USA, CINA, RUSSIA, cyberpotenze

Pubblicato sul **n. 297**, **maggio 2022**, della **Rivista Informatica "Storia in Network"** (www.storiain.net) con il titolo "**CYBERPOTENZE, USA, RUSSIA, CINA**"

Si dice cyberpotenza una entità pubblica o privata, che dispone di una capacità nello specifico settore, associata ad una strategia dedicata. Il cyberspazio rappresenta il quinto ambiente strategico (gli altri quattro sono la terra, il mare, l'aria e lo spazio) costituito dall'insieme dei sistemi d'informazione, di comunicazione, di controllo e dei dati che vi transitano, nelle sue funzioni civili e militari. Per semplificazione il cyberspazio si suddivide in tre strati: quelli informativo (detto semantico), quello software (logica) e quello materiale (fisico; hardware). Il cyberspazio dispone, inoltre, di una particolarità che influenza gli altri ambienti: la sua trasversalità, dove sono presenti componenti cyber.

Nel contesto delle cyber potenze, gli atteggiamenti degli USA, della Cina, della Russia, di Israele e del Regno Unito, oltre la Francia sono ormai meglio comprensibili in funzione dei testi ufficiali dei commentatori degli affari del cyberspazio e sulla base di rivelazioni. Alti paesi, più discreti, come il Giappone, le due Coree, l'Italia, il Brasile, l'Iran o la Germania hanno intenzione di rinforzarsi in questo settore strategico, spesso con il sostegno di cyber potenze affermate. Tutti gli indicatori ed i misuratori di potenza nello specifico settore sono concordi nell'affermare che sul podio di questa speciale graduatoria si trovano USA, Cina e Russia.

USA, campione storico

Senza dubbio, gli USA beneficiano ancora oggi del vantaggio tecnico offerto dalla

creazione e della diffusione allargata di internet. La messa in applicazione nell'ambito dell'**IPTO** (Information Processing Research Techniques Office), associando la preveggenza di **Joseph Licklider** (1915-1990) e i sussidi della **DARPA** (Defense Advanced Research Projects Agency, affiliata al Ministero delle Forze Armate americane), hanno dato vita alla prima rete di computer interconnessi, l'**Arpanet**, nell'ottobre 1969. Questa presenza di lunga data nel settore si è tradotta in un dominio strategico, che ha preso le sue mosse negli anni 1990 con il concetto di "autostrade dell'informazione", pubblicizzato dal vice presidente **Al Gore** (1948-), al fine di annunciare l'inizio di un grosso cantiere di ammodernamento delle telecomunicazioni (*Telecommunications Act* del 1996). Le autorità americane "hanno distribuito" il loro internet nel mondo, in armonia con una visione liberale conquistatrice conseguente all'implosione dell'URSS, pur mantenendo in mano una leva di de connessione (*kill switch*) più teorica che pratica (l'**Icann**, che gestisce i nomi dei domini mondiali non risulta più sotto la tutela del Ministero del Commercio americano dall'ottobre 2016).

Resta comunque il fatto che le capacità d'azione di questa cyber potenza sono reali, come quando lo ha rivelato **David E. Sanger** (1960-), giornalista del New York Times, divulgando il programma di cyber attacchi avanzati **Stuxnet** (**1**). Questo virus, molto evoluto, ha provocato nel 2010 il malfunzionamento delle centrifughe di arricchimento dell'uranio di Natanz, generando un conseguente ritardo nel programma nucleare iraniano

Quando si sa che il bilancio americano per le agenzie di intelligence ha raggiunto ufficialmente i 63 miliardi di dollari nel corso del 2020, si può ragionevolmente ipotizzare che la **NSA (National Security Agency**), per le sue specifiche missioni (spionaggio e controspionaggio) e per il suo territorio di "caccia" (tutti i tipi di telecomunicazioni) sia stata particolarmente favorita.

Come quasi sempre, a causa della difficoltà di attribuzione (vale a dire la difficoltà di determinare chi è l'aggressore o almeno il responsabile della concezione di un sistema informatico malevolo), si può anche subodorare che la NSA sia, ad esempio, all'origine del software dannoso Regin, che ha realizzato il compito di spionaggio delle istituzioni europee a Bruxelles (**2**) nel corso degli anni 2000. Tuttavia, i dati trasmessi nel 2013 da **Edward Snowden** (1968-), lavoratore a contratto per la NSA, consentono di confermare quello che numerosi esperti del settore avevano ipotizzato: questi ultimi hanno potuto mettere un nome a dei sistemi di sorveglianza elaborati, scoperti come **XkeyScore** o

PRISM.
Gli USA, nonostante la loro enorme potenza, devono fronteggiare altri attori del cyberspazio, capaci di contrastare le operazioni condotte contro di loro e in condizioni a loro volta di preparare ed eseguire operazioni di tipo offensivo (esempio: il tentativo di paralisi di una rete elettrica della costa ovest americana il 5 marzo del 2019). Il documento del 6 ottobre 2020, proveniente dal **DHS** (Department of Homeland Security) l'Homeland Threat Assessement (**3**), é rivelatore della percezione delle Cyberminacce da parte degli USA a prossima e lunga scadenza. La parte ed il posto dedicato al cyberspazio risulta conseguente e le dichiarazioni lasciano poco spazio all'ambiguità: Cina, Iran, Russia e Corea del Nord vengono menzionate come le più pericolose per la sicurezza delle infrastrutture americane (va inoltre precisato che anche l'attività di organizzazioni criminali transnazionali risulta repertoriata come effetto di possibili attentatori all'integrità degli USA). Il documento scende nel dettaglio, esplicitando che l'attivismo russo costituisce una minaccia attuale e continua e che è soprattutto di ordine politico ed, in minor misura, economica. Mentre le attività di cyber spionaggio cinesi, sempre secondo questa nota, necessitano prioritariamente un particolare attenzione rispetto al passato a causa della competizione economica e finanziaria frontale, iniziata sotto la presidenza Trump e della crescita rapida delle capacità cyber della Cina.
Insomma, anche se gli USA dispongono di mezzi cibernetici adeguati, il loro dominio nell'ambiente cibernetico viene scosso da due Stati, che intendono condurre una guerra asimmetrica: di fronte alla potenza economica e tecnologica americana. Il cyberspazio appare, per questi due rivali, un eccellente terreno per la condotta di operazioni mascherate o coperte, idonee ad indebolire il loro avversario geopolitico, senza peraltro sfociare in un conflitto di tipo convenzionale.

La Russia, l'orco cybernetico
Se ci si dovesse basare solo sull'esposizione mediatica, è un fatto manifesto che la Russia rappresenta una cyberpotenza onnipresente, se non onnipotente, se non fosse per i numerosi articoli dedicati agli eventi cibernetici che gli vengono attribuiti a torto come a ragione.
Un elemento da comunque ragione a coloro che disprezzano: l'eccellenza degli ingegneri informatici della Federazione della Russia, eredi delle filiere scientifiche dell'URSS. In tal

modo, in occasione delle competizioni internazionali di programmazione come l'***ICPC***, gli studenti russi terminano quasi regolarmente sul podio (in occasione dell'edizione del 2019, l'Università di Stato di Mosca ha vinto la competizione davanti al Massuchussets Institute of Technology ed all'Università di Tokio). All'***IOI*** (Olimpiadi Internazionali dell'Informatica); la Russia totalizza quasi 116 medaglie, di cui 65 d'oro (gli USA ne contano 107 e la Cina 127). Il Paese dispone anche di istituti specializzati in settori molto complessi, come l'***IKSI*** (Istituto di Telecomunicazioni, di Criptografia e di Scienze informatiche) o la prestigiosa università di telecomunicazioni di San Pietroburgo.
Questo fatto potrebbe (il condizionale é d'obbligo) spiegare le fughe di documenti del Partito Democratico Americano, in occasione delle presidenziali del 2016 o la grande campagna di cyber attacchi contro le agenzie governative americane dal marzo al dicembre 2020. L'assenza di firme evidenti e di rivendicazioni ufficiali impedisce, tuttavia, qualsiasi attribuzione definitiva,ma il semplice fatto di sospettare i servizi e gli ingegneri russi dietro queste operazioni di grande ampiezza, attesta il riconoscimento implicito delle loro reali capacità d'azione nella cibernetica.
Per sapere come le autorità russe considerino il cyberspazio, è assolutamente necessario prendere conoscenza di due testi: il primo è la dottrina di sicurezza internazionale della Federazione della Russia del 9 settembre 2000 (**4**), attualizzata in data 5 dicembre 2016; il secondo è la legge per l'internet sovrano (nazionale) del 1° maggio 2019. Il primo testo riveste una grande importanza poiché insiste prioritariamente sull'aspetto civilizzatore della sfera informatica, dove si sviluppa una guerra informatica condotta con armi informatiche: in definitiva è l'aspetto umano che costituisce l'anello debole e non l'aspetto tecnico. Il secondo testo deriva dalla volontà di premunirsi da un tentativo di interrompere l'internet mondiale e di garantirsi, in tal modo, una continuità di servizi per l'ecosistema russo (denominato RuNet). E' anche in questa ottica che è stato approntato e messo in opera il sistema di pagamenti interbancari MIR, al fine di parare qualsiasi paralisi volontaria o accidentale della rete Mastercard, Via o Paypal.
La Russia è fortemente sospettata di condurre operazioni ibride nel cyberspazio: laddove i servizi di informazioni americani e cinesi intendono controllare l'insieme della catena delle operazioni cibernetiche condotte attraverso il mondo, le autorità russe sembrano appoggiarsi, in misura diversa e livelli, sulle capacità e competenze dei loro servizi, rinforzati dall'ingegnosità e dall'intraprendenza della loro riserva nazionale di hackers, che

per certi aspetti possono essere considerati come "corsari" dello spazio. Questa ibridazione complica l'attribuzione delle azioni che vengono condotte e minimizza, in caso di scoperta di una operazione di vasta porta il rischio di essere accusato un organo di Stato.
Tuttavia, ed il discorso vale anche per la Cina, la Russia anche la Russia costituisce l'oggetto di regolari cyber attacchi, provenienti da strutture private o statali (**5**). Di fatto, nel novembre 2016, diverse banche russe hanno subito un'ondata di forti attacchi. Questa realtà, spesso occultata mediaticamente, relativizza alquanto il suo statuto di sempiterno aggressore del cyberspazio.

La Cina, la pretendente al primo posto

L'Impero di Mezzo è effettivamente considerato dagli USA come il rivale di domani e numerosi elementi non mancano di pesare sulla bilancia dei rapporti di potenza.
In primo luogo, la Cina può contare su un mercato interno fenomenale, formato da 989 milioni di internauti, su una popolazione di 1,44 miliardi di abitanti. Indubbiamente, questa situazione apre la porta ad una miriadi di sbocchi commerciali per le società che abbracciano o alimentano la rivoluzione numerica, di cui la **BATXH** (vale a dire i conglomerati: Baidu, Alibaba, Tencent, Xiaomi e Huawei) costituisce la parte più visibile dall'esterno. E questa opulenza demografica offre un serbatoio abbondante di talenti in ingegneria informatica, fatto che, analogamente alla Russia, viene attestato dei brillanti risultati nelle competizioni dedicati a questo settore (come l'IOI sopradetto). La Cina dispone, inoltre, di un corpo dottrinale che è spesso paragonato, in maniera semplicistica (**6**), al gioco del Go (gioco da tavolo strategico cinese fra due giocatori), consistente, al contrario degli scacchi, che mirano ad una vittoria frontale decisiva, in un lento ed inesorabile accerchiamento dell'avversario. Sulla base dei pochi elementi filtrati dal Paese, non si è in condizioni di estrarne la sua cyber strategia, a meno che sci si basi sui suoi *Libri Bianchi* dedicati alla difesa come quello del 2019. Si può, tuttavia, subodorare attivamente che l'Esercito Popolare di Liberazione dispone di sue proprie unità raggruppate intorno al Centro di Comando delle Forze Strategiche.
Ma soprattutto, la Cina possiede la capacità di agire sui tre strati del cyberspazio: 5G, intelligenza artificiale, calcolo quantico, elettromobilità, trasporti autonomi inoltre il Paese si è preoccupato di acquisire le materie prime, di produrre componenti ed

infrastrutture di telecomunicazioni, di sviluppare applicazioni, di sviluppare reti sociali capaci di assicurare la viabilità di tutto un ecosistema. E tutto questo con costituisce una semplice scommessa, in quanto per il momento, solo gli USA sono in condizioni di aspirare al controllo di questi tre strati., sebbene anche in questo campo la pressione asiatica diventi sempre più sensibile. Si tratta anche di una continuità sistemica attraverso le strade della seta, lanciata nel 2013 e che prosegue nella sua variante numerica come viene attestato dall'aggregazione degli operatori Cina Telecom e China Unicom al transito Europa-Asia, un cavo ad alto volume di traffico che attraversa la Russia da est ad ovest e supervisionato dall'operatore russo RosTelecom. Questo progetto dovrebbe prolungarsi fino al Giappone da un lato e fino in Germania dall'altro, fatto che spiega l'interesse delle autorità cinesi di diventare un agente indispensabile delle reti di comunicazioni Europa Asia.

La Cina si inorgoglisce di disporre del suo grande scudo dorato, la cui parte cibernetica si chiama *Grande Firewall*, o Grande Parafuoco, un gioco di parole in inglese che crea una analogia con la Muraglia cinese (The Great Wall). Non si tratta, in senso stretto, di una evoluzione tecnologica, ma di un insieme di disposizioni normative (come ad esempio: l'obbligo di proteggere i sistemi di informazione nazionali per mezzo di società autorizzate) e tecniche (l'analisi ed il filtraggio in tempo reale di dati sulle reti numeriche (detta anche, altrove, ispezione profonda dei pacchetti di informazioni): una architettura concepita ufficialmente da **Fang Binxing** (1960-), messa in opera dalla Commissione Centrale degli Affari del Cyberspazio e che risulta accusata dagli Occidentali di partecipare alla censura dell'internet cinese, ma che, nel suo altro versante, individua e blocca i tentativi esterni di destabilizzazione delle reti numeriche.

In effetti, se la Cina viene spesso citata per la condotta di campagne di cyberspionaggio (**7**), (si possono ricordare a tale riguardo le accuse del 2004 per Titan Rain - attacchi informatici della Cina ad alcune agenzie di governo USA - o del 2017 per Stone Panda o Red Apollo – attacchi informatici cinesi a compagnie giapponesi), essa è stata, a sua volta, oggetto di tentativi di intrusione cibernetici più o meno efficaci dall'interno come dall'esterno. E' probabilmente questa una delle sue grandi debolezze: l'aumento crescente dei mezzi allocati alla cibernetica del Grande Para Fuoco, coniugato con l'aumento di numerose cyberminacce esterne ed interne, determinerà un costo umano, tecnico e finanziario di grande ampiezza, che potrebbe risultare sproporzionato con le possibilità

effettive dello Stato cinese. A tutto questo va aggiunto il rischio di una fossilizzazione dell'ecosistema, che ha consentito di dare la nascita al BATXH, come anche a molteplici entità dinamiche. La possibilità di un esaurimento dell'internet cinese rappresenta una ipotesi da non sottostimare.

Conclusione

Se gli USA degli anni 1990 hanno fatto del Cyberspazio la loro nuova frontiera (**8**), esportando in modo originale i loro principini democrazia liberale, essi si scontrano ormai contro due formidabili avversari, che, ciascuno a suo modo, sono capaci di portare le loro minacce fino ai centri più nevralgici americani, proponendo un'altra visione del cyberspazio. Tuttavia, ad una analisi più attenta, il vero nemico degli USA forse si cela nell'autonomia sempre più crescente dei suoi conglomerati. In effetti, appare alquanto singolare che, mentre **Xi Jinping** (1953-) metteva in riga **Jack Ma Yun** (1964-), ambizioso miliardario e patron di Alibaba, per le sue dichiarazioni critiche verso la regolazione bancaria cinese, nello stesso periodo, le reti sociali occidentali censuravano un presidente americano in carica (**Donald Trump**, 1946-), senza aver atteso una qualsiasi condanna giudiziaria o politica preliminare. L'ecosistema della Silicon Valley, che è ormai diventato un centro di potere e che desidera agire secondo per proprio conto, avido di dati e di immortalità, potrebbe essere l'elemento in condizioni di minare dall'interno la cyberstrategia USA, laddove, Cina e Russia riescono a contenere queste velleità interne al prezzo di enormi sforzi. Tutto questo perché il gioco delle cyberpotenze statali risulta condizionato da queste entità private, per certi aspetti parassitarie, mastodonti finanziari e detentori di una potenza algoritmica determinante nella loro volontà di modellare a loro piacimento il nuovo uomo numerico. Risulta ormai un fatto acquisito che il cyberspazio è un ambiente conflittuale, dove ogni attore intende difendere i suoi propri interessi e diffondere la sua specifica percezione della civiltà: vi si svolge una lotta continua, che rappresenta e traduce in pratica un reale rapporto di forze contemporaneo.

NOTE

(1) **Sanger David E.,** *Confront and Conceal: Obama's Secret Warsand Surprising Use of American Power*, Broadway Books, 2013;

(2) **Marquis-Boire Morgan, Guarnieri Claudio, Gallagher Ryan**, *Secret Malaware in*

European Union Attack .Linked to US and British Intelligence, The Intercept, novembre 2014;
(**3**) Homeland Threat Assessment, Department of Homeland Security
(**4**) **Harrel Yannick**, *La Cyberstrategia russa,* Nuvis, 2013;
(**5**) **Ventre Daniel**, *Riflessioni generali sul cyber crimine e la cyber sicurezza alla luce del caso russo*, Cyber Circle, marzo 2021;
(**6**) **Fitz Jason**, *China's Cyber Warfare: The Evolution of Strategic doctrine*, Lexington Books, 2017 ;
(**7**) **Fremicourt Julia, Parent Yves, Sali Hichem**, *Il cyber spionaggio cinese*, EGE, dicembre 2018;
(**8**) **Harrel Yannick**, *Il concetto americano di nuova frontiera: dalla conquista dell'Ovest al Cyberspazio*. Diploweb, maggio 2016.