PER UNA GERARCHIA DELLE CIBERPOTENZE

di *Matthew Crosston*

Un quintetto di Stati guida le classifiche del potere cibernetico: Usa, Cina, Russia, Israele e Regno Unito. Obiettivi e ipocrisie dell'uso strategico della Rete. L'America resta il bullo più grosso e cattivo nel Web. Chi più fa meno dice: Mosca prenda nota.

1. Qualunque analisi che passi in rassegna e compari le potenze cibernetiche più avanzate e attive finisce in fretta per limitarsi ai soliti noti: Stati Uniti, Cina, Russia, Israele e Regno Unito. La ricorrenza di questo quintetto è generalmente dovuta a una combinazione di fattori: da quanto tempo i vari attori hanno iniziato a guardare alla dimensione cibernetica come a un legittimo ambito della potenza e a uno strumento statuale; i sempre maggiori investimenti sia in termini di risorse finanziarie che di personale; la dimostrata assertività nell'utilizzo di questo potere per raggiungere obiettivi strategici.

Almeno dal 2010 gli Stati Uniti si sono impegnati con determinazione a rimanere l'incontestata potenza guida in questo settore. Proprio in quell'anno raggiungeva la piena operatività il Cyber Command, la struttura militare nella quale nel 2009 Washington aveva fuso le disparate unità cibernetiche delle proprie Forze armate. Da quel momento, gli investimenti in questo ambito (non solo sulle capacità difensive, va specificato) hanno cominciato a essere contate nell'ordine dei miliardi di dollari e il personale dedicato è più che quadruplicato. E benché l'America sia riluttante ad ammetterlo pubblicamente, non è una coincidenza che dopo questi sviluppi istituzionali la Cina abbia praticamente copiato il piano a stelle e strisce, promettendo di unificare tutte le proprie capacità e i propri guerrieri cibernetici in una sola struttura e di stanziare massicce risorse finanziarie.

La Russia figura in tutte le analisi non tanto a causa delle dichiarazioni formali in tal senso da parte dei governi cinese e americano, ma in virtù delle crescenti prove dirette e circostanziali della sua volontà di trattare l'arma cibernetica alla stregua di qualunque altro tradizionale strumento bellico o di politica estera. Per rendersene conto, basta osservare quanto fatto in Estonia nel 2007, in Georgia nel 2008, in Ucraina dal 2014 e nelle elezioni presidenziali negli Stati Uniti nel 2016. L'ironia di tanto attivismo è che l'attore che in questo campo sembra più determi-

nato a mantenere l'attuale livello di segretezza sui propri sviluppi e investimenti cibernetici non è stato altrettanto in grado di cancellare le proprie tracce quando ha effettivamente usato tali strumenti nell'arena mondiale.

Questo paradosso – tale solo all'apparenza – ci porta di fronte a uno dei maggiori tratti che distinguono le cinque potenze elencate in partenza. Quattro di esse sono relativamente trasparenti sull'importanza del potere cibernetico, ma sono altrettanto intente a farne uso in segreto. La Russia, invece, non è per nulla trasparente, ma ha sempre finito per esporle in pubblico quando le ha impiegate a sostegno dei propri interessi.

Per molti versi, Israele può essere considerato la potenza più silenziosa del quintetto: in pochi tendono a riconoscere non solo l'aggressività di Gerusalemme nell'erigere la propria strategia difensiva attorno a capacità cibernetiche offensive, ma anche il fatto che allo Stato ebraico pertenga il 10% delle vendite mondiali di computer e tecnologie di sicurezza delle reti. Infine, il Regno Unito figura nella lista in gran parte a causa di due considerazioni. Primo, gli intensi e stretti legami politici con gli Stati Uniti e con Israele. Secondo, le enormi somme investite nell'incrementare i propri strumenti cibernetici nello scorso decennio, fino a essere senza dubbio indicato come lo specialista europeo del settore.

2. Se non c'è molto dibattito su chi faccia parte del quintetto di vertice, si può invece discutere su come ordinarne i membri in base alla sofisticatezza dei rispettivi arsenali cibernetici. Inevitabilmente, il livello di segretezza che li circonda costringe in parte questo esercizio al livello delle congetture. Tuttavia, alla base di una possibile classifica c'è un importante elemento che viene spesso sottovalutato in Occidente: l'elettrico clima politico che si genera attorno all'uso del potere cibernetico.

Gli Stati Uniti mantengono una linea molto delicata e forse leggermente ipocrita: dichiarano l'intenzione di conservare il dominio in questo campo su tutti gli altri paesi, investono cospicuamente nelle armi offensive potenzialmente più letali, eppure non vogliono che gli altri paesi si preoccupino di tale preminenza. Per esempio, la principale divisione cibernetica del panorama delle spie a stelle e strisce, la National Security Agency (Nsa), possiede un gigantesco quartier generale a Fort Meade che non è solo armato, ma dispone della propria forza di polizia indipendente. Il numero degli impiegati al suo interno equivale a una piccola città. Questa burocrazia si accresce sempre più col passare del tempo, tanto che l'Nsa ha recentemente unito le proprie forze con quelle del già menzionato Comando cibernetico. Le rivelazioni dello scandalo Snowden hanno anche dimostrato che l'agenzia non disdegnerebbe che Internet fosse trasformato in un enorme campo di battaglia, con i soli Stati Uniti a godere di un autentico dominio su questo nuovo territorio. La stessa organizzazione ha quantomeno dato il via ad alcuni programmi volti a impiegare i metadati intercettati per scopi spionistici «non intrusivi» nei confronti dei propri connazionali.

Il punto è che la postura cibernetica americana, sia in termini strategici che operativi, è presumibilmente la più aggressiva al mondo. Ma le critiche in tal senso

sono mute se paragonate a quelle che si levano contro due bersagli ricorrenti come la Cina e la Russia. Certo, questi due attori non se ne stanno con le mani in mano e sono molto attivi nell'utilizzo del potere cibernetico per avanzare i propri interessi e avvantaggiarsi in diverse partite. Mosca si è concentrata molto di più sui risultati politici e militari delle proprie missioni cibernetiche; mentre Pechino si è rivelata l'indiscusso campione dello spionaggio economico, del furto di proprietà intellettuale e dell'ingegneria inversa per acquisire la tecnologia necessaria a competere sui mercati globali. Ma qui non si tratta di scagionare l'operato dei due Stati né di ridimensionare la portata delle loro operazioni. È invece affascinante notare quante poche critiche vengano riservate agli Stati Uniti mentre questi ultimi si assicurano la più avanzata e paralizzante forza cibernetica del pianeta. La narrazione americana funziona più o meno come segue: «Ci stiamo dotando delle armi necessarie a disincentivare comportamenti cibernetici criminali da parte di altre nazioni». Davanti a questa argomentazione potrebbe non essere corretto dimostrarsi del tutto scettici. Tuttavia, è innegabile come la potenza statunitense stia anche spingendo paesi come Cina, Russia e Iran a cercare di compensare le capacità di Washington. L'ostinata ricerca da parte dell'America di tutto ciò che la conservi come il dominante poliziotto cibernetico del mondo potrebbe dunque stare approfondendo una competizione globale per sviluppare armi sempre più raffinate.

Quando si osservano il ruolino di marcia e le capacità degli Stati Uniti in questo settore, c'è davvero da meravigliarsi che non ci si preoccupi di più degli obiettivi manifesti di Washington. Consideriamo tre aspetti.

Primo. Lontano dai riflettori, l'America ha aggressivamente cercato di dare alle proprie armi cibernetiche una più spiccata componente offensiva. Stuxnet, il virus lanciato contro le centrifughe nucleari iraniane, è stato solo il primo, piccolo tassello di questo mosaico ed è estremamente probabile che gli siano succeduti *malwares* molto più affilati.

Secondo. Non importa quanti altri paesi investano nello sviluppo delle proprie forze cibernetiche. La loro somma comunque impallidisce se paragonata a quanto gli americani spendono ogni anno in questo ambito. È dunque corretto affermare che gli Stati Uniti non stanno davvero competendo con altri Stati in termini di pianificazione strategica di lungo periodo: proprio come nell'iniziale fase di sviluppo dell'arsenale nucleare, Washington non vuole che ci sia alcun dubbio su chi sia in grado di intraprendere operazioni cibernetiche unilateralmente nel momento ritenuto necessario e senza temere di pagare un gran prezzo.

Terzo. La sfacciataggine con cui gli Stati Uniti hanno condotto operazioni di spionaggio cibernetico, campagne di «influenza maligna» e intercettazioni in giro per il modo – a volte pure contro paesi tecnicamente alleati o «amici» come Germania e Messico – è finito sulle prime pagine di tutti i media e ha causato una discreta dose di imbarazzo pubblico. Tutto ciò non ha alcun impatto sulle future operazioni, ma fa venire al resto del pianeta più di un dubbio quando Washington punta il dito contro altri Stati per aver orchestrato missioni simili contro il territorio o soggetti americani. Cina, Russia, Corea del Nord, Iran, pure Israele

hanno subìto accuse del genere negli ultimi anni. Nelle conferenze globali a cui non partecipano relatori statunitensi la lamentela più comune è diretta contro questo smaccato doppiopesismo.

La Cina sta molto attenta a rivolgere tali critiche a Washington, probabilmente perché non vuole attirare su di sé ancor più attenzione di quanta già non ne ricevano le sue attività economiche in ambito cibernetico. Non è invece il caso della Russia, che alza sempre la voce e si schiera in prima fila per accusare gli americani di dire una cosa e fare l'esatto contrario. Per i russi, gli Stati Uniti sono di gran lunga la più aggressiva ciberpotenza del pianeta e rifiutano seccamente la narrazione secondo cui nessuno dovrebbe preoccuparsi delle politiche cibernetiche americane perché sono generalmente volte al bene del mondo. Va sottolineato come né Mosca né Washington si stiano impegnando a contenere le proprie capacità o a dare il la a una convenzione internazionale volta a sviluppare norme per il ciberspazio che limitino equamente il ricorso a questo strumento. Al contrario, i due attori combattono per il modo in cui i rispettivi stili cibernetici vengono caratterizzati: gli americani non vogliono essere criticati e pretendono il beneficio del dubbio; i russi vorrebbero che il mondo riconoscesse che essi fanno esattamente ciò che fanno gli Stati Uniti nell'ombra.

3. Se dunque si rimuove dall'equazione il modo in cui i vari attori si atteggiano pubblicamente, è sufficiente ammettere che le potenze del quintetto sono attive nel ciberspazio per scopi buoni e meno buoni, ma sempre per il proprio esclusivo interesse.

In quest'ottica, gli Stati Uniti sono l'hacker superpotente: hanno tutto il denaro, il talento, la motivazione per dominare questo territorio e la posizione in cui si trovano non li spaventa affatto. La Cina è l'hacker economico, principalmente intenta ad aumentare la propria posizione relativa nel sistema economico globale. Anche se ciò non vuol dire che il suo raggio di azione si fermi all'ambito pecuniario. Per esempio, benché lo neghi ufficialmente, è opinione corrente negli Stati Uniti che la Repubblica Popolare abbia hackerato le Forze armate a stelle e strisce sottraendo i piani dell'F-35. Un furto che, stando ai militari americani, ha direttamente portato allo sviluppo del caccia cinese J-31. Come spesso accade in questo mondo, non esistono pistole fumanti, ma le prove circostanziali suggeriscono fortemente questa conclusione.

La Russia, invece, è l'hacker politico spavaldo che, come del resto in altri campi, cerca di vedersi riconosciuta la propria ciberpotenza. In quest'ottica, quando Mosca nega il coinvolgimento nei sabotaggi di Estonia, Georgia e Ucraina non lo fa per reclamare la propria innocenza, ma per rifiutare ogni tipo di critica: quando è impegnato in un conflitto – prosegue il ragionamento – uno Stato ha il diritto di impiegare qualunque strumento abbia a propria disposizione. Secondo questa interpretazione, la natura delle relazioni internazionali è sempre stata così e tale deve rimanere. Dunque, per i russi, la potenza cibernetica non è qualcosa a sé stante, ma semplicemente un'estensione di ciò che già esiste.

Per converso, il Regno Unito tende a essere qualificato come l'hacker guardingo, molto qualificato nel raccogliere importanti volumi di informazioni ma non particolarmente portato ad agire di conseguenza. La caratterizzazione va presa con le pinze: vista la già menzionata vicinanza agli Stati Uniti e a Israele, il fatto che i britannici non impieghino attivamente le informazioni che rastrellano non significa che quelle informazioni non vengano impiegate da altri.

Il che ci porta appunto a Israele, l'hacker geopolitico, eminentemente preoccupato dall'uso delle capacità cibernetiche per proteggersi dal livello di ostilità e aggressività proprio della regione in cui sorge. La trasformazione della Rete in un campo di battaglia ha aggiunto nuove tensioni e requisiti difensivi per lo Stato ebraico, soprattutto nella sua sfida con l'Iran. Stuxnet è un perfetto esempio di come Gerusalemme impieghi strumenti cibernetici in modo collaborativo: benché il virus sia stato realizzato dall'Nsa americana, sono stati gli israeliani ad assicurarsi che esso raggiungesse la destinazione prefissata e distruggesse le centrifughe della centrale nucleare di Natanz.

La Corea del Nord merita una negativa menzione d'onore, in qualità di hacker aggressivo e disperato, essendosi per anni appoggiata a capacità cibernetiche che tutto sommato avanzate per riempire le proprie vuote casse – essere bollati come Stato canaglia ha un costo. Si stima che il 10-15% delle sue riserve di valuta estera provengano direttamente da attività cibernetiche illegali. Il furto da 81 milioni di dollari alla banca centrale del Bangladesh, l'intrusione nella Sony, l'infame attacco *ransomware* WannaCry (ironicamente frutto di un'arma rubata all'Nsa) è emblematico di quale sia l'attuale scopo dei talenti cibernetici coltivati a P'yŏngyang. È anche il motivo per cui i nordcoreani non figurano nella lista delle ciberpotenze mondiali: fintanto che il loro status internazionale rimarrà inalterato, è probabile che i loro sforzi nella Rete resteranno a un livello criminale, senza sfociare negli intrighi politici.

4. Sin qui ci siamo concentrati sulle sottigliezze e sfumature da adottare per avere un quadro più chiaro del quintetto delle ciberpotenze. Per concludere occorre però gettare uno sguardo sulle ricerche in corso che stanno provando a sviluppare idee più chiare su che cosa ci sia al di là di questi cinque attori. La İstanbul Teknik Üniversitesi (Itu) ha recentemente pubblicato una delle analisi sin qui più complete in tal senso, volta a valutare e categorizzare sistematicamente l'intero ciberspazio adottando le lenti del potere politico [1]. La Itu ha impiegato una matrice a 11 entrate per stabilire tre attributi del possesso e della proiezione del potere cibernetico: difesa, attacco e dipendenza. I paesi sono stati classificati in base alle seguenti variabili e valutazioni:

- bilancio cibernetico allocato alle Forze armate;
- spesa militare complessiva;

1. B. Çeliktaş, N. Ünlü, «Cyber Security Power Ranking by Country and Its Importance on World Politics», *The Journal of Academic Social Science Studies*, n. 67, primavera 2018, pp. 469-488.

- classifiche di sviluppo tecnologico;
- Global Cybersecurity Index;
- rapporto McAfee sulla difesa cibernetica;
- tasso popolare di impiego di Internet;
- classifiche di sviluppo delle industrie di software;
- traffico di attacchi cibernetici.

Impiegando tanti dati provenienti da ambiti così diversi del potenziale cibernetico di uno Stato, gli studiosi sono stati in grado di produrre una categorizzazione delle ciberpotenze che finalmente va oltre le tipiche valutazioni concentrate sul quintetto discusso finora. Nonché oltre l'abusata distinzione fra queste cinque potenze e gli attori cibernetici «canaglia» sia statali che non – un calderone di casi di studio in cui solitamente finiscono sia uno Stato come la Corea del Nord sia gruppi come lo Stato Islamico.

Così concepita, la potenza cibernetica si suddivide in quattro livelli.

- Livello 1: Usa, Cina, Russia.
- Livello 2: Francia, Regno Unito, Israele.
- Livello 3: India, Corea del Sud, Corea del Nord, Germania, Turchia.
- Livello 4: Brasile, Canada, Italia, Giappone, Iran.

L'aspetto forse più impressionante è che lo studio si spinge persino a classificare individualmente i paesi a seconda dei vari gruppi di dati interrogati. Ciò ci permette di considerare la profondità, l'adattamento, il cambiamento e la diversità dei vari attori, laddove in precedenza l'analisi era piuttosto statica e monotona. Ricerche come queste stabiliscono inoltre che il potere cibernetico sul palcoscenico mondiale è destinato a diventare sempre più contestato e la lotta per accaparrarselo sarà sempre più convulsa. Il che, onestamente, non può essere ritenuto uno sviluppo positivo. Il quintetto classico delle potenze si è fin qui meritato l'attenzione dell'opinione pubblica, ma questo scrutinio deve essere urgentemente espanso, poiché senza dubbio un numero maggiore di concorrenti farà presto il proprio ingresso in grande stile in quest'arena. Anche se un dato sembra essere immutato: nel futuro prossimo, il bullo più grosso e più cattivo in ambito cibernetico resterà l'America.

(traduzione di Federico Petroni)

GEOPOLITICA DELLA PROTEZIONE

di *Alessandro Aresu*

Gli Stati Uniti si attrezzano per vincere la guerra fredda tecnologica con la Cina. L'Internet delle cose allarga la sfera delle infrastrutture da proteggere: compito dello Stato. Il Cfius e la lotta alla penetrazione cinese nello hardware. L'Ue è out, la Francia no.

Se avete qualcosa di
davvero importante da dire,
scrivetelo a mano.
Donald J. Trump

1. «Protezione» è un concetto di alto rilievo geopolitico. Il capitano Mahan lo adopera sovente nei suoi scritti. Con la maiuscola, *Protection* è l'uso strumentale o strategico del protezionismo commerciale. La protezione riguarda anche, nella sua articolazione marittima, l'approccio verso le stazioni navali, ottenute attraverso l'occupazione militare o il consenso della popolazione.

Così come il commercio non ha un'esistenza separata dalle dinamiche geopolitiche, lo stesso accade per la tecnologia, che sarebbe senz'altro oggetto degli scritti di un Mahan contemporaneo. La geopolitica della protezione [1] è la prosecuzione della guerra economica [2] in un'arena tecnologica più matura. Identifica tre categorie: a) la protezione dei cittadini dalla tecnologia, per orientarne e limitarne lo sviluppo; b) le contrattazioni delle grandi imprese tecnologiche con gli Stati; c) gli strumenti con cui gli Stati, nei loro organismi nazionali o nel contesto internazionale, sviluppano e favoriscono strumenti, normativi e militari, di controllo degli investimenti, in particolare in ambiti ad alta tecnologia.

2. La prima categoria, la protezione dalla tecnologia, pone davanti una questione di sopravvivenza: cosa faremo se la «Provvidenza tecnologica» abolirà la

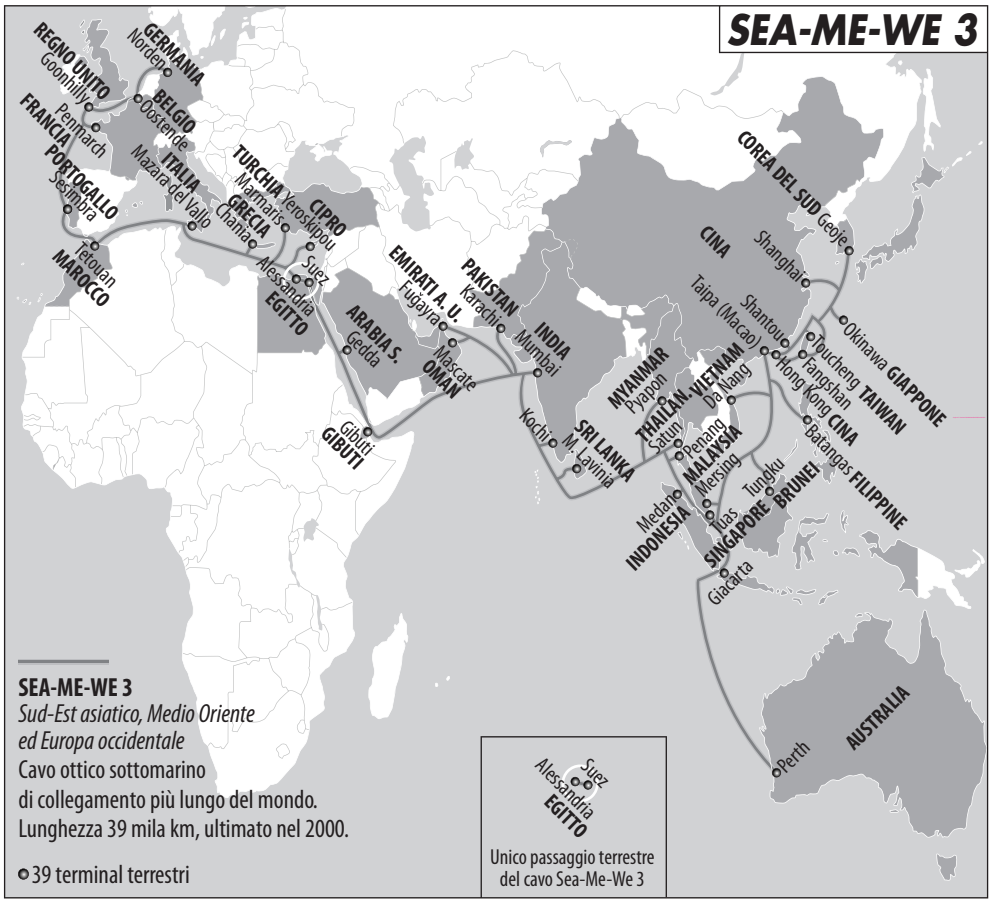
1. Riprendo qui i ragionamenti sviluppati in A. Aresu, M. Negro, *Geopolitica della protezione. Investimenti e sicurezza nazionale: gli Stati Uniti, l'Italia e l'UE*, Fondazione Verso l'Europa, novembre 2018. Il volume sviluppa questi argomenti attraverso l'analisi estesa della normativa relativa al Cfius.
2. Sulla guerra economica, si vedano i saggi raccolti in *Economic Warfare. Storia dell'arma economica*, a cura di V. Ilari e G. Della Torre, Quaderno Sism 2017. Sull'intelligence economica, sempre utile il documento pionieristico di P. Savona, «Presupposti, estensione, limiti e componenti dell'organizzazione dell'intelligence economica», *Per aspera ad veritatem*, n. 15, 1999, pp. 1023-1033.

geopolitica? L'interazione tra tecnologia e geopolitica non è nuova. Il primato mondiale degli Stati Uniti si lega allo sviluppo e all'uso strategico di mezzi scientifici e tecnologici. Secondo un preciso obiettivo: la «frontiera infinita» della tecnologia è figlia della frontiera americana. E con una nota implicita: l'infinito deve riguardare Washington, mentre agli altri deve essere precluso. Questo scenario tecnologico si trova in accelerazione. Lo sviluppo cibernetico diffonde ed estende le capacità di attacco [3], e quindi si interseca coi conflitti già esistenti. La dimensione spaziale è sempre presente nell'èra della Rete, perché «l'accesso e la fruizione dei servizi di Internet passa necessariamente attraverso l'utilizzo e l'installazione di un'infrastruttura fisica che permette la connessione dei diversi apparati» [4]. Tuttavia, l'immaginazione della fantascienza ci aiuta a gettare il cuore oltre l'ostacolo, eliminando il fattore umano. Cosa accadrà quando il pianeta, dopo la classica *robocalypse* (apocalisse robotica), sarà controllato da entità robotiche avanzate? Nel caso in cui l'umanità sopravviva, per esempio in una resistenza volta a colpire le strutture fisiche dei robot padroni, allora la geopolitica continuerà a esistere. Nel caso in cui l'umanità non sopravviva, la geopolitica non ci sarà più. Questa stessa rivista, sopravvissuta per il divertimento dei successori dell'umanità, sarà scritta da diverse voci dell'intelligenza artificiale.

Il dibattito sull'approssimarsi dell'apocalisse indotta dalla tecnologia è vasto. Include futurologi, regolatori, imprenditori e ciarlatani. Spazia da chi sottolinea la nostra distanza da «Terminator» a chi, come il fondatore di SpaceX e Tesla, Elon Musk, ritiene l'intelligenza artificiale la nostra fondamentale minaccia esistenziale. Musk invoca una maggiore regolazione, nazionale e internazionale, per proteggere l'umanità [5]. I programmi degli Stati sulla cibersicurezza sono, in questo senso, elementi di geopolitica della protezione. Il primo pilastro della strategia cibernetica dell'amministrazione Trump è «Protect the American People, the Homeland, and the American Way of Life» [6]. Non è detto, tuttavia, che la protezione non possa applicarsi a opzioni più estreme. Durante i festeggiamenti per il Capodanno 2017, l'allora presidente eletto Trump, interrogato sulla cibersicurezza, suscitò le risate degli specialisti. Semplice e diretto, come sempre, il lessico della sua «dottrina»: nessun computer è sicuro, se avete qualcosa di davvero importante da dire fate alla vecchia maniera, scrivete a mano e trovate un corriere, uno di fiducia. Lo scetticismo di Trump deriva dalle sue preferenze personali, da una dieta tecnologica in cui imperano le telefonate, Twitter e soprattutto la televisione (o le telefonate davanti alla televisione), ma non è previsto l'uso del computer.

Eppure, le parole di Trump pongono una questione di geopolitica della protezione: la recessione tecnologica. Il passaggio principale della discontinuità tecno-

3. Su questi aspetti, si veda B. Wittes, G. Blum, *The Future of Violence: Robots and Germs, Hackers and Drones – Confronting a New Age of Threat*, New York 2015, Basic Books.
4. P. Cellini, *La rivoluzione digitale. Economia di internet dallo Sputnik al machine learning*, Roma 2018, Luiss University Press, p. 144.
5. Le affermazioni di Elon Musk al Mit nel 2014 sono disponibili presso l'accurata sezione «Transcripts» del sito Shit Elon Says, goo.gl/5qESMZ
6. *National Cyber Strategy of the United States of America*, settembre 2018.



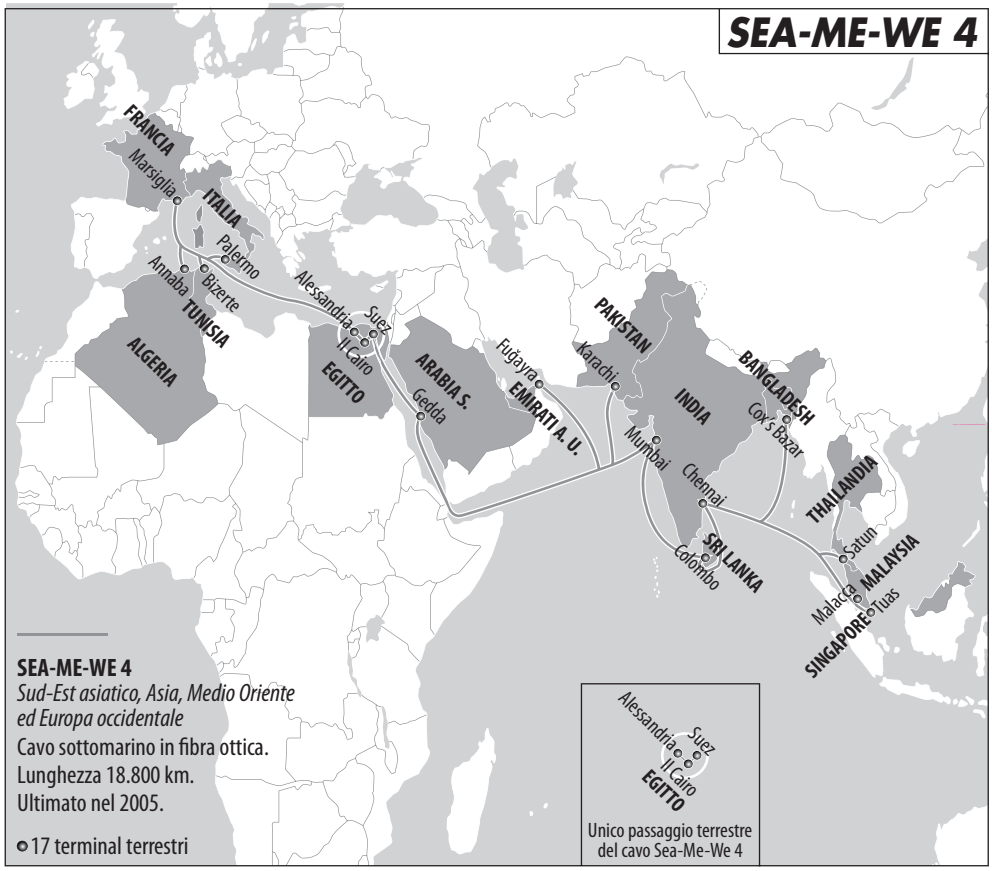
logica in corso è che l'Internet delle cose rende «critiche» infrastrutture che prima non lo erano. La connettività può riguardare gli elettrodomestici e i mezzi di trasporto, oltre alle infrastrutture dei servizi pubblici e i sistemi di sicurezza privati. Ciò aumenta la vulnerabilità di ogni sistema con cui gli uomini si interfacciano. lato, come vedremo, questo porta ad allargare le maglie della cosiddetta «sicurezza nazionale», fornendo nuove modalità di intervento degli Stati e di esercizio della sovranità. Dall'altro, o crediamo che il processo in corso sia inevitabile, e quindi non crediamo alla libertà umana, oppure possiamo pensare alla riduzione dei rischi. Il crittografo Bruce Schneier, che invece di «Internet delle cose» utilizza l'espressione «Internet+», per sottolineare che ogni cosa è Internet, suggerisce che alla fine della «luna di miele» della computerizzazione e della connettività ci sarà una reazione. La reazione, secondo Schneier, non «sarà guidata dal mercato, ma da norme, leggi e decisioni politiche che mettano la sicurezza e il benessere della società sopra gli interessi delle aziende e delle industrie. Ci sarà bisogno di un forte cambiamento sociale, che per alcuni sarà difficile da digerire, ma la nostra sicu-

rezza dipende da questo»[7]. Le analogie presentate da Schneier, l'energia nucleare e l'avionica, indicano l'importanza di erigere forti standard di regolazione e, se necessario di disconnessione. Agli attori geopolitici resta il loro compito storico: governare la sicurezza, attraverso la violenza della legge e delle armi. È un compito che alcuni possono esercitare, anche l'uno contro l'altro. La lezione di Max Weber sul potere non è superata, bensì approfondita dallo sviluppo tecnologico, che pone con più urgenza la solita domanda di fondo: chi esercita il monopolio della violenza legittima? E chi lo esercita nel numero due e nel numero uno della «frontiera infinita», la Cina e gli Stati Uniti?

3. L'ascesa cinese degli ultimi quarant'anni può essere raccontata anche come un rilancio scientifico-tecnologico. Inserendo, nel 1978, la scienza e la tecnologia (al fianco di agricoltura, industria e difesa) tra le «Quattro Modernizzazioni», Deng certificò un'azione già portata avanti nella seconda metà degli anni Settanta per migliorare il rapporto tra il Partito comunista cinese e gli scienziati, nonché per avviare relazioni e scambi in materia scientifica e tecnologica con il Giappone e gli Stati Uniti[8]. Nella visione cinese di lungo periodo della storia, il «secolo di umiliazione» della Cina è legato anche al ritardo tecnologico rispetto alle potenze coloniali europee e alla capacità nipponica di utilizzare le capacità occidentali come fattore di potenza. Il ritorno della Cina all'altezza della sua storia e della sua demografia passa per un recupero definitivo di questo ritardo. Il Partito comunista cinese non cela questa consapevolezza. Nello straordinario discorso di Xi Jinping agli scienziati e ingegneri nel 2014[9], si ripercorrono tutti i fattori della potenza tecnologica cinese: il primato robotico, il suo uso industriale, il «completamento» della modernizzazione con caratteristiche cinesi attraverso la crescita delle pubblicazioni scientifiche, dei brevetti e della forza lavoro impiegata nei centri di ricerca.

Secondo la leadership cinese, non è mai sufficiente fornire un elenco di risultati e di tecnologie chiave. Bisogna partire dalla profondità storica. Xi riprende il grande problema della civiltà cinese: il momento in cui la scienza e la tecnologia dell'Impero del Centro, tra la fine della dinastia Ming e l'inizio della dinastia Qing, sono rimasti drammaticamente indietro. Xi ricorda l'interesse dell'imperatore Kangxi per la scienza e le tecnologie occidentali e ne trae due lezioni. La prima è la scarsa visibilità e diffusione nella società di questi interessi, rappresentati dalla reclusione del grande atlante fatto realizzare da Kangxi. Bisogna combattere la tendenza a tenere la scienza come un segreto o un hobby, perché ciò indebolisce il suo uso come fattore di potenza. «Le conoscenze, per quanto ricche, non pos-

7. B. Schneier, *Click here to Kill Everybody*, capitolo «What a Secure Internet+ Looks Like», New York-London 2018, W.W. Norton & Company.
8. Per gli obiettivi di Deng Xiaoping in materia, si veda E. Vogel, *Deng Xiaoping and the Transformation of China*, Cambridge MA 2011, Harvard University Press.
9. Xi Jinping, «Accelerare la transizione da un modello di sviluppo basato su fattori produttivi e investimenti a un modello basato sull'innovazione», 9/6/2014, in Id., *Governare la Cina*, Firenze 2016, Giunti Editore, pp. 147-161. Estratti del discorso sono disponibili anche nel sito dell'Associazione Stalin, nella sezione «La Cina oggi: ben scavato vecchia talpa?», goo.gl/X17yBh



sono influenzare la società reale se sono archiviate come curiosità, interessi raffinati, o addirittura come abilità peculiari»[10]. Le «truppe degli scienziati e dei tecnici»[11] cinesi debbono sentirsi parte di un tutto armonioso. Un sistema aperto, nel senso di tessuto dal Partito e da esso collocato nelle vene della società cinese. La seconda lezione riguarda l'affidamento delle scoperte e delle innovazioni ai missionari stranieri. A redigere l'atlante di Kangxi sono stati i gesuiti francesi, e Xi è lieto di continuare il dialogo con i gesuiti, di ricordare i Matteo Ricci e i Matteo Ripa, di intensificare il dialogo industriale con le altre nazioni, anche attraverso l'acquisizione di aziende strategiche. Ma l'Impero del Centro deve essere più ambizioso. Deve imparare a fare da solo, perché la logica della scoperta e la logica della sicurezza sono intessute: «Solo padroneggiando pienamente le tecnologie chiave è possibile impadronirsi del potere d'iniziativa nella concorrenza e nello sviluppo e garantire la sicurezza economica nazionale, la sicurezza della difesa nazionale e la sicurezza in altri ambiti. Non è sempre possibile fregiare il proprio futuro con i traguardi del passato altrui, né far sempre affidamento sugli altrui

10. *Ivi*, p. 155.
11. *Ivi*, p. 159.

traguardi per elevare il proprio livello tecnico-scientifico; ancor meno possibile fare da appendice tecnologica di altri Stati. Non possiamo essere sempre un passo indietro agli altri, imitandoli pedissequamente. Non abbiamo altra scelta: dobbiamo perseguire l'innovazione autonoma» [12].

Questo concetto di innovazione, non sottoposto a regole, leggi o influenze altrui, regge l'estensione del dominio della sicurezza, sotto la guida del Partito e sotto il principio di *junmin ronghe*, la fusione tra militare e civile. In Cina «i settori dello shipping e delle telecomunicazioni hanno compiuto sviluppi continui nella ricerca, nello sviluppo e nella produzione, attraverso il loro inserimento nell'economia internazionale. Queste capacità tecnologiche sono state convertite in nuove capacità militari» [13]. Il tredicesimo piano quinquennale, con il programma Made in China 2025 e gli investimenti in intelligenza artificiale, rientrano nella logica esposta dal presidente cinese. Le grandi imprese digitali cinesi, come Alibaba, Huawei, Baidu, Tencent, Zte, Ztt, Ftt, non possono muoversi senza l'ombrello del Partito e del suo pensiero strategico. Illustrano l'inconsistenza dell'illusione occidentale di una classe media cinese in contrasto col Partito. Se Jack Ma vuole produrre semiconduttori [14], è incoraggiato a farlo. Se Jack Ma vuole andare in spiaggia a godersi la vita, può farlo. Se Jack Ma vuole agire contro gli obiettivi del Partito, non può farlo.

L'investimento cinese in infrastrutture è volto a portare all'estero capitali e a costituire un presidio fisico – in alcuni casi, anche con potenzialità militari, come per esempio nei porti o della realizzazione di basi – della potenza cinese. L'investimento in infrastrutture non si limita alle autostrade, alle ferrovie, ai porti e agli aeroporti, ma può riguardare anche le reti elettriche, le reti di telecomunicazioni e tutte le infrastrutture relative alla trasformazione digitale. Con «Industria 4.0» e con la realizzazione di catene del valore digitali, le stesse strutture industriali sono parte integrante di una più vasta infrastruttura. Parafrasando Schneier, una Internet+ con caratteristiche cinesi, che mette a frutto a livello domestico la grande disponibilità di dati posseduti dal Partito, e a livello internazionale i punti di accesso delle infrastrutture su cui la Cina si estende. Punti di accesso per obiettivi geopolitici: come gli Stati Uniti hanno utilizzato la politica della porta aperta (*open door policy*) nel commercio all'epoca di Mahan, oggi i cinesi sono accusati di utilizzare la politica della *backdoor* (*backdoor policy*), per superare le difese dei dispositivi e dei sistemi informatici, anche attraverso la componentistica hardware [15].

Dati e luoghi costituiscono insieme la collana di perle delle «vie della seta digitali». Pensiamo al progetto Peace (*Pakistan & East Africa Connecting Europe*), il

12. *Ivi*, pp. 151-152.
13. A. Segal, *Chinese Technology Development and Acquisition Strategy and the U.S Response*, dichiarazione allo House Committee on Financial Services, Monetary Policy and Trade Subcommittee, 12/12/2017, goo.gl/zAKwvv
14. A. Minter, «Why Can't China Make Semiconductors?», *Bloomberg*, 30/4/2018, goo.gl/QB7Y1b
15. Questa è l'accusa riportata tra l'altro da un'inchiesta di *Bloomberg* e respinta dalle imprese americane, in J. Robertson, M. Riley, «The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies», *Bloomberg*, 4/10/2018, goo.gl/JoDKGm

sistema di 12 mila chilometri di cavi con cui Hengtong e Huawei puntano a unire l'Asia, l'Africa e l'Europa. Come ricordano gli storici, «i cavi sottomarini che hanno connesso i continenti, cancellando le distanze oceaniche, furono il genere di miracoli moderni che hanno ispirato la fantascienza di Verne» [16]. Tuttavia, gli oceani non sono stati «annullati» dalla connessione dei cavi sottomarini. Al contrario, la loro connessione ha accentuato il rilievo del controllo degli oceani sul piano militare. La vulnerabilità dei cavi e la loro riparazione sono infatti all'attenzione della Marina militare statunitense, come il pericolo che altre potenze, a partire da Cina e Russia, possano attentare alla sicurezza dei cavi, in cui passa circa il 97% delle comunicazioni globali [17]. Per esempio, in uno scenario di conflitto su Taiwan, si può immaginare una strategia mirata di Pechino per escludere l'isola dalle comunicazioni, tagliando i cavi sottomarini.

Tutte le questioni sopra descritte non generano l'abrogazione della geopolitica da parte della tecnologia, ma una dinamica di conflitto e negoziazione. Il suo effetto è l'allargamento dei concetti di «sicurezza nazionale» e «infrastrutture critiche» per le potenze che possono permetterselo. Su questa base possiamo leggere i rapporti geopolitici con le grandi imprese digitali, creature ambigue, che non vanno né esaltate con presunzioni di onnipotenza («Nick Clegg dirige gli affari internazionali di Facebook, quindi è l'uomo più potente del mondo!») né ridotte a radice dei mali del mondo. Più utile coglierne il segno geopolitico e i rapporti coi governi.

Prendiamo Amazon, una creatura ormai matura, entità di grande interesse, sul cui destino negli Stati Uniti si è sviluppato un nuovo dibattito antitrust, soprattutto grazie ai lavori di Lina Khan. Al contrario della Compagnia delle Indie Orientali, Amazon non possiede un esercito propriamente detto. Dispone tuttavia di un esercito di utenti, più vasto di qualunque forza militare, e può creare un esercito di lobbisti. Per operare, nell'e-commerce come nel *cloud*, ha bisogno di spazi, di luoghi. Per parafrasare il complesso industriale-militare di Eisenhower, Amazon è un complesso tecnologico-logistico. La sua nuvola ha una struttura fisica e deve radicarsi nei luoghi per alimentarsi. Se vuole inserire lo spazio nella sua Rete (ed è una grande passione di Bezos con Blue Origin), ha bisogno di ottenerne l'accesso da parte del governo americano, altrimenti nello spazio non ci può andare. L'estensione del potere di Amazon richiede una contrattazione continua con gli apparati degli Stati Uniti. Le spese di lobbying sono aumentate del 400% dal 2012 a oggi [18].

Cruciali sono i rapporti tra i servizi di *cloud* di Amazon e il governo della difesa e della sicurezza. Sean Roche, vicedirettore dell'innovazione digitale della

16. S.C. Topik, A. Wells, «Commodity Chains in a Global Economy», in *A World Connecting (1870-1945)*, a cura di E. Rosenberg, Cambridge Ma 2012, The Belknap Press of Harvard University Press, p. 664.
17. È un tema affrontato in R. Sunak, *Undersea Cables. Indispensable, Insecure*, Policy Exchange, 2017, goo.gl/rAoZJE
18. S. Soper, N. Nix, B. Allison, «Amazon's Jeff Bezos Can't Beat Washington, so He's Joining It: The Influence Game», *Bloomberg*, 14/2/2018, goo.gl/MSSBGc

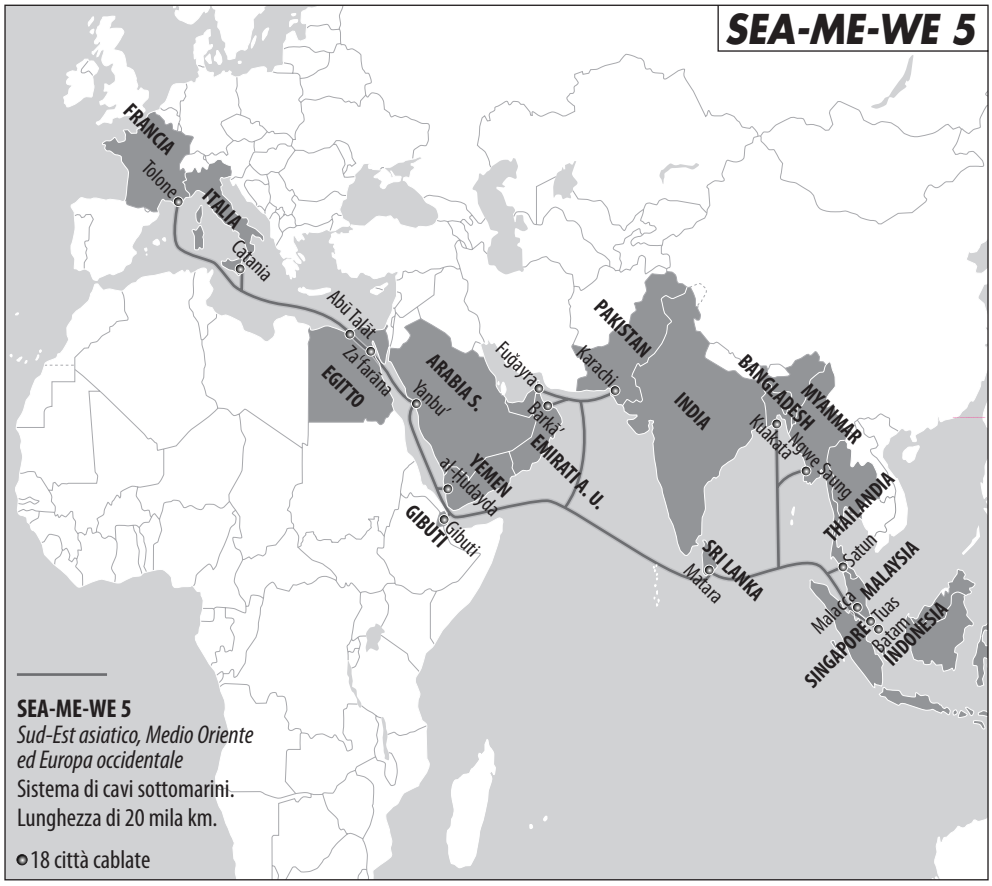
Cia, ha lodato la collaborazione tra Amazon e l'agenzia, cementata da un contratto del 2013. La prima slide della sua entusiastica presentazione al summit organizzato nel giugno 2018 a Washington da Amazon è un ringraziamento a Amazon Web Services [19]. Jeff Bezos in persona è intervenuto per difendere il coinvolgimento di Amazon con il Pentagono, e in particolare con il contratto Jedi (Joint Enterprise Defense Infrastructure) da 10 miliardi di dollari per il *cloud* del dipartimento della Difesa [20]. Nel 2016, Bezos ha attaccato Peter Thiel per il suo sostegno a Trump, ma Amazon Web Services fornisce servizi per Palantir, l'azienda cofondata da Thiel che supporta l'agenzia Ice (Immigration and Customs Enforcement) per l'attuazione delle politiche di controllo dell'immigrazione dell'amministrazione Trump [21].

4. Se esiste una guerra fredda tecnologica, una delle creature «abissali» degli apparati americani ne è un campo di battaglia. Si tratta del Cfius, acronimo che identifica il Committee on Foreign Investments in the United States, il comitato interdipartimentale del governo federale che vigila e controlla gli investimenti esteri diretti. Il Cfius è presieduto dal segretario al Tesoro e la sua attività amministrativa è gestita dal direttore dell'Ufficio della sicurezza degli investimenti del dipartimento del Tesoro.

La guerra fredda tecnologica implica un coinvolgimento sempre più marcato dei sottoapparati di sicurezza all'interno dei vari dipartimenti. Le figure che hanno una responsabilità diretta nelle operazioni del Cfius sono, come in ogni apparato, poco note e importanti. Da maggio 2018, a reggere le fila dell'apparato Cfius è Thomas Feddo, avvocato di Alston & Bird con forti credenziali nella sicurezza: laureato all'Accademia navale, tenente nei sottomarini nucleari e per sette anni in forza all'Ofac, l'agenzia che si occupa delle sanzioni economiche degli Stati Uniti. Un altro burocrate di primo piano è Brian Reissaus, già in forza durante l'amministrazione Obama e proveniente dal controllo delle politiche industriali del Defense Security Service [22].

Il Cfius è un soggetto di «geo-diritto» [23]. Nella sua storia si uniscono, fino a confondersi, considerazioni giuridiche e letture geopolitiche. La sua creazione risale a più di quarant'anni fa. È stato introdotto nell'amministrazione Ford tramite l'ordine esecutivo 11858 nel 1975, come risposta istituzionale ai risultati del Foreign Investment Study Act of 1974 [24], volto a studiare l'impatto degli investimenti esteri diretti negli Stati Uniti sulla sicurezza nazionale. La sua origine si inserisce nel di-

19. Il video è disponibile all'indirizzo www.youtube.com/watch?v=czc_r7Xzvwc
20. H. Kelly, «Jeff Bezos: Amazon Will Keep Working with the DoD, *CNN Business*, 16/10/2018, goo.gl/tVMGkZ
21. Così la lettera di un dipendente di Amazon, «I'm an Amazon Employee. My Company Shouldn't Sell Facial Recognition Tech to Police», *Medium*, 16/10/2018, goo.gl/sGq2RT. Su Thiel rimando a A. Aresu, «L'agenda di Peter Thiel», *Limes*, «L'agenda di Trump», n. 11/2016, pp. 97-103.
22. Si veda B. Reissaus, «New FOCI Collocation Review Process», in *DSS Access. Official Magazine of the Defense Security Service*, vol. 1, 3, p. 14, goo.gl/Wa8zhr
23. Si veda anzitutto N. Irti, *Norma e luoghi. Problemi di geo-diritto*, Roma-Bari 2001, Laterza.
24. Foreign Investment Study Act of 1974, Public Law No. 93-479, 26/10/1974.



battito sul «pericolo giapponese», nell'instabilità del sistema alla fine degli accordi di Bretton Woods. Negli anni Ottanta gli investimenti giapponesi negli Stati Uniti destano crescente preoccupazione, ma si dimentica che in termini geopolitici ciò rende il Giappone sempre più dipendente dagli Stati Uniti [25].

La Fujitsu nel 1986 si mostra interessata ad acquisire un'azienda storica nello sviluppo americano dei semiconduttori, Fairchild Semiconductor, dove aveva lavorato anche il genio italiano Federico Faggin. L'accordo suscita una forte opposizione nel Congresso e da parte del dipartimento del Commercio, del dipartimento della Difesa (guidato da veterani dall'amministrazione Reagan, Baldrige e Weinberger) e dell'Nsa. Baldrige, campione di rodeo che morirà tragicamente nel 1987 proprio per un rodeo, è duro nelle motivazioni. Indica che l'acquisizione avrebbe creato un effetto domino, erodendo la base tecnologica degli Stati Uniti. Inoltre, un'espansione giapponese nel mercato dei semiconduttori e dell'informatica avrebbe aumentato il deficit commerciale statunitense. Ancor più esplicito l'allora vicesegretario alla Difesa per la sicurezza del commercio Stephen Bryen:

25. G. Friedman, M. Lebard, *The Coming War with Japan*, New York 1991, St Martin's Press, p. 149.

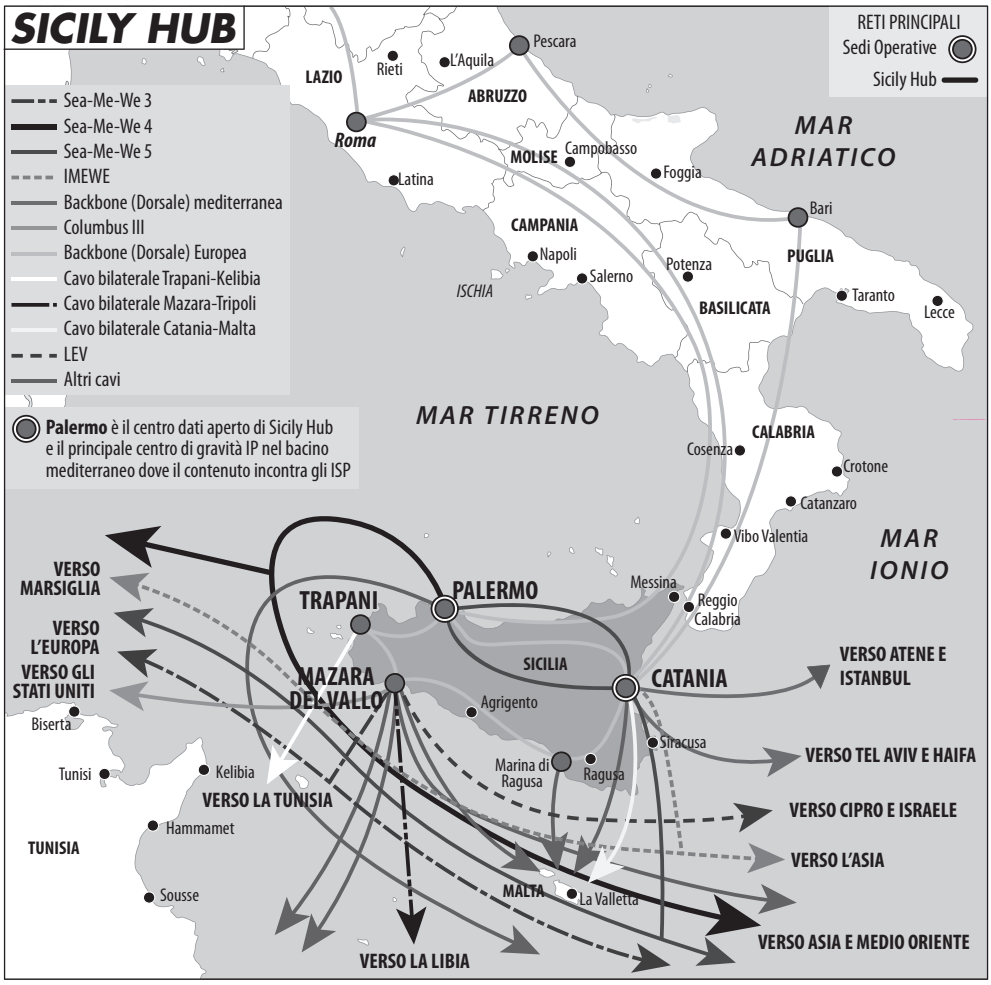
«Se una delle nostre aziende di semiconduttori giunge nelle mani dei giapponesi, potremmo finire per non avere più una industria di semiconduttori. Potremmo perdere di default la corsa tecnologica» [26]. L'impulso congressuale, dovuto soprattutto al senatore democratico del Nebraska John Exon, porta all'approvazione dell'emendamento Exon-Florio al Defence Production Act, istituendo il potere per il presidente di sospendere o proibire fusioni e acquisizioni straniere che mettono in pericolo la sicurezza nazionale, a seguito di un'istruttoria del Cfius. La sicurezza nazionale mantiene una definizione ambigua, nei vari interventi che revisionano il ruolo del Cfius, per esempio nel 2007 con l'approvazione del Foreign Investment in the United States Act (Finsa). Ciò accade perché la sicurezza nazionale, per un impero, è ciò che esso vuole che sia.

Oggi la sicurezza nazionale, nella prospettiva degli Stati Uniti, non è legata solo agli armamenti o alla protezione dal terrorismo, ma riguarda la «capacità tecnologica di lungo termine, il vigore economico e finanziario di lungo termine, e la privacy nel lungo termine dei dati medici e finanziari dei cittadini, oltre che altre forme di dati» [27]. La sicurezza nazionale non risponde a statiche definizioni politologiche o accademiche. Aderisce alla realtà della propria sopravvivenza. E risponde alle sfide, agli avversari, trasformandosi e adeguandosi. Pertanto, i casi Cfius possono e potranno essere letti anche secondo la lente geopolitica.

La riforma che porta al rafforzamento dei poteri reca il segno di due casi, entrambi emersi del 2005, riguardanti gli investimenti di China National Offshore Oil Corporation e Dubai Ports World. Segni geopolitici dell'importanza della sicurezza energetica e del sistema portuale internazionale.

La situazione presente svela un altro significato dell'acronimo Cfius: Chinese Foreign Investment in the United States. Il principale oggetto di scontro riguarda, ancora una volta, la dimensione spaziale della tecnologia: l'hardware. L'escalation è avviata durante l'amministrazione Obama, con l'offerta d'acquisto di 670 milioni di euro lanciata nel maggio 2016 dal fondo di investimenti cinese Fujian per Aixtron, azienda tedesca focalizzata sui mercati asiatici, quotata alla Borsa di Francoforte e attiva nella produzione di chip. L'operazione è finanziata da Sino Ic Leasing Co, controllata di China Ic Industry Investment Fund, partecipata del governo cinese. Il 2 dicembre 2016 il presidente Obama decide di bloccare la transazione per le attività di Aixtron negli Stati Uniti, poi portando all'abbandono dell'offerta da parte di Fujian. Nel novembre 2016 Canyon Bridge Capital Partners, fondo di *private equity* col sostegno finanziario del governo cinese, annuncia l'intenzione di acquistare Lattice Semiconductor, impresa americana produttrice di semiconduttori, per 1,3 miliardi di dollari. Nel settembre 2017, Trump blocca la transazione [28]. Nel 2018,

26. B. Lojek, *History of Semiconductor Engineering*, Berlino-Heidelberg 2007, Springer, p. 173. Stephen Bryen ha ricoperto in seguito diversi altri incarichi in materia di difesa e tecnologia, anche come presidente di Finmeccanica North America e commissario della U.S.-China Security Review Commission.
27. M. Kuo, «CFIUS Scrutiny of Chinese Investment. Insights from Robert Hockett», *The Diplomat*, 8/1/2018, goo.gl/3V2rbD
28. *Order Regarding the Proposed Acquisition of Lattice Semiconductor Corporation by China Venture Capital Fund Corporation Limited*, 12/9/2017.



i casi Broadcom/Qualcomm e Zte aumentano ulteriormente il rilievo della sicurezza nazionale negli investimenti. Il 12 marzo, Trump blocca l'acquisizione da 117 miliardi di dollari da parte di Broadcom, che ha sede a Singapore, della statunitense Qualcomm [29], basandosi sull'istruttoria Cfius. In una lettera del 5 marzo ad Aimen Mir, allora vice sottosegretaria al Tesoro per la sicurezza degli investimenti, Trump illustra quanto la decisione sia stata influenzata dalla minaccia cinese. Aggiungendosi alle «ben note preoccupazioni di sicurezza nazionale su Huawei e altre aziende cinesi di telecomunicazioni», l'operazione colpirebbe la capacità di ricerca e sviluppo degli Stati Uniti e, soprattutto, favorirebbe il dominio cinese negli standard 5G, anch'essi di interesse nazionale per gli Stati Uniti [30].

29. *Presidential Order Regarding the Proposed Takeover of Qualcomm Incorporated by Broadcom Limited*, 12/3/2018.
30. La lettera si può consultare nel sito della Sec, goo.gl/JUpQDL

A proposito delle note preoccupazioni: una delle principali imprese digitali cinesi, Zte, nel 2016 è stata accusata di violare le leggi americane sulle sanzioni all'Iran e alla Corea del Nord. Viene raggiunto un accordo monetario nel 2017 tra l'azienda e le autorità statunitensi, che impone alla società una multa e alcune precise prescrizioni. Nell'aprile 2018 il dipartimento del Commercio indica il mancato rispetto da parte di Zte delle prescrizioni e decide di colpirne la giugulare, vietandole per sette anni di acquistare prodotti da fornitori degli Stati Uniti (come i semiconduttori di Qualcomm e Intel). Una mossa in grado di portare Zte alla bancarotta, che infatti nel maggio 2018 annuncia di cessare le proprie operazioni. A seguito di un intervento personale del presidente Trump su richiesta di Xi Jinping, le condizioni imposte a Zte vengono ridotte nel giugno 2018, rendendo possibile la sua sopravvivenza. Previo commissariamento. Il 24 agosto 2018[31] l'ufficio relativo a industria e sicurezza del dipartimento del Commercio sceglie Roscoe C. Howard, Jr. per coordinare la *compliance* dell'azienda, con un accesso senza precedenti e un mandato molto ampio per monitorare il rispetto delle leggi degli Stati Uniti sul controllo delle esportazioni da parte di tutto il gruppo. L'amministrazione Trump e il Congresso marciano uniti nell'attenzione per il Cfius, espandendo le sue caratteristiche e la sua potenzialità di intervento, tramite il Firmma (Foreign Investment Risk Review Modernization Act). Il 10 ottobre 2018 il dipartimento del Tesoro identifica, *ad interim*, 27 industrie di applicazione, che comprendono la manifattura aeronautica, le batterie, le trasmissioni radiotelevisive e le reti di telecomunicazione, la ricerca e sviluppo in biotecnologie e nanotecnologie. E ovviamente i semiconduttori.

Oggi solo il 16% dei semiconduttori usati in Cina sono prodotti nell'Impero del Centro. È un obiettivo indiretto della sicurezza nazionale degli Stati Uniti impedire alla Cina di raggiungere gli obiettivi di autonomia fissati dalla pianificazione del Partito (40% nel 2020 e 70% nel 2025[32]). Per questo Washington potrebbe colpire – se necessario – anche gli altri investitori asiatici che marciano insieme ai capitali cinesi, come la finanza sovrana di Singapore[33].

La guerra fredda tecnologica tra Pechino e Washington può portare sia a ricomposizioni negoziali su altri tavoli che a dissidi ancora più profondi in ambito culturale, fino a barriere reciproche nella ricerca e a una netta riduzione dell'interscambio tra studenti. In questa «trappola di Tucidide tecnologica», altri animali possono restare impigliati. Anzitutto, l'Unione Europea, che si presenta in una posizione di debolezza in merito alla frontiera scientifico-tecnologica rispetto agli Stati Uniti e alla Cina. La capacità di incidere sulla frontiera scientifico-tecnologica richiede, se non il *junmin ronghe* cinese, un circolo virtuoso tra in-

31. Si veda «U.S. Department of Commerce Announces Selection of ZTE Special Compliance Coordinator», Office of Public Affairs, Department of Commerce, 24/8/2018, goo.gl/aPGuX7

32. G. Levesque, «Here's How China Is Achieving Global Semiconductor Dominance», *The National Interest*, 25/6/2018.

33. Il fondo Temasek Holdings è tra gli investitori di Hou An Innovation Fund. Si veda M. Chan, C. Ting-Fang, «Arm's China Joint Venture Ensures Access to Vital Technology», *Nikkei*, 3/5/2018, goo.gl/4ySd6v

dustrie civili e militari, un sentire comune capace di far circolare le idee. Gli Stati dell'Unione Europea dovrebbero uscire dalla loro «vacanza dalla storia» e accettare di vivere in un mondo in cui difesa e sicurezza determinano in modo decisivo l'esistenza e la sostenibilità dei progetti politici. Improbabile. L'Unione Europea sarà oggetto, non soggetto, della geopolitica della protezione. Se non per la sua competizione interna, come quella tra Italia e Francia. Caduto il suo appello per costruire una «Darpa europea», cioè per rafforzare la tecnologia francese coi soldi degli altri, Emmanuel Macron si fa la Darpa francese, sfruttando il proprio lungimirante aumento delle spese militari [34]. Non nasceranno giganti tecnologici europei che abbiano autonomia militare, e pertanto decisionale. Le regolazioni europee, e i poteri speciali dei vari Stati, andranno perciò considerati come pedine della guerra fredda tecnologica tra Washington e Pechino. Che toccherà la geopolitica della protezione degli algoritmi e dagli algoritmi, ma anche dell'hardware, della logistica, dei cavi.

5. Lo storico israeliano Yuval Noah Harari, che ha venduto dodici milioni di libri, illustra il futuro che ci attende nel 2048. Tra trent'anni, al risveglio mattutino fronteggeremo «migrazioni nello spazio cibernetico, identità di genere fluide e nuove esperienze sensoriali generate da computer impiantati nel corpo». Harari ne è certo: al compimento dei trentacinque anni diremo di essere «una persona di genere indefinito che si sta sottoponendo a un intervento di aggiornamento anagrafico, la cui attività neocorticale ha luogo principalmente nel mondo virtuale New Cosmos, e la cui missione esistenziale è andare dove nessuno stilista è mai andato prima» [35]. Il novello Marx-Engels non ha dubbi: «Entro il 2048, anche le strutture fisiche e cognitive si dissolveranno nell'aria o in una nuvola di dati» [36]. O forse anche le sue nuvole, nel 2048, risiederanno più prosaicamente nel presidio geopolitico delle terre e dei mari. Specialmente in terra d'Israele.

34. M.G. Barone, «Una DARPA francese», *RID*, 3/4/2018, goo.gl/SrEZjx
35. Y.N. Harari, *21 lezioni per il XXI secolo*, Milano 2018, Bompiani, p. 383.
36. *Ivi*, p. 382.