

INDIPENDENZA ENERGETICA SVILUPPO DEL FOTOVOLTAICO E QUESTIONI DI SICUREZZA

INTRODUZIONE

L'espansione delle energie rinnovabili è uno dei principali strumenti con cui l'Unione Europea intende da un lato contribuire a combattere i cambiamenti climatici, dall'altro ridurre, fino ad azzerare in prospettiva, la dipendenza energetica dai paesi produttori di fonti fossili, riduzione che il conflitto in Ucraina ha reso un obiettivo strategico primario.

Tuttavia, un'accelerazione nello sviluppo delle rinnovabili pone questioni da affrontare dal punto di vista delle dipendenze strategiche sia in termini dell'accesso alle materie prime (le cosiddette terre rare) usate per la realizzazione di impianti per la produzione di energie rinnovabili, sia in termini di utilizzo della componentistica e della capacità produttiva.

Si pone cioè il problema di evitare di passare da una dipendenza all'altra, facendo affidamento per la fornitura di componenti essenziali per l'installazione di una infrastruttura basata su impianti fotovoltaici su un numero troppo ristretto di paesi e, soprattutto, non del tutto affidabili.

L'obiettivo di questo studio è quello di analizzare le dipendenze strategiche dell'Europa nel settore delle energie rinnovabili e, in particolare, nel fotovoltaico evidenziando i rischi in termini di sicurezza dell'infrastruttura di rete elettrica e dei settori critici.



LE DIPENDENZE STRATEGICHE DELL'EUROPA

I progressi tecnologici che determineranno la capacità dell'UE di ridurre le emissioni di carbonio sono fortemente influenzati dalla capacità di accesso alle materie prime critiche.

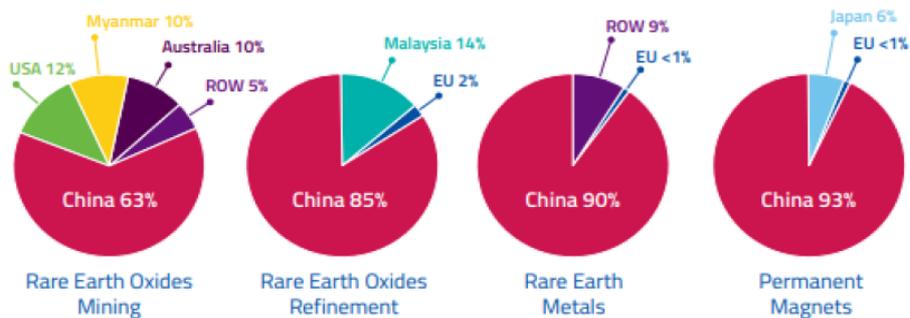
Le terre rare sono input importanti per prodotti e tecnologie chiave in una vasta gamma di settori, dall'elettronica alla generazione di energia, all'assistenza sanitaria, allo spazio e alla difesa.

La domanda dell'UE di magneti permanenti in terre rare – una componente chiave, ad esempio, per i veicoli elettrici e alcune turbine eoliche – potrebbe raddoppiare entro il 2030 fino a 40.000 tonnellate all'anno.

Anche la domanda di magnesio – un materiale rilevante per la produzione di alluminio, ad esempio con un ruolo importante nella riduzione del consumo di carburante e delle emissioni di CO2 nell'ecosistema della mobilità – dovrebbe aumentare significativamente parallelamente al consumo di alluminio.

In questo settore, come mostrato nella Fig. 1 la Cina è in una posizione dominante, mentre l'Europa è fortemente dipendente con una scarsa possibilità di diversificare le proprie fonti di approvvigionamento.

Fig. 1 Distribuzione geografica della produzione nella catena del valore nel settore delle terre rare



Fonte: ERMA-European Raw Materials Alliance (2021)

Un altro fronte critico riguarda le tecnologie solari fotovoltaiche, diventate la tecnologia in più rapida crescita nel settore dell'energia.

Il settore fotovoltaico svolgerà un ruolo importante nel garantire quantità sufficienti di elettricità pulita, tanto che la Commissione stima che il raggiungimento degli obiettivi del Green Deal europeo comporterà un aumento di tre volte della produzione di energia solare entro il 2030 e un aumento di quasi dieci volte entro il 2050.



Su quest'ultimo aspetto, l'ultimo Rapporto della Commissione Europea sulle dipendenze strategiche dell'Unione¹ evidenzia come il mercato globale del solare fotovoltaico sia dominato da aziende asiatiche, in particolare cinesi.

La maggior parte delle importazioni dell'UE proviene da meno di tre paesi terzi, con la Cina che rappresenta il 63% delle importazioni dell'UE.

Sebbene le imprese dell'UE siano leader mondiali in una serie di segmenti a valle della catena del valore del solare fotovoltaico, queste svolgono un ruolo minore in diverse aree importanti dei segmenti manifatturieri upstream.

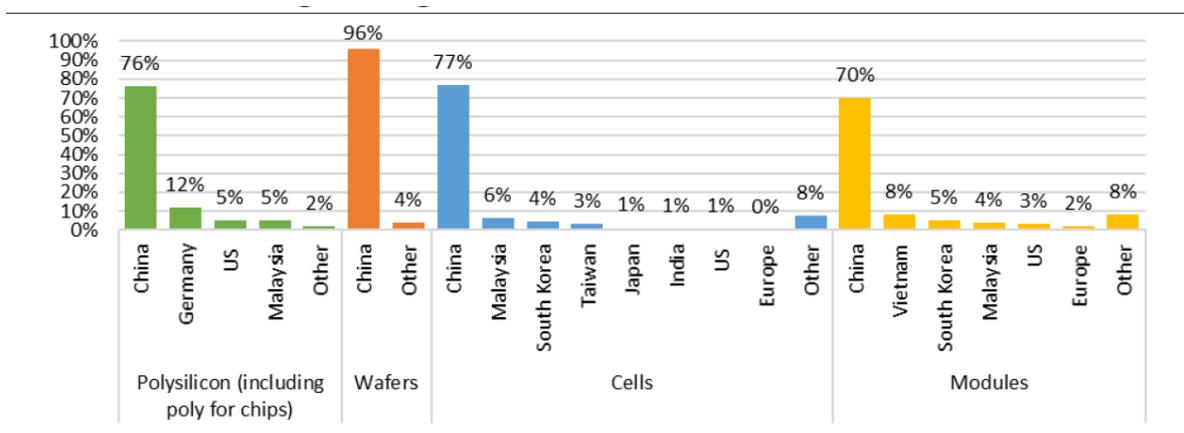
Le dipendenze strategiche dell'UE sono principalmente legate all'assenza di capacità produttive significative per lingotti, moduli e, in particolare, celle solari basate su wafer di silicio.

Nel 2020, la quota di produzione globale dell'UE nel settore del fotovoltaico era dell'11% per il polisilicio, del 2-3% per i moduli, dell'1% per i wafer solari e dello 0,4% per le celle solari.

In particolare, per quanto riguarda la produzione di celle e moduli solari, le aziende dell'UE sono rimaste significativamente indietro rispetto ai concorrenti asiatici a causa della limitata disponibilità di nuovo capitale in Europa dopo la crisi finanziaria del 2008, mentre la Cina, nello stesso periodo, ha investito ingenti risorse.

In pochi anni, il dominio cinese nelle fasi di produzione del polisilicio e delle celle fotovoltaiche è cresciuto significativamente: nel 2020, la Cina ha raggiunto una quota di produzione del 76% per il polisilicio e del 77% per le celle.

Fig. 2 Distribuzione geografica della produzione nella catena del valore nel settore fotovoltaico



International Energy Agency – IEA, PVPS and Trends Report 2021.
Nota: dati arrotondati

¹ "EU strategic dependencies and capacities: second stage of in-depth reviews", pubblicato il 22 febbraio 2022, disponibile al seguente link: <https://ec.europa.eu/docsroom/documents/48878>.

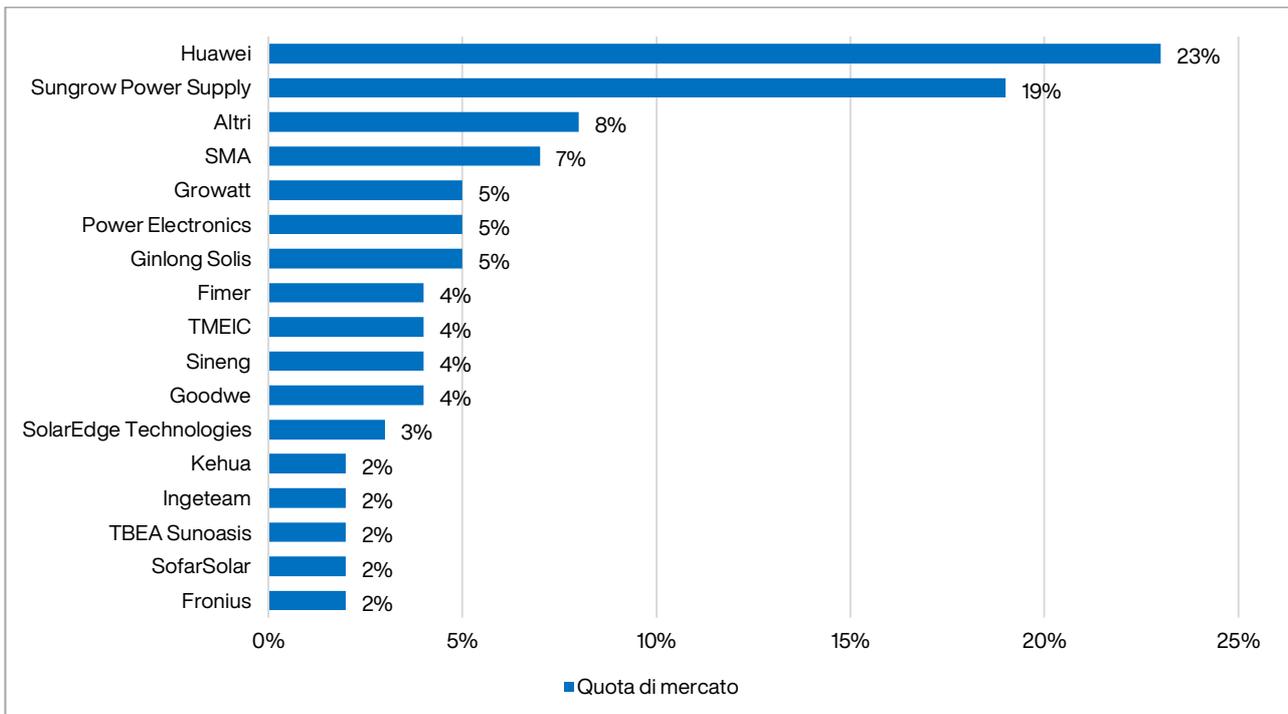


LA PRODUZIONE DI INVERTER

Per quanto concerne la produzione di inverter, una componente essenziale di un sistema fotovoltaico che consente di convertire in corrente alternata l'energia generata dai pannelli solari, come mostra la Figura 3, nel 2020 è stata l'azienda cinese Huawei la più grande produttrice di inverter fotovoltaici a livello mondiale, con quasi il 23% della quota di mercato, sulla base delle spedizioni.

Huawei è seguita da un'altra azienda cinese, la Sungrow Power Supply e dalla tedesca SMA, che rispettivamente detenevano nel 2020 il 19% e il 7% della quota di mercato.

Fig. 3 Quota di mercato degli inverter fotovoltaici a livello mondiale nel 2020, sulla base delle spedizioni.



Fonte: Statista.

La Cina è quindi leader in tutte le fasi della catena del valore della produzione fotovoltaica.

Alla luce di una concentrazione di mercato così significativa, l'industria solare può trovarsi di fronte a una situazione in cui non è più in grado di mitigare tali rischi diversificando o rispondendo in modo flessibile a essi.

Unitamente alla dipendenza nell'accesso alle terre rare, una tale situazione potrebbe ostacolare la futura diffusione delle tecnologie solari da parte dell'UE.



LE IMPLICAZIONI PER LA SICUREZZA

Esiste un'ulteriore fonte di preoccupazione legata a questi dati, su cui manca un dibattito adeguato e una conseguente consapevolezza, specie a livello europeo.

Il problema risiede nel fatto che l'espansione di forme decentralizzate di produzione di energia e il passaggio da una rete centralizzata a una rete diffusa e smart amplifica enormemente la vulnerabilità dell'ecosistema energetico rispetto ad attacchi cibernetici.

Come evidenziato da un importante rapporto del World Economic Forum già nel 2019², la produzione diffusa di energia avviene infatti attraverso dispositivi connessi digitalmente (IoT, Internet of Things), che possono essere soggetti ad attacchi informatici con conseguenze non solo per i singoli utenti ma per l'intera infrastruttura di rete.

Man mano che le reti elettriche diventano sempre più intelligenti e interdipendenti, infatti, anche l'impatto di un attacco informatico diventa più grave e di vasta portata.

Inoltre, tenuto conto che il sistema elettrico è alla base del funzionamento di quasi tutte le attività umane, compreso il sistema industriale e produttivo, quello dei trasporti, idrico e della sicurezza, gli effetti di eventuali attacchi possono essere estremamente rilevanti.

È quello che gli esperti definiscono "effetto a cascata", in cui la vulnerabilità cyber di un anello debole della catena può generare conseguenze significative su tutta la collettività.

Secondo il Global Risk Report 2019 del World Economic Forum³, gli attacchi cyber su larga scala sono al quinto posto tra i rischi più probabili nei prossimi 10 anni.

Il costo di un attacco informatico alla rete elettrica smart degli Stati Uniti è stimato in 1.000 miliardi di dollari, circa otto volte il costo della bonifica del disastro nucleare di Fukushima.

Un blackout invernale di sei ore in Francia potrebbe causare danni per oltre 1.7 miliardi di dollari.

Uno dei principali elementi di vulnerabilità è rappresentato dagli inverter fotovoltaici.

Il punto chiave è che gli inverter sono essenzialmente dei dispositivi IoT, collegati alla rete elettrica, che trasmettono e ricevono dati, inclusi quelli, decisamente sensibili, su come si distribuisce il consumo nazionale.

² Martel, E., Kariger, R., & Graf, P. A. (2019). Cyber Resilience in the Electricity Ecosystem: Principles and Guidance for Boards. Center for Cybersecurity and Electricity Industry Community. Si veda anche <https://www.weforum.org/agenda/2019/04/the-growing-risk-to-our-electricity-grids-and-what-to-do-about-it/>.

³ World Economic Forum, The Global Risks Report 2019 – 14th Edition, disponibile al seguente link: <https://www.weforum.org/reports/the-global-risks-report-2019/>.



Come sottolineato da un recente Report dell'Enisa⁴, l'Agenzia dell'Unione Europea per la Cybersecurity, è in questo modo che l'inverter rappresenta una potenziale superficie di attacco cyber e può fare da "ponte" per incursioni malevole nelle reti intelligenti in grado di provocare estesi blackout o sbilanciamenti nella rete elettrica.

Tramite l'inverter, infatti, un hacker potrebbe accedere al software della batteria per danneggiarla, o potrebbe manomettere il funzionamento dell'impianto fotovoltaico, fino a paralizzare, nelle ipotesi peggiori, l'intera infrastruttura di rete.

Il report evidenzia che nell'ultimo decennio le organizzazioni hanno dovuto affrontare diverse minacce alla sicurezza informatica delle loro infrastrutture di rete.

Ad esempio, nel 2015 in Ucraina sono state scollegate dalla rete circa trenta sottostazioni.

L'attacco informatico ha lasciato otto province senza elettricità per diverse ore, ha colpito più di 200.000 persone, i sistemi di controllo sono stati fisicamente danneggiati e le operazioni della rete sono state compromesse per diverse settimane dopo l'attacco.

Episodi come questo mostrano chiaramente come senza adeguate considerazioni sulla sicurezza, le risorse di rete, come i pannelli solari o i parchi eolici, possono diventare il bersaglio perfetto per gli hacker.

Il problema è che nell'ambito delle nuove reti energetiche intelligenti con migliaia di dispositivi connessi è molto difficile garantire l'inviolabilità dell'intero sistema cyber-fisico.

La teoria informatica, infatti, parla di "comportamento emergente", quindi non programmato o previsto: scopro quello che succede quando succede, quando diversi algoritmi progettati da diverse utility si trovano a "girare" insieme sulla stessa rete⁵.

Queste considerazioni pongono, quindi, l'esigenza di una riflessione attenta sui necessari livelli di cybersicurezza che tali dispositivi dovrebbero garantire e sul grado di dipendenza da paesi terzi nella loro produzione, in particolare dalla Cina, essendo l'azienda Huawei diventata uno dei maggiori fornitori al mondo di inverter solari.

Sulla questione esiste già da tempo un dibattito presso il Congresso USA.

La posizione dominante di Huawei nel mercato degli inverter, unita al sostegno di cui gode da parte del governo cinese, ha sollevato tali preoccupazioni negli Stati Uniti che, nel 2019, un gruppo bipartisan di senatori statunitensi ha inviato una lettera al Segretario all'Energia Rick Perry e al

⁴ EU Cybersecurity Market Analysis - IoT in Distribution Grid, disponibile al seguente link:

<https://www.enisa.europa.eu/publications/eu-cybersecurity-market-analysis-iot-in-distribution-grid>.

⁵ Si veda <https://www.qualenergia.it/articoli/20180222-energia-perche-gli-attacchi-informatici-sono-una-minaccia-concreta/> e <https://www.qualenergia.it/articoli/20180525-inverter-fotovoltaici-hackerati-pochi-minuti-quanto-sono-sicure-le-nostre-reti/>.



Segretario del Dipartimento di Sicurezza Nazionale Kirstjen Nielsen, esortandoli a vietare la vendita di tutti i prodotti solari di Huawei negli Stati Uniti, citando una minaccia alla sicurezza nazionale delle infrastrutture energetiche statunitensi, per via dei legami dell'azienda con i servizi segreti cinesi: "Both large-scale photovoltaic systems and those used by homeowners, school districts, and businesses are equally vulnerable to cyberattacks. Our federal government should consider a ban on the use of Huawei inverters in the United States and work with state and local regulators to raise awareness and mitigate potential threats."⁶

Le richieste di divieto sugli inverter Huawei da parte del gruppo di senatori sono proseguite con una seconda lettera, nello stesso anno, questa volta indirizzata alla Federal Energy Regulatory Commission (FERC) e al suo presidente, Neil Chatterjee, continuando a sostenere che gli inverter prodotti da Huawei e collegati alla rete elettrica degli Stati Uniti potessero rendere la nazione vulnerabile alla sorveglianza straniera e dare alla Cina "l'accesso a intromettersi in porzioni dell'approvvigionamento elettrico americano"⁷.

In parallelo, il presidente Biden ha fatto un ulteriore passo nella direzione di affrontare il dominio statale cinese nel settore dell'energia pulita firmando un ordine esecutivo volto a rendere le catene di approvvigionamento degli Stati Uniti più resilienti.

Queste forti pressioni politiche hanno portato Huawei a chiudere una parte delle sue attività nel business dell'energia solare sul suolo statunitense, mentre in Europa, nonostante crescano le preoccupazioni sul dominio statale cinese nel settore, ancora si tentenna sulle regolamentazioni da intraprendere⁸.

Nell'UE è stato inizialmente adottato un approccio più ambivalente verso Huawei, avendo solo accettato di ridurre la sua dipendenza da apparecchiature suscettibili di influenza del governo cinese per le future reti 5G.

Tuttavia, i funzionari di un certo numero di paesi dell'UE hanno recentemente lanciato un allarme sul ruolo dello stato cinese in settori delle loro economie che rappresentano interessi chiave per la sicurezza nazionale, tra cui le banche, l'energia e le infrastrutture⁹.

⁶ "Sia gli impianti fotovoltaici su larga scala che quelli utilizzati da proprietari di case, distretti scolastici e aziende sono ugualmente vulnerabili ai cyberattacchi. Il governo federale dovrebbe prendere in considerazione la possibilità di vietare l'uso di inverter Huawei negli Stati Uniti e collaborare con le autorità di regolamentazione statali e locali per sensibilizzare e mitigare le potenziali minacce."

Si veda al riguardo <https://www.forbes.com/sites/rrapier/2021/03/12/political-shifts-in-us-and-europe-bring-clean-energy-supply-chains-to-the-fore/?sh=1e4bfb2261f0>.

⁷ <https://www.pv-magazine.com/2019/12/12/u-s-senators-call-for-huawei-ban-in-letter-to-energy-regulator/>.

⁸ <https://www.globalist.it/economy/2021/03/15/libero-mercato-e-concorrenza-sleale/>.

⁹ Si veda <https://www.forbes.com/sites/rrapier/2021/03/12/political-shifts-in-us-and-europe-bring-clean-energy-supply-chains-to-the-fore/?sh=b04eef361f04>.



Queste preoccupazioni si estendono all'energia solare, con i responsabili politici dell'UE che hanno espresso preoccupazione anche per l'uso da parte della Cina del lavoro forzato musulmano nelle catene di fornitura dei moduli fotovoltaici.

Questo problema ha dato ulteriore slancio al Parlamento europeo, che sta spingendo per il divieto di commercio delle attrezzature cinesi per i moduli solari se gli abusi dei diritti umani sono coinvolti nella loro produzione.

Oltre alla questione dei diritti umani, è importante che anche in Europa si ponga attenzione alle questioni di sicurezza e affidabilità legate alla catena di approvvigionamento nel settore fotovoltaico, e valutare se perseguire un approccio simile a quello adottato negli USA.

Il tema delle catene di approvvigionamento di energia pulita non ha ricevuto molta attenzione politica fino a poco tempo fa, ma i governi sono sempre più sotto pressione per garantire che le potenziali minacce a queste catene di approvvigionamento non facciano deragliare gli sforzi globali per la decarbonizzazione e non mettano in pericolo la sicurezza delle infrastrutture energetiche dei paesi europei.



CONCLUSIONI

Le evidenze e le considerazioni sviluppate in questo studio risultano essere particolarmente significative nell'attuale contesto di crisi nel settore dell'energia.

Emerge infatti con chiarezza l'importanza di definire e implementare una strategia efficace per garantire la capacità effettiva dell'Europa di ridurre in maniera decisa la dipendenza da fonti fossili e aumentare la propria autonomia energetica nei confronti sia dei paesi produttori di fonti fossili sia dei paesi attualmente dominanti nella catena del valore del settore delle energie rinnovabili.

Una questione su cui esiste già un dibattito presso il Congresso USA e su cui anche in Italia e in Europa è quanto mai urgente sviluppare un'attenta riflessione in considerazione dell'attuale contesto geostrategico.

Una discussione che ponga in evidenza i rischi a cui siamo esposti, e che chiarisca anche che qui non si tratta di sviluppare un'autonomia tecnologica e produttiva tout court, bensì di evitare dipendenze unilaterali, soprattutto nei confronti di partner internazionali ritenuti meno affidabili, dove l'affidabilità è quella che si afferma a monte e a valle di una relazione con un partner con cui si instaura un sistema valoriale, di visione, interessi strategici e di fiducia condivisi.

Accrescere la capacità tecnologica e produttiva a livello europeo e riorientare la catena di approvvigionamento verso paesi terzi ritenuti affidabili dal punto di vista della sicurezza appare infatti un obiettivo da perseguire, considerato che secondo gli obiettivi europei la produzione di energia solare dovrà triplicare nell'Unione entro il 2030 da 147 TWh nel 2019 a 447 TWh, e quasi decuplicare entro il 2050 (1286 TWh).

Rispetto a questo, è bene evidenziare che la leadership di mercato che le imprese cinesi detengono nel mercato degli inverter fotovoltaici è dovuta principalmente a vantaggi competitivi legati a minori fattori di costo nella produzione.

L'obiettivo di riorientare la catena di approvvigionamento all'interno dell'UE o verso altri paesi partner che garantiscano livelli di affidabilità adeguati può quindi essere raggiunto attraverso opportune politiche in grado di influenzare sia la domanda sia l'offerta.

È un processo che non avverrà a costo zero poiché nelle scelte di approvvigionamento i criteri di efficienza andranno in parte sostituiti con quelli di affidabilità e i criteri economici andranno bilanciati con criteri di sicurezza, come peraltro avvenuto nell'ultimo anno e mezzo con l'esercizio da parte del governo italiano, dei poteri di Golden Power.

Tuttavia, se nei calcoli vengono inserite opportune considerazioni di risk assesment che includono i costi legati ai rischi per la sicurezza nazionale, il conto di questa operazione potrebbe non essere così salato.