



di **Francesco Galofaro** per Marx21.it
Politecnico di Milano

Tecnopolitica e protezionismo

Questa settimana *The Economist* [1] ha dedicato la propria copertina alla battaglia tra Stati Uniti e Cina per la supremazia digitale. Pur adottando il punto di vista del governo americano, l'articolo è molto utile per collocare il delicato confronto in corso nel quadro più vasto delle politiche protezionistiche promosse da Donald Trump. I temi di conflitto sono diversi: mercati on-line; hardware; supercomputer; computazione quantistica; navigazione satellitare; Intelligenza Artificiale; armamenti avanzati; sicurezza nelle telecomunicazioni; potere di imporre gli standard internazionali.

Alcuni tra questi problemi, cruciali per la comprensione delle relazioni internazionali contemporanee, andrebbero approfonditi meglio. Ad esempio, gli articoli dell'*Economist* collocano la supremazia quantistica al primo posto tra i problemi più urgenti, senza tuttavia spiegare di cosa si tratti. Occupandomi professionalmente di computazione quantistica e di *Information Retrieval*

[2], vorrei cogliere l'occasione per spiegare di cosa si tratta, dato che la funzione della comunicazione quantistica è meno intuitiva a comprendersi rispetto ai sistemi di riconoscimento dei volti o agli impieghi dei droni militari.

Protezionismo

I liberali condannano ideologicamente il protezionismo di Trump. E' invece più interessante da un punto di vista politico ricostruire i motivi della guerra economica cui stiamo assistendo. Ve ne sono diversi: tra i questi, alcuni sono strettamente legati alla tecnopolitica e alla lotta per l'egemonia tra cyberpotenze.

Per cominciare da un caso concreto, è forse sorprendente per noi europei sapere che la vendita di telefonini Huawei è vietata negli Stati Uniti. Il motivo è semplice: potrebbero avere una 'porta di servizio' (*backdoor*) che permetterebbe alle spie cinesi di carpire informazioni importanti. Di recente, il colosso americano delle comunicazioni AT&T si è accordato con Huawei per distribuire il loro ultimo modello; per tutta risposta la *National Security Agency* (NSA) ha messo in guardia i cittadini americani dall'uso dei 'telefonini rossi'.

Pura paranoia? Per nulla: i lettori probabilmente ricordano che, dopo l'attacco terroristico di San Bernardino del dicembre 2015, l'FBI ha tentato più volte di obbligare Apple a fornire di una simile *backdoor* i propri Iphone [3]. Forse ora è più chiaro il motivo per cui Apple non ha mai accettato di collaborare alle indagini della polizia e ha rifiutato le proposte di mediazione di Hillary Clinton e Bernie Sanders. Non si tratta tanto del problema di difendere la privacy dei cittadini americani; si tratta piuttosto del fatto che Apple rappresenta un modello di collaborazione USA – Cina. Come reagirebbe la Cina se Apple permettesse alla CIA di acquisire tutte le informazioni conservate sugli smartphone degli utenti cinesi?

Il modello economico Apple è basato sul binomio tra design occidentale e tecnologie orientali. Oggi questo modello è in crisi: le competenze possedute dalla Cina la rendono ormai in grado di fare da sé. Basta pensare al successo di aziende come Huawei o Xiaomi, o ancora a prodotti di design sperimentali proposti da Lenovo. Le aziende orientali possiedono una capacità di ideazione originale che le rende competitive. Infatti, la battaglia protezionista degli USA nei confronti di Huawei verte sul controllo della prossima rete di trasmissione dati mobile di quinta generazione (5G). Per questo motivo il comitato sugli investimenti stranieri negli USA (CFIUS) ha impedito la fusione tra Qualcomm – azienda americana leader nel *wireless* – e la malaysiana Broadcom, nel timore che la nuova gestione indebolisse gli USA nella lotta contro la Cina.

La Cina propone un nuovo modello di relazioni internazionali di tipo *win-win*, in cui non debba esserci per forza un vincitore e un vinto. E'precisamente questo modello a spaventare gli USA, autori del vecchio modello della globalizzazione entrato ufficialmente in crisi nel 2007, che un tempo avremmo chiamato 'capitalismo di rapina'. Ad ogni modo, come vedremo, la Cina possiede le risorse per combattere e vincere la guerra commerciale contro gli Stati Uniti.

Supercomputer

Non esiste campo della ricerca tecnologica che non abbia ricadute di tipo economico e militare. Per questo motivo restringiamo il nostro campo di indagine al problema della *cybersecurity*, la protezione dei dati da orecchie indiscrete. A questo proposito è interessante come la Cina abbia il primato nel campo dei supercomputer [4]. La Cina batte gli USA sia per quantità (202 a 143) che per velocità di calcolo. Nella classifica dei computer più potenti del mondo troviamo ai primi due posti i cinesi Sunway Taihu light e Milkyway 2; al terzo il supercomputer europeo Piz Daint; al quarto il giapponese Gyoukou; solo al quinto posto l'americano Titan, che pure era il più celere del mondo nel 2012. Oggi la sua potenza di calcolo è inferiore a un quinto del concorrente cinese. I supercomputer sono utili per scopi molto diversi, dalle previsioni del tempo alle simulazioni in fisica e in economia; tra gli altri impieghi abbiamo la criptoanalisi, il

complesso di tecniche impiegate per decodificare i messaggi in codice.

La minaccia rappresentata dai supercomputer cinesi per gli USA è molto più grave di quanto non si pensi. Oggi capita spesso di leggere che non vale più la legge di Moore: la tendenza, empiricamente verificata nella seconda metà del '900, per cui la velocità di un microprocessore quadruplicava ogni tre anni. La ricerca tecnologica sui microprocessori ha raggiunto i propri limiti fisici, e di conseguenza è sempre più difficile assemblare nuovi computer con crescenti potenze di calcolo. Questo è il motivo per cui la ricerca si è orientata verso i computer quantistici.

Come decodificare un messaggio segreto

Perché i supercomputer sono così importanti in crittoanalisi? Perché le tecniche che permettono di criptare i dati sono basate su problemi matematici la cui soluzione è difficile. Vediamo di spiegarlo con un esempio. Il problema principale di un agente segreto è fare avere al destinatario di un messaggio in codice anche la chiave con cui è stato cifrato. Se Alice deve inviare a Bob sia il messaggio cifrato sia la chiave, c'è il rischio che questa venga intercettata da Eva, sollecita agente del controspionaggio. Una soluzione consiste nei sistemi di cifratura asimmetrica: il sistema genera due chiavi (diretta e inversa) legate da una complessa funzione matematica. Bob genera entrambe le chiavi, e rende pubblica la chiave diretta. Quando Alice vuole scrivere un messaggio in codice per Bob, lo codifica con la chiave diretta, nota a tutti, compresa Eva. Ma Eva non conosce la parte inversa della chiave, indispensabile per decodificare il messaggio e nota solo a Bob.

A questo punto, Eva ha bisogno di un supercomputer per tentare di trovare la chiave inversa di Bob a partire da quella pubblica, diretta. L'impresa può richiedere milioni di dollari - cifra che le agenzie di sicurezza hanno senz'altro a loro disposizione; richiede anche diversi anni di lavoro, e il tempo è al contrario un fattore che gioca *contro* Eva e il suo governo.

Computer quantistici

Lo scenario è reso ancora più complicato dalla fisica quantistica. I computer quantistici del futuro saranno in grado di decodificare i dati a velocità finora inedite, permettendo di aggirare il problema della fine della legge di Moore. In che modo? Ad esempio, per risolvere un problema come 'trovare il sentiero che esce dal bosco' un computer classico esplora, per così dire, un sentiero alla volta. Quando non trova quel che cerca torna indietro, e prova con il secondo sentiero, poi il terzo e così via. Pensiamo ora a un computer capace di esplorare *tutti i sentieri contemporaneamente*

: avremmo così compreso il computer quantistico.

Sono davvero possibili i computer quantistici? Nata da un'intuizione di Feynman, la teoria matematica per la costruzione dei computer quantistici risale agli studi pionieristici di David Deutsch (seconda metà degli anni '80 [5]). Da allora, la loro realizzazione è divenuta essenzialmente un problema ingegneristico, sebbene non manchino le novità anche da un punto di vista teorico. Google ha annunciato la realizzazione di un microprocessore quantistico per quest'anno [6]; tuttavia, data l'importanza militare di questa tecnologia, la domanda da porsi

dovrebbe essere: 'e se i computer quantistici esistessero già?'. Ad esempio, se la nostra agente Eva scoprisse il computer quantistico, avrebbe tutto l'interesse a tenere la notizia nascosta, per decodificare indisturbata i segreti di Alice e Bob, del tutto ignari del fatto di venire intercettati.

Crittografia quantistica

La fisica quantistica tuttavia offre ad Alice e Bob un modo sicuro per prevenire l'interferenza del supercomputer quantistico di Eva. Non devono far altro che collegare i propri computer con un canale classico – che trasmette bit di informazione – e un canale quantistico, che trasmette fotoni polarizzati (qubit) i cui stati sono correlati a coppie: ad esempio, ogni volta che il fotone A è in stato 1, anche il fotone B è in stato 1. Se il canale quantistico viene intercettato da Eva, l'effetto pratico sarà quello di disturbare questa correlazione. Bob e Alice possono verificare se ciò è avvenuto comunicando tramite il canale classico. Un altro indubbio vantaggio di questa tecnologia è il fatto che la generazione delle chiavi è del tutto casuale: non è la soluzione a un problema matematico, come avviene nella crittografia classica [7]. A differenza del computer quantistico la crittografia quantistica è una tecnologia matura, già commercializzata da diverse compagnie [8].

Supremazia cinese

Come nel campo dei supercomputer, la Cina detiene attualmente il primato della computazione quantistica e delle sue applicazioni. QUASS (Quantum Experiments at Space Scale) è un progetto di collaborazione tra Europa e Asia che impiega un satellite per le comunicazioni quantistiche. Nel 2016 ha permesso una storica videochiamata tra gli scienziati cinesi ed austriaci attraverso un canale quantistico sicuro lungo 7500 km. La creazione di una rete quantistica sicura tra Europa ed Asia è prevista per il 2020 [9].

Inoltre, nel settembre 2017, la Cina ha lanciato la prima rete quantistica di comunicazione privata commerciale che connette 200 utenti governativi e ufficiali a Jinan, capitale della provincia di Shandong. Il prossimo obiettivo è collegare Pechino e Shanghai [10]. Infine, la Cina ha annunciato la creazione di un computer quantistico con applicazioni militari entro il 2020 [11].

Le ragioni di Trump

Così come nel campo dei supercomputer e delle applicazioni della fisica quantistica, la Cina è egemone in un insieme di campi, dalle telecomunicazioni cellulari all'intelligenza artificiale. Secondo i dati dell'Economist, in Cina la percentuale di laureati in scienze, tecnologie, ingegneria e matematica è del 6% sul totale, mentre negli USA è del 2%; il primato riguarda anche il numero assoluto dei laureati [12]. Dal punto di vista USA, la Cina è l'erede unico di due minacce tradizionali della seconda metà del '900: quella bellica, rappresentata dall'Unione sovietica, e quella tecnologica, rappresentata dal Giappone. Un sistema *win-win* è precisamente ciò che gli USA non vogliono, perché porterebbe la loro economia a dipendere inestricabilmente da quella Cinese, la quale ha già una bilancia commerciale in attivo di 375 miliardi di dollari rispetto agli USA. I colpi di frusta della globalizzazione sui lavoratori americani fanno sì che anche tra le file dei democratici si stia creando un gruppo favorevole all'introduzione di dazi; pensiamo ad esempio ad Elizabeth Warren, senatrice del

Massachusetts; Bill Richardson, ex-governatore del New Mexico e ambasciatore USA presso l'ONU; Marcy Kaptur, membro della camera dei rappresentanti per lo stato dell'Ohio; Sherrod Brown, senatore dell'Ohio [13].

Opportunità per i Paesi europei

Esiste la possibilità concreta che la guerra commerciale tra USA e Cina avvantaggi l'Europa. Come abbiamo già visto, esistono già collaborazioni scientifiche importanti con tra Europa e Cina nel campo delle tecnologie quantistiche. Allo stesso modo, se la guerra dovesse estendersi, la Cina non dovrà far altro che acquistare Airbus al posto di Boeing; collaborare con l'ESA, e non con la NASA; scambiare i propri studenti con quelli del Plateau de Saclay e non più con quelli della Silicon Valley. Ciò che si richiede ai Paesi europei interessati è condurre una politica estera improntata al pragmatismo. Allo stesso modo, non si vede perché le forze politiche della sinistra europea dovrebbero sposare il libero scambio come unica ideologia economica ammissibile, invece di analizzare le cause dei conflitti economici in atto e trarne le dovute conseguenze.

Per una ridefinizione della tecnopolitica

La nozione di *tecnopolitica* è stata definita da Stefano Rodotà come l'insieme delle trasformazioni che l'innovazione tecnologica ha apportato non solo al modo in cui la sfera della politica si presenta ma anche al modo in cui essa si struttura [14]. Questa nozione è stata esplorata in maniera ancora insufficiente: molte considerazioni sono state dedicate al potere, al rapporto tra governanti e governati, alla democrazia e al suo futuro; poca attenzione è stata dedicata alle *Relazioni internazionali*, ai rapporti di forza tra Paesi, tra l'infrastruttura economica e le prospettive di culture diverse sul ruolo delle tecnologie. In particolare, le nuove soggettività della politica, collettive e transnazionali, apparse negli ultimi vent'anni sul piano della manifestazione fenomenologica (ad esempio Apple e Huawei) sembrerebbero generate da una dialettica tra due tendenze opposte: la lotta per l'egemonia tecnologica, per il potere di imporre i propri standard allo scopo di instaurare nei Paesi egemonizzati una dipendenza culturale prima ancora che economica; un modello di cooperazione alternativa alla globalizzazione bancarottiera che ha gettato l'Occidente in una crisi senza sbocchi. Si direbbe questa la reale contraddizione che segna le dinamiche più attuali del capitalismo contemporaneo.

NOTE

1 The Economist, March 17th-23rd 2018.

2 Ad es. <http://ieeexplore.ieee.org/document/7982319/?reload=true>;

3 https://en.wikipedia.org/wiki/FBI%E2%80%93Apple_encryption_dispute#FBI_withdrawal_of_request

4 <https://www.top500.org/news/china-pulls-ahead-of-us-in-latest-top500-list/>

5 Deutsch, David (1985). "Quantum theory, the Church-Turing principle and the universal quantum computer". *Proceedings of the Royal Society A*. 400 (1818): 97–117, doi:10.1098/rspa.1985.0070.

6 <https://research.googleblog.com/2018/03/a-preview-of-bristlecone-googles-new.html>

- 7 <https://simons.berkeley.edu/sites/default/files/docs/1319/slidesdiamanti.pdf>
- 8 https://en.wikipedia.org/wiki/Quantum_cryptography
- 9 https://en.wikipedia.org/wiki/Quantum_Experiments_at_Space_Scale
- 10 <https://www.reuters.com/article/us-china-quantum/china-sets-up-first-commercial-quantum-network-for-secure-communications-idUSKCN1BO0CT>
- 11 <http://www.scmp.com/news/china/society/article/2110563/china-building-worlds-biggest-quantum-research-facility>
- 12 <https://www.forbes.com/sites/niallmccarthy/2017/02/02/the-countries-with-the-most-stem-graduates-infographic/#21ab86f5268>
- 13 <https://www.cnbc.com/2018/03/02/democratic-congresswoman-supports-trumps-tariffs-we-cant-afford-to-lose-us-steel-production.html>
- 14 http://www.treccani.it/enciclopedia/tecnopolitica_%28XXI-Secolo%29/