevolati dalla Commissione Europea fino a un massimo di 150 miliardi di euro.

Safe permette di finanziare sia progetti in corso sia nuovi progetti in diversi settori prioritari: sistemi di munizioni e artiglieria, piattaforme di combattimento terrestri e supporto alle forze terrestri, difesa aerea e missilistica, droni e sistemi anti-drone, capacità strategiche (logistica e mobilità), difesa informatica e protezione delle infrastrutture critiche.

Il programma richiede inoltre che la maggior parte del valore dei progetti provenga dalla base industriale europea o alleata, contribuendo così a rafforzare l'autonomia strategica della difesa dell'Ue.

L'Italia accederà a finanziamenti per 14 miliardi in cinque anni (2026-2030) per i programmi già definiti. Credo però che, alla luce delle ultime novità di Trump e del possibile divaricamento geopolitico tra Usa ed Europa, sia insufficiente finanziare solo ciò che è già stabilito. Penso che l'Italia debba uscire dalla sua comfort zone e candidarsi a un ruolo industriale e tecnologico ben più rilevante, dalla cybersicurezza al munizionamento.

Occorre essere cinicamente realisti senza per questo essere tacciati di guerrafondaismo, perché la crisi dei Paesi dell'Unione Europea si supera rilanciando l'industria (auto e difesa) e salvaguardando al tempo stesso i principi della democrazia contro guerre, nazionalismi e falsi patriottismi.

Torino ha un problema di riprogrammazione e rilancio industriale: possediamo il coraggio di affrontare argomenti politicamente scabrosi?

https://www.lospiffero.com/ls_article.php?id=94141